Appendix 2

Research on Data Related Regulations of AMSs Utilised in Chapter 3

As explained in the Chapter 2, based on the research items identified, we collected information on AMSs' regulations on data flows. Here, we will show the outcomes. As we need to cover all the items for 10 AMSs, there are blank cells indicating no regulations of the specified items in a AMS. There are regulations identified in Annex A, but have no corresponding item in Annex B. This means such regulations have no regulation on data flows. We intentionally indicate as it is, because this meaning that they are thought by secondary sources as a regulation on data flows but in reality,they do not regulate. This is also important information for businesses.

For example, Singapore banking law of 1970 is referenced by secondary source as "In addition, certain sector-specific laws such as the Banking Act 1970 and the Securities and Futures Act 2001 include provisions relating to the protection of certain personal data" (Linklaters, Data Protected – Singapore (2024)[1]). However, it stipulates only one article, Art. 47 on privacy of customer data and no stipulations of definitions of such data, legal basis or other items identified in Chapter 2. Therefore, we do not cite any substantial item on banking law.

A) Brunei Darussalam

Legal System Overview

#	Regulation	Translation	Purpose of the Legal System
			What purpose does the legal system serve? (e.g. cybersecurity)
		Google translation or Translation by certain organization	
1	Personal Data Protection Order		1.2 The rationale of introducing this data protection law is two-fold: 1.2.1 to provide for the protection of individuals' personal data by private sector organisations (including both commercial and non-commercial organisations) which seek to collect, use, disclose or otherwise process such personal data for their purposes; and 1.2.2 to facilitate

[1] https://www.linklaters.com/ja-jp/insights/data-protected/data-protected---singapore

			cross-border flows of personal data, which will further the development of the digital economy in Brunei Darussalam.
2	Banking Order 2006		providing for the licensing and regulation of the businesses of banks,
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation	Form of legal system	Target Business
		Is it introduced in accordance with government ordinances and guidelines? (Is it introduced in a format that ensures lead time?)	Does the law target specific industry or in general? Is it clearly stated in the regulations?
		Regulation level	Industry
1	Personal Data Protection Order		General
2	Banking Order 2006	Law	Bank
3	Islamic Banking Order, 2008	Law	Bank
4	Data Protection Policy, 2015 (Revised version)	Policy	
5	Accountants Order, 2010	Law	Others
6	Legal Profession Act, 1987, Cap. 132	Law	Others

#	Regulation	Regulatory authority	Jurisdiction
		Which regulatory authority has jurisdiction over regulation?	Cyber security, data security, personal information protection, etc.
		Name of ministry/organization	Similar to purpose?
1	Personal Data Protection Order	1.5 In response to this, MTIC has given AITI the mandate to develop and implement a	Personal data protection

		framework for the protection of individuals' personal data by the private sector. AITI has developed and prepared the draft PDPO, which sets out a general data protection framework which will apply to the private sector in Brunei Darussalam.	
2	Banking Order 2006	Autoriti Monetari Brunei Darussalam	Finance
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation	Status	Citation
		Legislation / Public Comment / Passage / Enforcement / Amendment, etc.	
		Status of the regulation: Draft = drafting (new regulation) published = published in the gazzette but not yet enacted Enact = published in the gazzette and already enacted Amendment = enacted regulation being on amending process	URL
1	Personal Data Protection Order	Public Consultation	https://www.aiti.gov.bn/media/jc4mhify/pcp_personaldataprotectionprivatesector_20052021_final3.pdf
2	Banking Order 2006	Enforcement	https://www.agc.gov.bn/AGC%20Images/LAWS/BLUV/BANKING%20ORDER,%202006.pdf
3	Islamic Banking Order, 2008	Enforcement	—
4	Data Protection Policy, 2015 (Revised version)	Enforcement	https://www.information.gov.bn/PublishingImages/SitePages/New%20Media%20and%20IT%20Unit/Data%20Protection%20Policy%20V.2.2.pdf
5	Accountants Order, 2010	Enforcement	—

6	Legal Profession Act, 1987, Cap. 132	Enforcement	https://www.agc.gov.bn/AGC%20Images/LAWS/ACT_PDF/Cap132(06).pdf

Definitions for basic items

#	Regulation	Type and Scope of Data	Data processing and handling
		Personal data, personal information/sensitive and important data/children and minors' data, etc. Is the scope of data clearly written in the regulations? What are the unclear points?	Processing, handling / disclosure, sharing, provision, transmission, outsourcing / use for advertising, etc.
		Specific type of data required to complied with the regulation	Provision for data processing
1	Personal Data Protection	3.2 Categories of Personal Data 3.2.1 Personal data under the PDPO includes personal data which may be of a more sensitive nature, for example, data concerning the physical or mental health of an individual, financial information, genetic data, biometric data and personal history involving any criminal offence. 3.2.2 However, the PDPO does not expressly recognise a distinction between sensitive and non-sensitive categories of personal data or define a category of "sensitive personal data". It is proposed that the PDPO applies across all types of personal data as a baseline, although sector-specific frameworks may address specific concerns relating to different types of data (e.g. financial data). This approach is consistent with some laws, such as Singapore's Personal Data Protection Act 2012, although it differs from others, such as EU's General Data Protection Regulation. 3.2.3 As personal data which is of a more sensitive nature falls within the definition of personal data in the PDPO, it is subject to all the obligations in the PDPO. Organisations complying with	

		the PDPO are required, as part of acting reasonably, to take into account the sensitivity of the personal data in question where appropriate, for example, in assessing the amount of information to be provided to individuals when collecting their personal data or when determining the security arrangements to be put in place to protect the personal data. 3.2.4 Accordingly, organisations implementing policies and practices to comply with the PDPO would need to take into account the specific personal data in question (amongst other factors), for instance, how "sensitive" it may be. This may entail an assessment of the category of personal data and how the individual may be impacted should the personal data be subject to unauthorised access, disclosure or other risks.	
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation	Data handlers
		Classification/ distinction by responsibility (data processor, data controller)/ size of data, (national security) critical services, etc.
		Provision on type of data handler

1	Personal Data Protection	3.3 Organisations 3.3.1 In general (and subject to the specified exceptions noted in paragraph 3.4 below), the PDPO will apply to organisations, which is defined in the PDPO to mean "any individual, company, association or body of persons, corporate or unincorporated, whether or not (a) formed or recognised under the law of Brunei Darussalam; or (b) resident, or having an office or place of business, in Brunei Darussalam". 3.3.2 The PDPO will maintain a baseline regime that applies to all private sector organisations, including small businesses that have low annual turnover, to ensure a minimum data protection standard across the private sector. AITI notes that the exemption of small companies in some jurisdictions has added to the complexities of implementation and such exemptions may encourage larger companies to set up smaller entities to circumvent the law. 3.7 Data Intermediaries / Processors 3.7.1 The PDPO contains a partial exception for "data intermediaries" (sometimes referred to as "data processors") that process personal data on behalf of another organization or a public agency. Such data intermediaries / processors doing so pursuant to a contract which is evidenced or made in writing are subject to a reduced number of Data Protection Obligations, namely: (a) the Protection Obligation referred to in paragraph 4.2.9 below; (b) the Retention Limitation Obligation referred to in paragraph 4.2.10 below; (c) the Transfer Limitation Obligation referred to in paragraph 4.2.11 below; and (d) the duty to notify the organisation or public agency under the Data Breach Notification Obligation as referred to in paragraph 4.2.12 below. 3.7.2 In this regard, the PDPO provides for a category of organisations called "data intermediaries/ processors". A data intermediary / processoris an organisation which processes personal data on behalf of another organisation or public agency. This is in contrast with organisations (sometimes referred to as data controllers) which have direct control over the means and purposes for processing of the personal data. 3.7.3 The term "processing", in relation to personal data, is defined in the PDPO to mean the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following: collection; recording; holding or storage; organisation, structuring, adaptation or alteration; retrieval; alignment or combination; use; disclosure by transmission, dissemination or otherwise making available; or erasure or destruction. 3.7.4 Data intermediaries / processors are required to comply with fewer Data Protection Obligations in view of their limited role in connection with the processing of personal data including, in particular, their lack of control over the purposes and other aspects of data processing (e.g. the scope of the data intermediary / processor's activities in relation to such personal data is restricted and subject to the contract between the data controller and the data

		intermediary / processor). 3.7.5 Subjecting data intermediaries / processors to fewer Data Protection Obligations will also reduce compliance costs for such organisations and potentially transactions costs as between data intermediaries / processors and data controllers. 3.7.6 Nonetheless, the organisations or data controllers engaging these data intermediaries / processors will be subject to the Data Protection Obligations in respect of personal data processed on its behalf and for its purposes by a data intermediary / processor as if the personal data were processed by the organisation or data controller itself. 3.7.7 Such an approach is also consistent with international norms as data protection regimes in most countries similarly require data controllers to be fully compliant with data protection laws and remain liable, even where they outsource the processing of personal data to a third party, regardless of whether there is a formal distinction between data controllers and data processors (as in the EU).
2	Banking Order 2006	
3	Islamic Banking Order, 2008	
4	Data Protection Policy, 2015 (Revised version)	
5	Accountants Order, 2010	
6	Legal Profession Act, 1987, Cap. 132	

Legal basis

#	Regulation		
		consent	necessary for the performance of a contract
1	Personal Data Protection	4.6.1 Under the PDPO, an individual's consent is required before an organisation can collect, use or disclose such individual's personal data, unless otherwise required or authorised by law or an exception in the PDPO applies. Such consent must be validly obtained and may be either expressly given or deemed to have been given.	(b) if the collection, use or disclosure of the personal data is reasonably necessary for the conclusion of the contract between the individual and the organisation; and
2	Banking Order 2006		

3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation		
		necessary for compliance with a legal obligation	necessary in order to protect the vital interests
1	Personal Data Protection		
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation		
		necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	necessary for the purposes of the legitimate interests pursued by the controller or by a third party
1	Personal Data Protection		
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		

6	Legal Profession Act, 1987, Cap. 132		

#	Regulation		
		opt-out	others
1	Personal Data Protection Order	(c) if the organisation, after conducting a prescribed assessment for adverse effect on the individual, notify the individual of the new purpose and provide a reasonable period of time for them to opt out (provided that the individual does not opt out or otherwise withdraw their consent).	(a) if the individual, without giving express consent, voluntarily provides the personal data for that purpose; and it is reasonable that the individual would voluntarily provide the data;
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

Rights of the data subject

#	Regulation		
		Right to be informed	Right of access
1	Personal Data Protection Order		5.1.2 Right to request access to personal data; 5.3.4 Withdrawal of consent does not affect the legal consequences of withdrawal. In other words, if the individual subsequently withdraws consent to his personal data in a manner which makes it impossible for the contract to be fulfilled, any legal consequences arising out of such withdrawal would not be affected.

			5.4 Right to Request for Access to Personal Data 5.4.1 Under the PDPO framework, individuals have the right to request an organisation to provide them with their personal data that is in the possession or under the control of the organisation, and information about the ways in which that personal data has been or may have been used or disclosed within a year before the date of request for access, subject to exceptions. This is also known as the "Access Obligation". 5.4.2 An organisation is only required to provide the individual with access to his personal data and the requested information. The organisation is not required to provide the individual with access to excluded information under this Access Obligation (see paragraph 5.4.6 below). 5.4.3 An organisation must not accede to the individual's access request if the information requested could reasonably be expected to: (a) threaten the safety or physical or mental health of an individual other than the individual who made the request; (b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request; (c) reveal personal data about another individual; (d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or (e) be contrary to the national interest. 5.4.4 Sub-paragraphs (c) and (d)

			above do not apply to any user activity data about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual. 5.4.5 In this regard, "user activity data" is defined as personal data about an individual that is created in the course or as a result of the individual's use of any product or service provided by the organisation, while "user-provided data" is defined as personal data provided by an individual to the organisation. 5.4.6 Organisations are not required to disclose certain types of information when responding to an individual's access request. Upon receiving an access request, an organisation is not required to provide information that is: (a) opinion data solely kept for evaluative purposes; (b) an examination conducted by education institution, examination scripts, results; (c) personal data of beneficiaries of a private trust kept solely to administer the trust; (d) personal data kept by an arbitral institution or mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; (e) documents related to prosecution if all proceedings have not been completed; (f) personal data subject to legal privilege (g) personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of

			the organisation; (h) personal data collected, used or disclosed without consent (in accordance with the PDPO) for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed; or (i) the personal data was collected or created by a mediator or arbitrator in the conduct of a mediation or arbitration for which he was appointed to act by agreement between the parties to the mediation or arbitration; under any written law; or by a
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation	Right to rectification	Right to erasure
1	Personal Data Protection Order	5.1.3 Right to request a correction of an error or omission in the personal data; and 5.5 Right to Request for a Correction to an Error or Omission in Personal Data 5.5.1 An individual may request an organisation to correct an error or omission in his personal data. This obligation only extends to personal data that is in the organisation's possession or under its control. This is also known as the "Correction Obligation".	

		5.5.2 Unless the organisation issatisfied on reasonable grounds that a correction should not be made, the organisation shall correct the personal data as soon as practicable. 5.5.3 The organisation must also send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose. 5.5.4 When organisation A is notified by another organisation B of a correction of personal data, A shall correct the personal data in its possession or under its control unless organisation A is satisfied on reasonable grounds that the correction should not be made. 5.5.5 If no correction to the personal data is made despite a correction request, the organisation shall annotate the personal data record that the correction that was requested but not made. 5.5.6 An organisation is not required to correct or alter an opinion, including a professional or an expert opinion. 5.5.7 An organisation does not need to accede to an individual's correction request in certain situations. Upon receiving a correction request, an organisation not required to correct personal data that is: (a) opinion data solely kept for evaluative purposes; (b) an examination conducted by education institution, examination scripts, results; (c) personal data of beneficiaries of private trust kept solely to administer the trust;	

		(d) personal data kept by an arbitral institution or mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; (e) documents related to prosecution if all proceedings have not been completed; or (f) derived personal data.	
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation	Right to restrict processing	Right to data portability
1	Personal Data Protection		5.1.4 Right to data portability. 5.2 These data subject rights are not unfettered and will be subject to exceptions in the PDPO. When an individual exercises any of these rights, organisations would have a corresponding obligation to give effect to these rights. 5.6 Right to Data Portability 5.6.1 The PDPO may introduce a data portability obligation which requires a porting organisation to port an individual's data to another organisation under certain circumstances upon receiving a data porting request, unless an exception applies. This is also known as the "Data Portability Obligation". 5.6.2 When an individual submits a data porting request, the

			porting organisation is required to transmit the applicable data to the receiving organisation in the prescribed manner if certain conditions are fulfilled. The data porting request must satisfy the prescribed requirements and there must be an ongoing relationship between the individual and the porting organisation. 5.6.3 The Data Portability Obligation will only apply to "applicable data" which is held in electronic form, and that was collected or created by the porting organisation within the prescribed period. 5.6.4 In terms of exceptions, a porting organisation does not need to transmit applicable data that has been specifically excluded by the PDPO or applicable data in specifically excluded circumstances. 5.6.5 A porting organisation which does not transmit data upon receiving a data porting request must notify the individual of the refusal within the prescribed time and in the prescribed manner. 5.6.6 A porting organisation must preserve any data specified in a data porting request for the prescribed period of time (or longer). This obligation applies regardless of whether the organisation accedes to the porting request. A porting organisa
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		

6	Legal Profession Act, 1987, Cap. 132		

#	Regulation	Right to object	Right not to be subject to a decision based solely on automated processing
1	Personal Data Protection Order		
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation	Right to withdraw consent
1	Personal Data Protection Order	5. Data Subject Rights 5.1 The PDPO will give individuals four main rights: 5.1.1 Right to withdraw consent; 5.3 Right to Withdraw Consent 5.3.1 On giving reasonable notice to an organisation, an individual may, at any time, withdraw his consent in respect of the collection, use or disclosure of his personal data for any purpose by an organisation. This ability to withdraw consent applies to both express consent and deemed consent. 5.3.2 Under the PDPO, the organisation is required to inform the individual of the likely consequences of withdrawing his consent. 5.3.3 The organisation shall not prohibit an individual from withdrawing his consent. Moreover, upon withdrawal of consent, an organisation must cease (and cause its data intermediaries and agents to cease) to collect, use or disclose the personal data for such purposes.
2	Banking Order 2006	
3	Islamic Banking Order, 2008	
4	Data Protection	

	Policy, 2015 (Revised version)	
5	Accountants Order, 2010	
6	Legal Profession Act, 1987, Cap. 132	

Extraterritorial application

#	Regulation	applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction	applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction
1	Personal Data Protection		
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation	no express territorial scope, but would require some nexus to the jurisdiction	other
1	Personal Data Protection		3.6 Territorial Scope 3.6.1 The PDPO applies to all private sector organisations that collect, use or disclose personal data in Brunei Darussalam, regardless of whether they are formed or recognised under Brunei law or whether they are resident or have an office or place of business in Brunei Darussalam. 3.6.2 As such, organisations that

			are located overseas may still be subject to the PDPO as long as they collect, use or disclose personal data (i.e. engage in data processing activities) in Brunei Darussalam. In addition, organisations that collect personal data overseas and host or otherwise process it in Brunei Darussalam will also be subject to the relevant obligations under the PDPO from the point that such data is brought into Brunei Darussalam. 3.6.3 It is acknowledged that there might be practical difficulties in carrying out investigations and taking enforcement actions against organisations with no presence in Brunei Darussalam, and any complaints against or contraventions made by such organisations may not be adequately addressed. Nonetheless, as a matter of principle, the scope of the PDPO should cover these organisations, and such coverage may act as deterrence for these overseas organisations such that they will process personal data in a responsible and accountable manner that is consistent with the PDPO. The Responsible Authority may, in due course, cooperate with foreign data protection authorities where necessary and appropriate to investigate a matter with cross-border elements
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		

6	Legal Profession Act, 1987, Cap. 132		

#	Regulation	Representatives of controllers or processors not established in the country
1	Personal Data Protection	
2	Banking Order 2006	
3	Islamic Banking Order, 2008	
4	Data Protection Policy, 2015 (Revised version)	
5	Accountants Order, 2010	
6	Legal Profession Act, 1987, Cap. 132	

Notification obligation

#	Regulation	Data breach notification to authorities	Data breach notification to affected individuals
1	Personal Data Protection	4.14 The Data Breach Notification Obligation 4.14.1 Under the PDPO, organisations are required to, as soon as practicable, but in any case, no later than 3 calendar days after making the assessment, notify the Responsible Authority of a data breach that: (a) results in, or is likely to result, in significant harm to the individuals to whom any personal data affected by a data breach relates; or (b) is or is likely to be, of a significant scale. 4.14.2 Unless an exception applies or a waiver is granted, organisations will also be required to notify affected individuals on or after notifying the Responsible Authority, if the data breach results in, or is likely	4.14 The Data Breach Notification Obligation 4.14.1 Under the PDPO, organisations are required to, as soon as practicable, but in any case, no later than 3 calendar days after making the assessment, notify the Responsible Authority of a data breach that: (a) results in, or is likely to result, in significant harm to the individuals to whom any personal data affected by a data breach relates; or (b) is or is likely to be, of a significant scale. 4.14.2 Unless an exception applies or a waiver is granted, organisations will also be required to notify affected individuals on or after notifying the Responsible Authority, if the data breach results in, or is likely

		to result in, significant harm to an affected individual. 4.14.3 In this regard, this mandatory notification requirement allows organisations to receive guidance from the Responsible Authority on post-breach remedial actions where necessary and informs the Responsible Authority early of any possible systematic issues within the organisation, which Responsible Authority can seek to address. Notifying affected individuals allows them to take steps, where possible, to protect themselves (e.g. changing passwords, cancelling credit cards) in the event of a data breach. This encourages accountability in organisations but also allows the Responsible Authority to have oversight over data breaches at a national level. 4.14.4 With respect to the criteria for notification, the Responsible Authority will take a riskbased approach and impose a threshold for notification. This is because not all data breaches justify notification, especially where the impact of the data breach is minimal. It is acknowledged that organisations may require time to determine the veracity of suspected breaches. Accordingly, the time frame for notifying the Responsible Authority will thus commence from the time the organisation determines that the breach is eligible for reporting. Unreasonable delays in reporting breaches that cannot be justified will be considered a breach of the Data Breach Notification Obligation.	to result in, significant harm to an affected individual. 4.14.3 In this regard, this mandatory notification requirement allows organisations to receive guidance from the Responsible Authority on post-breach remedial actions where necessary and informs the Responsible Authority early of any possible systematic issues within the organisation, which Responsible Authority can seek to address. Notifying affected individuals allows them to take steps, where possible, to protect themselves (e.g. changing passwords, cancelling credit cards) in the event of a data breach. This encourages accountability in organisations but also allows the Responsible Authority to have oversight over data breaches at a national level. 4.14.4 With respect to the criteria for notification, the Responsible Authority will take a riskbased approach and impose a threshold for notification. This is because not all data breaches justify notification, especially where the impact of the data breach is minimal. It is acknowledged that organisations may require time to determine the veracity of suspected breaches. Accordingly, the time frame for notifying the Responsible Authority will thus commence from the time the organisation determines that the breach is eligible for reporting. Unreasonable delays in reporting breaches that cannot be justified will be considered a breach of the Data Breach Notification Obligation.
2	Banking Order 2006		

3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

Obligations of Data Fiduciaries

#	Regulation	external	
		Notification of data processing	registration of database
1	Personal Data Protection	4.8 The Notification Obligation 4.8.1 Under the PDPO framework, the requirement to provide an individual with notice is tied to the Consent Obligation. As part of obtaining valid consent, the organisation must provide the individual with information on: (a) the purposes for the collection, use or disclosure of his personal data, on or before collecting the personal data; and (b) any other purpose for the use or disclosure of personal data that has not been notified to the individual, before such use or disclosure of personal data. 4.8.2 While the PDPO requires that such notice be provided to the individual on or before the collection, use and disclosure of his personal data, there is no prescribed manner or form in which such a notice must be given. This requirement relates to the principle of transparency, specifically, that organisations should be open about the purposes for which personal data is being processed so that individuals are able to make an informed decision as to whether to consent to such processing. 8. Do Not Call ("DNC") Regime 8.1 The PDPO may provide for	

		the establishment of a DNC regime. Individuals may request for their telephone numbers to be added to the DNC Registry if they do not wish to receive telemarketing messages via phone call, text message (i.e. SMS, MMS or any electronic communications sent using a telephone number, e.g. WhatsApp, Telegram) or fax. The DNC Registry will be administered by the Responsible Authority. 8.2 As part of providing individual consumers with some level of control over the number of unsolicited commercial marketing messages received, the Responsible Authority may establish and administer a national DNC Registry for Brunei Darussalam, which would allow individuals to opt-out of marketing messages sent by way of phone call, text message (including Short Messaging Service and Multimedia Messaging Service) or fax. The registration of phone numbers on the DNC Registry will be free-of-charge. 8.3 Generally, organisations in Brunei Darussalam that make marketing calls or send marketing messages by way of text message or fax will be required to check the phone numbers against the DNC Registry and ensure that they do not make calls or send messages to registered numbers, unless an exception or exclusion applies. For example, where the individual had given explicit consent for the company to contact him or her for marketing purposes, or the recipient is in an ongoing relationship with the sender. 8.4 Personal messages, messages from charitable	

		organisations soliciting donations and market research surveys are not considered marketing in nature and it is proposed that the DNC Registry will not block such messages. Marketing messages sent by way of email are not covered under the DNC regime. 8.5 Duty to Check the DNC Register 8.5.1 Under the DNC regime, a sender will have a duty to check the relevant DNC Register and obtain valid confirmation that the receiving Brunei telephone number is not on the DNC Register before sending the specified message to that number. 8.5.2 A sender may obtain valid confirmation from the Responsible Authority that the Brunei telephone number is not listed on the relevant DNC Register. The sender may do so by making an application to the Responsible Authority in receive this confirmation. This application to the Responsible Authority has to be made within the prescribed duration before sending the specified message. 8.6 Role and Responsibility of Checkers 8.6.1 A checker has to ensure information provided is accurate and compliant with requirements under the PDPO. These checkers are persons who, for reward, provide another person (P) with information on whether a Brunei telephone number is listed on the DNC Register for P's compliance with the PDPO. 8.6.2 Checkers must ensure that the information provided to P about whether the Brunei telephone number is listed on the DNC Register is accurate. Checkers must provide such information to P in accordance with any prescribed requirements. 8.6.3	

		Checkers are deemed to have ensured the accuracy of information if it is in accordance with a reply from the Responsible Authority in response to the checker's application for confirmation and this information is provided before the expiry of the prescribed period. 8.7 Sending of a Specified Message 8.7.1 A sender of a specified message must provide its contact information and other prescribed details in the specified message. When sending a specified message to a Brunei telephone number, the sender must include clear and accurate information on: (a) how to identify the sender; (b) how the recipient can readily contact the sender; and (c) other prescribed information (e.g. if the Responsible Authority prescribes further requirements in subsequent regulations). 8.7.2 All the information to be included in the specified message must be reasonably likely to be valid for at least 30 days after the specified message is sent. 8.7.3 In addition, the sender of the specified message must not conceal the calling line identity of the sender or perform any operation, or issue any instruction that would conceal or withhold the calling line identity. 8.8 Clear and Unambiguous Consent 8.8.1 The sender does not need to obtain valid confirmation from the Responsible Authority or checkers of the DNC Registry if the subscriber or user of the Brunei telephone number gives his clear and unambiguous consent to the organisation for the sending of the specified message to that number. This	

		consent from the subscriber or user must be in writing or a form that is accessible for subsequent reference. 8.8.2 With respect to consent, similar rules apply in the context of the sending specified messages. The sender cannot require a subscriber or user of a Brunei telephone number to give consent to the sender to send them a specified message as a condition of contract unless it is reasonable to do so. 8.8.3 Similarly, the sender must not obtain consent to send a subscriber or user of a Brunei telephone number a specified message by providing them false or misleading information or by employing deceptive or misleading practices. Such consent will be deemed to be invalid. 8.8.4 A subscriber or user of a Brunei telephone number can revoke their consent to the sending of a specified message at any time by giving notice to the sender. The sender must stop sending the specified messages to that telephone number after the expiry of the prescribed period. It is proposed that this period be 21 days. 8.9 Prohibition Against Dictionary Attacks and Address-Harvesting Software 8.9.1 An organisation must not send a message to a telephone number that is generated or obtained through a dictionary attack or address-harvesting software. This would be considered an offence under the PDPO. 8.9.2 However, there is a defence for an employee acting in good faith who does so in the course of his employment or in accordance with instructions	

		given to him in the course of his employment will not be liable. 8.9.3 These provisions aim to deter spammers who randomly generate telephone numbers and send marketing messages (including robocalls) to those phone numbers. In many cases, spammers employ the use of dictionary attacks or exploit address harvesting software and other similar technologies to indiscriminately send unsolicited marketing messages to a high volume of recipients, causing consumer annoyance, inconvenience, and, in some cases, distress. 8.10 Enforcement of DNC Provisions 8.10.1 The DNC provisions are enforced under the same administrative regime as the Data Protection Provisions. If the Responsible Authority is satisfied that a person is not in compliance with the DNC provisions, the Responsible Authority may issue any direction to ensure compliance. 8.10.2 If a person is found to have intentionally or negligently contravened any of the DNC provisions, the Responsible Authority may require, by written notice, the organisation or person to pay a financial penalty. (a) For a contravention of the DNC provisions (except the prohibition on use of dictionary attacks and address harvesting software), the financial penalty must not exceed a maximum of B$200,000 in the case of an individual; or B$1 million in any other case. (b) For a contravention of the prohibition on use of dictionary attacks and address harvesting software, the financial penalty must not exceed a maximum of B$200,000 in the case of an	

		individual; in case of a person whose annual turnover in Brunei Darussalam exceeds B$20 million — 5% of the annual turnover of the organisation in Brunei Darussalam; and B$1 million in any other case.	
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation	External	
		Data protection impact assessment	Others
1	Personal Data Protection		
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation		
		technical and organisational measures	Purpose Limitation
1	Personal Data Protection	4.11 The Protection Obligation 4.11.1 Under the PDPO, an organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent: (a)	4.7 The Purpose Limitation Obligation 4.7.1 Under the PDPO framework, an organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable

		unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. 4.11.2 To ensure that organisations are accountable to consumers in relation to the protection of their personal data, the PDPO imposes upon organisations the obligation to make reasonable security arrangements to prevent data breaches. In recent years, there have been several high-profile data breaches internationally, which are usually due to criminal activities like hacking, or organisations failing to impose sufficient or adequate security measures. 4.11.3 The PDPO provides for a reasonable standard for such security measures, and the degree or nature of the measures required may differ depending on factors such as the nature and sensitivity of the data, the form in which the personal data is stored or held, and the impact to the individual if the personal data is subject to unauthorised access, disclosure or other risks.	person would consider appropriate in the circumstances. 4.7.2 In general, organisations must obtain personal data by lawful and fair means and, where appropriate, with the individual's consent. Fresh consent would need to be obtained where personal data collected is to be used for a different purpose from which the individual originally consented. The main objective of the Purpose Limitation Obligation is to ensure that organisations collect, use and disclose personal data that are relevant for the purposes, and only for purposes that are reasonable. This requirement also seeks to prevent over-collection of personal data by organisations.
2	Banking Order 2006	Banking confidentiality. 58. (1) Customer information shall not, in any way, be disclosed by a bank in Brunei Darussalam or any of its officers to any other person except as expressly provided in this Order. (2) A bank in Brunei Darussalam or any of its officers may, for such purpose as may be specified in the first column of the Third Schedule disclose customer information to such persons or class of persons as may be specified in the second column of that Schedule, and in compliance with such conditions	

		as may be specified in the third column of that Schedule. (3) Where customer information is likely to be disclosed in any proceedings referred to in item 3 or 4 of Part I of the Third Schedule, the court may, either of its own motion, or on application of any party to the proceedings or the customer to which the customer information relates – (a) direct that the proceedings be held in camera; and (b) make such other orders as it may consider necessary to ensure the confidentiality of the customer information. (4) Where an order has been made by a court under subsection (3), any person who, contrary to such an order, publishes any information that is likely to lead to the identification of any party to the proceedings is guilty of an offence and liable on conviction to a fine not exceeding $150,000. (5) Any person (including where a person is a body corporate, an officer of the body corporate) who receives customer information referred to in Part II of the Third Schedule shall not, at any time, disclose the customer information or any part thereof to any other person, except as authorised under that Schedule or if required to do so by an order of the court. (6) Any person who contravenes subsection (1) or (5) is guilty of an offence and liable on conviction to fine not exceeding $150,000, imprisonment for a term not exceeding 3 years or both. (7) In this section and in the Third Schedule, unless the context otherwise requires – (a) where disclosure of customer information is authorised under	

		the Third Schedule to be made to any person which is a body corporate, customer information may be disclosed to such officers of the body corporate as may be necessary for the purpose for which the disclosure is authorised under that Schedule; and (b) the obligation of any officer or other person who receives customer information referred to in Part II of the Third Schedule shall continue after the termination or cessation of his appointment, employment, engagement or other capacity or office in which he had received customer information. (8) For the avoidance of doubt, nothing in this section shall be construed to prevent a bank from entering into an express agreement with a customer of that bank for a higher degree of confidentiality than that prescribed in this section and in the Third Schedule. (9) Where, in the course of an inspection under section 53 or an investigation under section 54 or the carrying out of the Authority's function of supervising the financial condition of any bank, the Authority incidentally obtains customer information and such information is not necessary for the supervision or regulation of the bank by the Authority, then, such information shall be treated as confidential by the Authority. (10) This section and the Third Schedule shall also apply, with such modifications as may be prescribed by the Authority, to any licence granted under section 23.	
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015		

	(Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation		
		Accuracy	Retention Limitation
1	Personal Data Protection	4.10 The Accuracy Obligation 4.10.1 Under the PDPO, an organisation must make a reasonable effort to ensure that personal data collected by it is accurate and complete, if it is likely to use such personal data to make a decision that affects the individual concerned, or disclose such personal data to another organisation. 4.10.2 To ensure that decisions relating to the individuals are not made with outdated or otherwise erroneous data, it is important for organisations to ensure, to the extent that is practicable, that the personal data they collect and use is accurate. However, it may be overly onerous for it to be an absolute obligation, hence, organisations are required to make a reasonable effort to ensure that such personal data is reasonably accurate and complete if it is likely such personal data will be disclosed or used to make a decision which affects the individual.	4.12 The Retention Limitation Obligation 4.12.1 Under the PDPO, an organisation must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the retention of such personal data no longer serves the purpose for which it was collected and is no longer necessary for legal or business purposes. 4.12.2 The PDPO seeks to strike a balance between the need for organisations to retain personal data, where there are valid reasons to do so, and the requirement to delete personal data (or render such data anonymous, such that the data is no longer personally identifiable). This obligation recognises that the longer the organization retains the personal data, for instance, in perpetuity, the greater the risks of contravening the other Data Protection Obligations of the PDPO (e.g. that such personal data may be subject to a data breach or other unauthorised disclosure).
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection		

	Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation		
		drawing up of codes of conduct	record of processing activities
1	Personal Data Protection	4.5 The Accountability Obligation 4.5.1 Under the Accountability Obligation in the PDPO, an organisation must appoint a person to be responsible for ensuring that it complies with the PDPO, typically referred to as a data protection officer ("DPO"); and develop and implement policies and practices that are necessary to meet its obligations under the PDPO, including a process to receive complaints. In addition, the organisation is required to communicate to its staff information about such policies and practices and make information available upon request to individuals about such policies and practices. 4.5.2 The Accountability Obligation allows consumers to contact the organisation easily in relation to queries about the organisation's data protection policies and issues related to the organisation's compliance with the PDPO. These aspects of data protection are sometimes referred to as transparency and individual participation. The concept of accountability in relation to personal data protection also relates to the undertaking and demonstration of responsibility for the personal data in the organisation's possession or control. It is one of the key principles highlighted under the APEC Privacy	5.5.5 If no correction to the personal data is made despite a correction request, the organisation shall annotate the personal data record that the correction that was requested but not made.

		Framework and also one of the obligations in the EU GDPR.	
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation	Designation of the data protection officer	Others
1	Personal Data Protection	4.5 The Accountability Obligation 4.5.1 Under the Accountability Obligation in the PDPO, an organisation must appoint a person to be responsible for ensuring that it complies with the PDPO, typically referred to as a data protection officer ("DPO"); and develop and implement policies and practices that are necessary to meet its obligations under the PDPO, including a process to receive complaints. In addition, the organisation is required to communicate to its staff information about such policies and practices and make information available upon request to individuals about such policies and practices. 4.5.2 The Accountability Obligation allows consumers to contact the organisation easily in relation to queries about the organisation's data protection policies and issues related to the organisation's compliance with the PDPO. These aspects of data protection are sometimes referred to as transparency and individual participation. The	

		concept of accountability in relation to personal data protection also relates to the undertaking and demonstration of responsibility for the personal data in the organisation's possession or control. It is one of the key principles highlighted under the APEC Privacy Framework and also one of the obligations in the EU GDPR.	
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

Data Cross Boarder Dist

#	RegulationData Cross Boarder Dist	Cross-border data transfer & Exceptions	Data localization
		Provisions for Transborder Data Transfer. What are the exceptions? (e.g., sufficient authorization, transfers based on contracts equivalent to Standard Contract Clauses (SCC) or Binding Corporate Rules (BCR), transfers based on corporate certification, etc.), Transborder transfer assessment (TIA)	Presence or absence of provisions, stipulations regarding the types of data that must be stored in the country
		Provisions for cross boarder data transfer	Provisions on requirement of localization; and Type of data required for localization
1	Personal Data Protection	4.13 The Transfer Limitation Obligation 4.13.1 Under the Transfer Limitation Obligation, an organisation must not transfer personal data to a country or territory outside Brunei Darussalam except in	

		accordance with requirements prescribed under the PDPO to ensure that the transferred personal data will be accorded a standard of protection that is comparable to that under the PDPO. 4.13.2 The Transfer Limitation Obligation is to maintain the level of trust and confidence of consumers in Brunei Darussalam, especially as cross-border data transfers become more commonplace, e.g. in relation to cloud-based computing. It recognises that other jurisdictions may not necessarily have similar laws to protect the personal data transferred. 4.13.3 In this regard, some jurisdictions (e.g. EU) impose stringent and prescriptive conditions in relation to transfer of personal data outside of its territories. In contrast, the PDPO places the onus on the organisation to ensure that appropriate measures are taken to protect personal data transferred out of Brunei through the imposition of contractual obligations or otherwise.	
2	Banking Order 2006		
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

#	Regulation	Governent Access
		National Security Law, Cybersecurity Law Provisions
		Provision allowed govt to access regulated data/to not comply to data regulation

1	Personal Data Protection	6. Investigations, Enforcement and Appeal 6.1 The PDPO provides for the setting up of a Responsible Authority to administer and enforce the PDPO. 6.2 Powers of Investigation 6.2.1 In the course of its investigations, the Responsible Authority may, upon complaint or of its own motion, conduct an investigation under this section to determine whether or not an organisation or a person is complying with the PDPO. The Responsible Authority's powers of investigation include: (a) requiring, by written notice, an organisation to produce any specified document or specified information; (b) examining orally any person who appears to be acquainted with the facts or circumstances of the matter; (c) by giving at least two working days' advance notice of intended entry, entering into an organisation's premises without a warrant; and (d) obtaining a search warrant to enter an organisation's premises and taking possession of, or remove, any document. 6.3 Penalties for Obstruction 6.3.1 An organisation or person who with an intent to evade an access or correction request disposes of, alters, falsifies, conceals or destroys a record containing personal data or other information; who obstructs or hinders the Responsible Authority or an authorised officer in the exercise of their powers or performance of their duties under the PDPO; or knowingly or recklessly makes a false statement to the Responsible Authority, or knowingly misleads or attempts to mislead the Responsible Authority, commits an offence for which that person would be liable upon conviction to a fine of up to B$10,000 and / or to imprisonment for a term of up to 12 months (in the case of an individual), or a fine of up to B$100,000 (in any other case). 6.3.2 Additionally, any person who neglects or refuses to comply with an order to appear before the Responsible Authority, or without reasonable excuse neglects or refuses to furnish any information or produce any document specified in a written notice to produce information, will be guilty of an offence punishable by a fine not exceeding B$10,000 or to imprisonment for a term not exceeding 12 months, or both. 6.4 Power to Issue Directions 6.4.1 The Responsible Authority will be given powers to issue directions to organisations to take specific steps or corrective measures to address non-compliance with the Data Protection Provisions. Some of these directions for non-compliance include: (a) to stop collecting, using, or disclosing personal data in contravention of the PDPO; (b) to destroy personal data collected in contravention of the PDPO; (c) to provide access to or correct personal data; or (d) if an organisation has intentionally or negligently contravened the Data Protection Provisions, to pay a financial penalty of up to B$1 million or up to 10% of the annual turnover of the organisation in Brunei Darussalam (whichever is higher).

		6.4.2 With regard to the quantum of financial penalty, the Responsible Authority will be guided by the degree of harm caused by the breach, the seriousness of the violation and other factors. The amount must provide sufficient deterrence as well as serve to motivate organisations to put in place appropriate measures to safeguard personal data and comply with the PDPO. 6.5 Reconsideration and Appeal Mechanism 6.5.1 The PDPO provides for the establishment of a Data Protection Appeal Panel ("DPAP"). 6.5.2 An individual or organisation aggrieved by a decision or direction of the Responsible Authority in the exercise of its powers under the PDPO may make a written application to the Responsible Authority to reconsider its direction or decision. Thereafter, any individual or organisation aggrieved by the Responsible Authority's reconsideration decision may lodge an appeal to the DPAP. 6.5.3 Alternatively, an aggrieved individual or organisation may appeal directly to the DPAP without first submitting a reconsideration request. 6.5.4 Where an appeal is lodged with the DPAP, the Chairman of the DPAP shall nominate a Data Protection Appeal Committee ("Appeal Committee") comprising 3 or more members of the DPAP. 6.5.5 The Appeal Committee hearing an appeal may confirm, vary or set aside the direction or decision which is the subject of the appeal and, in particular, may: (i) remit the matter to the Responsible Authority; (ii) impose or revoke, or vary the amount of, a financial penalty; (iii) give any direction, or take any other step, that the Responsible Authority could itself have given or taken; or (iv) make any other direction or decision that the Responsible Authority could itself have made. The direction or decision of the Appeal Committee shall be final. 6.6 Right of Private Action 6.6.1 The PDPO provides for a standalone right of private action. An individual who suffers loss or damage directly as a result of a contravention of certain provisions of the PDPO may also commence a private civil action in court. The court may grant relief by way of injunction, declaration, damages or any other relief as the court thinks fit. 6.6.2 However, if the Responsible Authority has made a decision under the PDPO in respect of a contravention of the PDPO, the right of private action is only exercisable after all avenues of appeal, in respect of the relevant decision issued by the Responsible Authority, have been exhausted.
2	Banking Order 2006	Powers of entry in cases of suspected contraventions. 51. (1) A magistrate may issue a warrant under this section if satisfied on information laid on oath by the Authority or an officer or agent of the Authority that there are reasonable grounds for suspecting that a person is guilty of such a contravention as is mentioned in section 50 and – (a) that person has failed to comply with a notice served on him under that section; (b) that there are reasonable grounds for suspecting the completeness of any information provided or documents produced

		by him in response to such a notice; or (c) that there are reasonable grounds for suspecting that if a notice were served on him under that section it would not be complied with or that any documents to which it would relate would be removed, tampered with or destroyed. (2) A warrant under this section shall authorise any police officer together with any other person named in the warrant and any other police officer – (a) to enter any premises occupied by the person mentioned in subsection (1) which are specified in the warrant, using such force as is reasonably necessary for the purpose; (b) to search the premises and take possession of any documents appearing to be such as are mentioned in paragraph (c) of subsection (1) or to take, in relation to any such documents, any other steps which may appear necessary for preserving them or preventing interference with them; (c) to take copies of or extracts from any such documents; (d) to require any person named in the warrant to answer questions relevant for determining whether that person is guilty of any such contravention as is mentioned in section 50. (3) A warrant under this section shall continue in force until the end of the period of one month beginning with the day on which it is issued. (4) Any documents of which possession is taken under this section may be retained – (a) for a period of 3 months; (b) for such further period as the Magistrate considers fit and proper in the circumstances; or (c) if within that period proceedings to which the documents are relevant are commenced against any person for any such contravention as is mentioned in section 50, until the conclusion of those proceedings. (5) A statement made by a person in compliance with a requirement imposed by virtue of this section may be used in evidence against him. (6) Any person who intentionally obstructs the exercise of any right conferred by a warrant issued under this section or fails without reasonable excuse to comply with any requirement imposed in accordance with paragraph (d) of subsection (2) is guilty of an offence and liable on conviction to a fine not exceeding $100,000, imprisonment for a term not exceeding 2 years or both. Inspection in Brunei Darussalam by parent supervisory authority. 56. (1) In relation to a bank incorporated outside Brunei Darussalam, a parent supervisory authority may, with the prior written approval of the Authority and under conditions of confidentiality, conduct an inspection in Brunei Darussalam of the books, accounts and transactions of any branch or office of that bank in Brunei Darussalam in accordance with this section if the following sections

		are satisfied – (a) the inspection is required by the parent supervisory authority for the sole purpose of carrying out its supervisory functions; (b) the parent supervisory authority has given to the Authority such written undertaking as to the confidentiality of the information obtained, as the Authority may determine; and (c) the parent supervisory authority has given a written undertaking to the Authority to comply with the provisions of this Order and such conditions as the Authority may impose under subsection (2). (2) The Authority may at any time, whether before, on or after giving written approval for an inspection under this section, require the parent supervisory authority to comply with conditions relating to – (a) the classes of information to which the parent supervisory authority shall or shall not have access in the course of the inspection; (b) the conduct of the inspection; (c) the use or disclosure of any information obtained in the course of the inspection; and (d) such other matters as the Authority may determine. (3) Subject to compliance by a parent supervisory authority with such conditions as the Authority may impose under subsection (2), a bank under inspection – (a) shall afford the parent supervisory authority access to such books, accounts, documents and other records, however kept or maintained, of the branch or office of the bank under inspection, and provide such information (including information relating to the bank's internal control systems) and facilities as may be required to conduct the inspection; and (b) shall not be required to afford the parent supervisory authority access to its books, accounts, documents and other records, however kept or maintained, or to provide information or facilities at such times or at such times or at such places as would unduly interfere with the proper conduct of the normal daily business of the bank. (4) A parent supervisory authority may, with the prior written approval of the Authority, appoint another body to conduct the inspection under subsection (1), and in such event the provisions of this section shall apply to the appointed body as they apply to the parent supervisory authority. (5) For the purposes of ensuring the confidentiality of any information obtained in the course of an inspection by a parent supervisory authority under this section, subsection (1) of section 58 shall, with the necessary modifications, apply to any official of the parent supervisory authority as if the official is an officer of a bank. (6) Any bank which refuses or neglects, without reasonable excuse, to afford access to any book, account, document or other record, however kept or maintained, or provide any information or facility as may be required by this section is guilty of an offence and liable on conviction to fine not exceeding $100,000 and, in the case of a continuing offence, to a further fine not exceeding $10,000 for every day during which the offence continues after conviction.

3	Islamic Banking Order, 2008	
4	Data Protection Policy, 2015 (Revised version)	
5	Accountants Order, 2010	
6	Legal Profession Act, 1987, Cap. 132	

Penalties

#	Regulation	Corporate Punishments	Individual Punishments
		Forms of penalties (e.g., recommendations for corrective action, public penalties, fines, confiscation of assets and income, data deletion, data processing, business suspension, etc.)	Penalties (penalties, fines, demotion, etc.)
		Forms of penalties on corporate	Forms of penalties on individual
1	Personal Data Protection	7. Offences Affecting Personal Data and Anonymised Information 7.1 There are specific offences in the PDPO which aims to hold individuals accountable for egregious mishandling of personal data in the possession of or under the control of an organisation. There are 3 main offences which the PDPO addresses. 7.1.1 Knowing or reckless unauthorised disclosure of personal data: If an individual discloses, or causes disclosure of, personal data in the possession or under the control of an organisation or a public agency to another person, which is not authorised, and the individual does so knowingly, or is reckless to the disclosure not being authorised, the individual shall be guilty of an offence. 7.1.2 Improper Use of Personal Data: If an individual makes use of personal data in the possession or under the control of an organisation or a public	7. Offences Affecting Personal Data and Anonymised Information 7.1 There are specific offences in the PDPO which aims to hold individuals accountable for egregious mishandling of personal data in the possession of or under the control of an organisation. There are 3 main offences which the PDPO addresses. 7.1.1 Knowing or reckless unauthorised disclosure of personal data: If an individual discloses, or causes disclosure of, personal data in the possession or under the control of an organisation or a public agency to another person, which is not authorised, and the individual does so knowingly, or is reckless to the disclosure not being authorised, the individual shall be guilty of an offence. 7.1.2 Improper Use of Personal Data: If an individual makes use of personal data in the possession or under the control of an organisation or a public

		agency, which is not authorised, and the individual does so knowingly, or is reckless to the use not being authorised, and as a result of the use of the personal data, the individual (a) obtains a gain, (b) causes harm to another individual, or (c) causes loss to another person, that individual shall be guilty of an offence. 7.1.3 Knowing or reckless unauthorised re-identification of anonymised data: If an individual takes any action to re-identify an affected person or cause the reidentification of anonymised information in the possession or under the control of an organisation or a public agency, which is not authorised, and the individual does so knowingly, or is reckless to the re-identification not being authorised, that individual shall be guilty of an offence. 7.2 For all 3 offences, the penalty is a fine not exceeding B$10,000 or imprisonment for a term not exceeding 2 years, or both. Notwithstanding, the PDPO provides for defences in respect of these offences, for example: 7.2.1 where the information is publicly available (or the information was publicly available solely because of an applicable contravention, and the accused did not know, and was not reckless as to whether, that was the case); 7.2.2 where the conduct is permitted or required under other laws; 7.2.3 where the conduct is authorised or required by an order of the court; 7.2.4 where the individual reasonably believes that he had the legal right to do so; or 7.2.5 in the case of the re-identification of anonymised	agency, which is not authorised, and the individual does so knowingly, or is reckless to the use not being authorised, and as a result of the use of the personal data, the individual (a) obtains a gain, (b) causes harm to another individual, or (c) causes loss to another person, that individual shall be guilty of an offence. 7.1.3 Knowing or reckless unauthorised re-identification of anonymised data: If an individual takes any action to re-identify an affected person or cause the reidentification of anonymised information in the possession or under the control of an organisation or a public agency, which is not authorised, and the individual does so knowingly, or is reckless to the re-identification not being authorised, that individual shall be guilty of an offence. 7.2 For all 3 offences, the penalty is a fine not exceeding B$10,000 or imprisonment for a term not exceeding 2 years, or both. Notwithstanding, the PDPO provides for defences in respect of these offences, for example: 7.2.1 where the information is publicly available (or the information was publicly available solely because of an applicable contravention, and the accused did not know, and was not reckless as to whether, that was the case); 7.2.2 where the conduct is permitted or required under other laws; 7.2.3 where the conduct is authorised or required by an order of the court; 7.2.4 where the individual reasonably believes that he had the legal right to do so; or 7.2.5 in the case of the re-identification of anonymised

		information, the accused reasonably believed that the re-identification was for a specified purpose and notified the Responsible Authority or the organisation or public agency of the re-identification as soon as was practicable. 7.3 The aim of introducing these offences is to reinforce the accountability of individuals who have access to, and process, personal data by punishing the egregious mishandling of personal data (i.e. where the individual acted knowingly or recklessly). 7.4 As a counterbalance, the PDPO also provides for defences to these offences such that employees acting in the course of their employment, or in accordance with instructions of their employer, will be protected from criminal liability. Notwithstanding the above, the organisation is ultimately accountable for compliance with the PDPO and retains liability for the actions of its employees.	information, the accused reasonably believed that the re-identification was for a specified purpose and notified the Responsible Authority or the organisation or public agency of the re-identification as soon as was practicable. 7.3 The aim of introducing these offences is to reinforce the accountability of individuals who have access to, and process, personal data by punishing the egregious mishandling of personal data (i.e. where the individual acted knowingly or recklessly). 7.4 As a counterbalance, the PDPO also provides for defences to these offences such that employees acting in the course of their employment, or in accordance with instructions of their employer, will be protected from criminal liability. Notwithstanding the above, the organisation is ultimately accountable for compliance with the PDPO and retains liability for the actions of its employees.
2	Banking Order 2006	Action by Authority if bank cannot meet its obligations. [S 110/2010] 59. (1) Where a bank – (a) considers that it is likely to become unable to meet its obligations, or that it is insolvent, or about to suspend payments; or (b) becomes unable to meet its obligations, or is insolvent, or suspends payments, it shall forthwith inform the Authority of such fact. (2) Upon receiving such information, and after an inspection or investigation is made under section 49, 50, 51, 52, 53 or 54, the Authority is of the opinion that – (a) the bank is insolvent or is likely to become unable to meet	

		its obligations or is about to suspend payment; (b) the bank has contravened or failed to comply with any of the provisions of this Order; or (c) the bank has contravened or failed to comply with any condition attached to its licence; or (d) the bank has contravened or failed to comply with any condition attached to its licence; or (e) it is in the public interest to do so, the Authority may exercise such one or more of the powers specified in subsection (3) as appears to the Authority to be necessary. (3) The powers referred to in subsection (2) are that the Authority may – (a) require the bank concerned forthwith to take any action or to do or not to do any act or thing whatsoever in relation to its business as the Authority may consider necessary; (b) appoint a person to advise the bank in the proper conduct of its business; or (c) assume control of and carry on the business of the bank or direct some other person to assume control of and carry on the business of the bank. (4) The Authority may, upon representation made to him or on his own motion, modify or cancel any action taken by it under subsection (2), and in so modifying or cancelling any action may impose such conditions as he thinks fit, subject to which the modification or cancellation shall have effect. (5) In this Order, any reference to the Authority having assumed control of or carrying on the business of a bank pursuant to the provision of this section shall	

		be deemed to include a reference to the Authority having directed some other person to assume control of and carry on the business of that bank. Powers of Authority. 60. Where the Authority has taken action under subsection (2) of section 59, it may, without prejudice to the power conferred by paragraph (h) of subsection (1) of section 21 exercise one or more of the following powers, that is to say – (a) confirm, vary or reverse any requirement, appointment or direction made by it; (b) make such order as it may think fit in relation to the affairs of the bank concerned and exercise any power which it may exercise under section 59; (c) present a petition to the High Court for the winding-up of the bank by the High Court Bank under control of Authority. 61. (1) Where the Authority has assumed control of the business of a bank in pursuance of section 59, the bank shall submit its business into the control of the Authority; and shall provide the Authority with such facilities as it may require to carry on the business of the bank. (2) Where the Authority has assumed control of the business of a bank in pursuance of section 59, the Authority shall remain in control of, and continue to carry on the business of, that bank in the name and on behalf of the bank until such time as it is satisfied that – (a) the reasons for which it assumed control of the business have ceased to exist; or (b) it is no longer necessary in the public interest that it should	

		remain in control of the business (3) Where the Authority has assumed control of the business of a bank in pursuance of section 59 or has ceased to control the business of such a bank in pursuance of this section, it shall provide public notification of that fact in the Gazette and such newspaper as the Authority considers appropriate. (4) A bank which fails to comply with subsection (1) or with any requirement of the Authority thereunder is guilty of an offence and liable on conviction to a fine not exceeding $100,000 and, in the case of a continuing offence, to a further fine not exceeding $10,000 every day during which the offence continues after conviction.	
3	Islamic Banking Order, 2008		
4	Data Protection Policy, 2015 (Revised version)		
5	Accountants Order, 2010		
6	Legal Profession Act, 1987, Cap. 132		

B) Cambodia

Legal system overview

#	Regulation	Translation	Purpose of the Legal System
			What purpose does the legal system serve? (e.g. cybersecurity)
		Google translation or Translation by certain organization	
1		Translation by scertain organization	Article 1: Purposes The purposes of this law are as

	E-Commerce Law dated 2 November 2019		follows: 1. To govern electronic commerce in the Kingdom of Cambodia and with the international; 2. To create legal certainty in the civil and commercial transactions by electronic system; 3. To give confidence to the public in the usage of electronic communication.
			Article 2: Goals The goals of this law are as follows: 1. To determine the authenticity, perfection and reliability of an electronic form; 2. To promote the development of legal and business framework in order to conduct safe electronic commerce; 3. To prevent and enforce against acts which are harmful to data and information systems; 4. To eliminate obstacles which hinder electronic commerce and which created by the uncertainty of requirements of written documents and signature; 5. To facilitate electronic filing of documents with public institutions and promote an efficient delivery of services of public institutions through the use of reliable electronic records; and 6. To establish rules, regulations and standards regarding the authenticity and perfection of electronic records.
			Article 3: Scope This law shall apply to all activities, documents and civil and commercial transactions that are made via electronic system except for the activities, documents and transactions relating to: 1. Formation or enforcement of Power of Attorney; 2. Formation or execution of a

			testament, codicil or other matters relating to succession; 3. Any contract for sale, transfer or disposition of rights to immovable property or any interests in such property; 4. Transfer of immovable property or any interests relating to the immovable property; and 5. Any other exceptions as provided for by Sub-Decree.
2	Law on Consumer Protection No 1119_016 dated October 2019	Translation by scertain organization	Article 1: Purpose The purpose of this law is to ensure the protection of consumers and to contribute to the promotion of fair competition.
			Article 2: Objective The objective of this law is to determine the rules and mechanisms in order to contribute to creating a business environment in which: - The rights and interests of consumers are protected; - Businesses are conducted with fair competition; and - Consumers and traders engage with each other with confidence.
			Article 3: Scope This law shall apply to any person who conduct a business, whether for a profit or for non-profit, including the sale of goods or services or real rights over immovable property, to consumers in the Kingdom of Cambodia unless otherwise provided by separate provisions.
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021	Google translation	Article 1 This sub-decree defines the management, use and security of personal data in order to ensure security, order, public interest, improve the quality of services and develop the nation effectively and securely.
			Article 2 This sub-decree applies to the management, use and security of personal identity data in the Kingdom of Cambodia.

4	Law on Banking and Financial Institutions dated November 18, 1999	Translation by scertain organization	Banking and financial services policy and regulation
5	Prakas on Credit Reporting dated June 26 2020	Translation by scertain organization	Article 1.-Purpose The purpose of this Prakas is to establish framework and cooperation for Credit Reporting System (CRS) to enhance responsible and effective lending and fair competition with the aim of reducing credit risk of the Banks and Financial Institutions and promoting financial inclusion in Cambodia.
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007	Translation by scertain organization	Article 1. Purpose The present Law has the purpose to set up measures against money laundering and financing of terrorism as well as the organization and the control of those measures enforcement.
			Article 2. Scope of Application The present Law and other regulations set forth for it implementation are to be used for the prevention and the control of money laundering and financing of terrorism.
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008	Translation by scertain organization	set up measures against money laundering and financing of terrorism as well as the organization and the control of those measures' enforcement.
8	Sub-Decree No. 61 on Physician's Code of Ethics	Translation by scertain organization	Article 1: This Sub-decree aims at determining the provisions on professional ethics for physicians and interned campus medical students who are capable for replacing the active physicians throughout the Kingdom of Cambodia.
9	Sub-Decree on Dental Ethics no 156	Translation by scertain organization	Article 1: This Sub-decree aims at determining the provisions on professional ethics for dentists in the Kingdom of Cambodia.

			Article 2: The objectives of this Sub-decree are to: - Promote ethics of dentists - Uphold honor and dignity for professional dental service practice - Improve Quality and Effectiveness of professional dentists.
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015	Translation by scertain organization	Article 1 The purposes of this Law are: - To ensure the utilization and provision of effective, safe, quality, reliable, and affordable telecommunication infrastructure, networks and services in response to the needs of social and economic development; and - To ensure the development and governance of the telecommunications sector, the regulation of telecommunication operators and persons involved with the telecommunications sector and the lawful and fair competition in order to enhance the mobilization of national revenue and to protect subscribers. - To ensure the protection of users and mobile revenues for National Budget.
			Article 2 The objectives of this Law are to determine: - The authority of the Ministry of Posts and Telecommunications; - The establishment, functions and duties of the Telecommunication Regulator of Cambodia; - The classification and types of permits, certificates and licenses; - The control and utilization of infrastructure and networks; - The national telecommunication numbering plan and electronic address; - The standard, quality of services and telecommunication

			equipment, telecommunication service tariffs and lawful and fair competition; - The universal services obligation, capacity building, research and development; - The rights of telecommunications operators, persons involved with the telecommunications industry and subscribers and 4 /42 - The regulatory fines and criminal offenses in telecommunications sector - Rights of telecommunication operators and legal and fair competitions - Rights of users.
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017	Google translation	Article 1 This sub-decree aims to manage and promote the safe and effective use of digital signatures in the Kingdom of Cambodia.
			Article 2 This sub-decree aims to: - Principles of digital signatures and competent institutions - Provision, modification, suspension, termination and revocation of digital signature licenses - Digital Signature Certificate - Duties of the Digital Signature Authority - Obligations of the owner of the digital signature certificate.
12	Law on Cybercrime Draft V.1	Translation by scertain organization	Article 1: Purpose This law has a purpose to determine education, prevention measures and combat all kinds of offense commit by computer system.
			Article 2: Objective This law has objectives: • Ensure the implementation of law, anti-cybercrime and combating all kinds of offense commit by computer system • Ensure safety and prevent all legitimate interest in using and developing technology

13	The Constitution of the Kingdom of Cambodia 2008	Translation by scertain organization	Cambodian Constitution is the supreme law of the Kingdom of Cambodia, enshrining values such as the rule of law, human rights, democracy and power separation deep into the Kingdom's legal and political system. Its relevance and importance for ordinary Cambodian citizens covers varying aspects, ranging from freedom of religion, expression and access to information to fundamental rights such as labor, economic, women's and social rights as well as the right to education and institutional protection. Furthermore, the Constitution regulates Cambodia's state organization by identifying roles and responsibilities of the country's institutions, the electoral system and political parties.
14	The Civil Code	Translation by scertain organization	This code sets forth the general principles governing legal relations in civil matters. Except where otherwise provided by special law, the provisions of this code shall apply to property related matters and family relations.
15	The Criminal Code 2009 ('the Penal Code')	Translation by scertain organization	Criminal Code of the Kingdom of Cambodia 2009 aims to provide the limitation of the criminal law, what people should and should not do, and other mechanisms pertaining to the criminal procedure.
16	The Code of Civil Procedure 2008	Translation by scertain organization	This Code was created with the purpose to determine the procedure in relation to civil actions as in accordance with the law in order to protect the rights of private parties.

#	Regulation	Form of legal system	Target Business

		Is it introduced in accordance with government ordinances and guidelines? (Is it introduced in a format that ensures lead time?)	Does the law target specific industry or in general? Is it clearly stated in the regulations?
		Regulation level	Industry
1	E-Commerce Law dated 2 November 2019	Law	Commerce
2	Law on Consumer Protection No 1119_016 dated October 2019	Law	General
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021	Sub-decree	General
4	Law on Banking and Financial Institutions dated November 18, 1999	Law	Finance
5	Prakas on Credit Reporting dated June 26 2020	Prakas	Finance
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007	Law	Finance
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008	Prakas	Finance
8	Sub-Decree No. 61 on Physician's Code of Ethics	Sub-decree	Healthcare
9	Sub-Decree on Dental Ethics no 156	Sub-decree	Healthcare
10	Law on Telecommunications (Telecom	Law	Telecommunication

	Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017	Sub-decree	General
12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom of Cambodia 2008	Law	General
14	The Civil Code	Law	General
15	The Criminal Code 2009 ('the Penal Code')	Law	General
16	The Code of Civil Procedure 2008	Law	General

#	Regulation	Regulatory authority	Jurisdiction
		Which regulatory authority has jurisdiction over regulation?	Cyber security, data security, personal information protection, etc.
		Name of ministry/organization	Similar to purpose?
1	E-Commerce Law dated 2 November 2019	Ministry of Commerce	E-Commerce, Data protection
2	Law on Consumer Protection No 1119_016 dated October 2019	Ministry of Commerce	Data security
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021	Article 21 The Minister in charge of the Office of the Council of Ministers, the Minister of the Ministry of Interior, the Minister of Economy and Finance, the ministers of all ministries and the heads of all relevant institutions shall be responsible for the implementation of this sub-decree according to their respective duties from the date of signing.	Personal data
4	Law on Banking and Financial Institutions	Minister of Economy and Finance	Financial service, Financial data security

	dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020	National Bank of Cambodia Article 26.- Roles of the National Bank of Cambodia A. The NBC has the authority to set up any regulations to control and oversee all credit reporting activities, including any relationships with CRSPs or data providers and authorized users regarding the efficiency and fair functioning of the CRS. B. The NBC has authorities to: 1. Issue, suspend and de-license the CRSPs; 2. Monitor the compliance with the rules, regulations, code of conduct, terms, procedures and operating systems; 3. Supervise the adequacy of mechanisms in ensuring continuity of the CRSPs, including the entry and exit requirements and other requirements; 4. Monitor all implementation of resolutions adopted by the advisory council; 5. Require the CRSPs to adopt necessary measures enabling the mandatory participation of all covered entities and authorizèd users, and the voluntary participation of non-covered entities operating in the credit market in credit reporting; 6. Penalize and disciplinary sanction as set forth in the Article 9 of this Prakas on all parties interacting with the CRS, including but not limited to data providers, authorized users and consumers; and 7. Require the CRSPs to provide periodic report and upon request	Data security

6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007	National Bank of Cambodia	Sharing on Data related to anti-money laundering
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008	National Bank of Cambodia	Personal information storing
8	Sub-Decree No. 61 on Physician's Code of Ethics	Minister of Health,	Healthcare data
9	Sub-Decree on Dental Ethics no 156	Ministry of Health	Healthcare data
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015	Minister of Posts and Telecommunication	General regulations on telecommunication. Not about data security
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017	Article 5 The Ministry of Posts and Telecommunications (MPT) is the authority governing digital signatures and provides digital signature certificates to ministries, institutions and national and sub-national authorities. The General Department of Information and Communication Technology (ICT) is a staff of In Management, provision, inspection and monitoring of the implementation of licenses, digital signatures in accordance with this sub-decree and other relevant regulations.	Personal information, Signature
12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom	Constitutional Council	Constitution and rights

	of Cambodia 2008		
14	The Civil Code	Minister of Justice	Constitution and rights
15	The Criminal Code 2009 ('the Penal Code')	Minister of Justice	Constitution and rights
16	The Code of Civil Procedure 2008	Minister of Justice	Constitution and rights, Judiciary and courts

#	Regulation	Status	Citation
		Legislation / Public Comment / Passage / Enforcement / Amendment, etc.	
		Status of the regulation: Draft = drafting (new regulation) published = published in the gazzette but not yet enacted Enact = published in the gazzette and already enacted Amendment = enacted regulation being on amending process	URL
1	E-Commerce Law dated 2 November 2019	Enact	https://data.opendevelopmentcambodia.net/laws_record/law-on-e-commerce
2	Law on Consumer Protection No 1119_016 dated October 2019	Enact	https://s2.moc.gov.kh/mocspace/mocspace_1684120340123.pdf
			https://data.opendevelopmentcambodia.net/laws_record/law-on-consumer-protection
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021	Enact	https://data.opendevelopmentcambodia.net/laws_record/sub-decree-no-252-on-the-management-usage-and-security-protection-of-personal-data
4	Law on Banking and Financial Institutions dated November 18, 1999	Enact	https://data.opendevelopmentcambodia.net/laws_record/law-on-banking-and-financial-institutions
5	Prakas on Credit Reporting	Enact	https://www.nbc.gov.kh/download_files/legislation/prakas_eng/P

	dated June 26 2020		rakas_on_Credit_Reporting_26-06-2020_ENG.pdf
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007	Enact	https://www.nbc.gov.kh/download_files/legislation/laws_eng/91537-Law-on-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-2007.pdf
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008	Enact	https://www.nbc.gov.kh/download_files/legislation/prakas_eng/3356B7-08-089.pdf
8	Sub-Decree No. 61 on Physician's Code of Ethics	Enact	https://data.opendevelopmentcambodia.net/laws_record/sub-decree-on-physicians-code-of-ethics
9	Sub-Decree on Dental Ethics no 156	Enact	https://www.dentalcouncilofcambodia.com/uploads/laws/5.%20Sub-decree%20on%20Dentist%20Code%20of%20Ethics_Eng.pdf
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015	Enact	https://data.opendevelopmentcambodia.net/laws_record/law-on-telecommunications
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017	Enact	https://mptc.gov.kh/laws-regulations/sub-decrees/30229/
12	Law on Cybercrime Draft V.1		—
13	The Constitution of the Kingdom of Cambodia 2008	Enact	https://mptc.gov.kh/en/laws-regulations/laws/13615/
			https://data.opendevelopmentcambodia.net/laws_record/the-constitution-of-united-kingdom-of-cambodia
14	The Civil Code	Enact	https://mptc.gov.kh/en/laws-regulations/laws/13618/
			https://data.opendevelopmentcambodia.net/laws_record/the-civil-code

15	The Criminal Code 2009 ('the Penal Code')	Enact	https://mptc.gov.kh/en/laws-regulations/laws/13617/
			https://data.opendevelopmentcambodia.net/laws_record/criminal-code
16	The Code of Civil Procedure 2008	Enact	https://www.wipo.int/edocs/lexdocs/laws/en/kh/kh032en.pdf

Definition BasicTerm

#	Regulation	Type and Scope of Data	Data processing and handling
		Personal data, personal information/sensitive and important data/children and minors' data, etc. Is the scope of data clearly written in the regulations? What are the unclear points?	Processing, handling / disclosure, sharing, provision, transmission, outsourcing / use for advertising, etc.
1	E-Commerce Law dated 2 November 2019	Annex Definition 9. Data refers to a group of numbers, characters, symbols, message, images, sound, video, information or electronic program which are prepared in a form suitable for use in database or an electronic system.	Annex Definition The key terms used in this law shall be defined as follows: 1. Access means accessing into a computer program, a computer system, a system or an electronic network in order to communicate, transmit, store, or download data, information, or other documents contained in the electronic system by any means.
		Annex Definition 13. Electronic commerce refers to activities involving purchase, sale, rental, exchange of goods or services, including business activities and civil as well as activities and various transactions by the state through electronic system.	Annex Definition 24. Information system refers to a system for generating, sending, receiving, storing or otherwise processing electronic records.
		Annex Definition 15. Electronic communication means information, which is communicated, processed, recorded, displayed, created, stored, received or transmitted by electronic means.	
		Annex Definition	

		17. Electronic evidence means any information, data or documents which are created, stored, sent or received in electronic format or electronic communication for being used to prove facts in legal proceedings, and such information, data or documents shall be authentic in accordance with the e-Commerce Law.	
		Annex Definition 22. Electronic signature means any signatures which are created through electronic means for using to identify the signatory, including digital signature, biometric signature and other signatures.	
2	Law on Consumer Protection No 1119_016 dated October 2019	Article 4 Definition 5. Consumer: refers to a person receiving/obtaining goods or services: A. Which is ordinarily for personal, domestic, or household use; and B. For the purpose of: - not resupplying in conducting a business; or - not consuming/using in the process of a production line or production; or - not utilizing goods for any commercial activity such as repairing a building or to be used as an item attached to immovable property for commercial purposes.	Article 4 Definition 8. Information Disclosure: refers to the disclosure of sufficient and proper information to the public.
		Article 4 Definition 6. Consumer rights refer to: - Right to receive information and education for balancing the difference between the goods or services, and to be protected against fraud and misrepresentation by advertisements; - Right to choose goods or services with fair and competitive prices and quality;	Article 4 Definition 13. Dissemination of information: refers to the making known to general public including the dissemination via the website of the relevant regulators or by other means in which the public may access the information freely and without any obstacle.

		- Right to be heard about concerns and to receive settlements from the competent regulator and the royal government; - Right to demand compensation under this law or by other laws.	
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021	Article 3 The main terms used in this sub-decree are defined as follows: Personal identification data refers to information that can identify an individual. Personal identification data can be data about the name, gender, date of birth, place of birth, current residence, nationality, nationality, as well as biometric data or other data related to the identity of the individual. Personal information refers to a combination of data that can reveal information about a person's private or confidential information.	
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020	Article 3.- Definitions Consent refers to a written or other forms of authorized agreement that allow data providers to upload credit information and dishonored check information into CRS and share with authorized users for permissible purposes provided in this Prakas.	
		Article 3.- Definitions Dishonored check information refers to the information related to issued checks that do not have funds or have insufficient funds for settlement.	
		Article 3.- Definitions Credit Information refers to information related to economic and financial obligations of a consumer, including the payment history, guarantees,	

		publicly available information, and other relevant data for credit approval.	
		Article 3.- Definitions Positive Credit Information refers to consumer's information or data related to loan applications and credit quality such as loan size, maturity, payment's terms and conditions, collaterals, etc.	
		Article 3.- Definitions Negative Credit Information refers to information related to past due or default status of 90 (ninety) days or write-off of loan.	
		Article 3.- Definitions Consumer refers to any legal or natural person whose data/information have been or might have been included in CRS despite a contractual relation with a lender or a lending application signed by consumer or any other legitimate purposes.	
		ANNEX 1 A) IDENTIFICATION DATA OF CONSUMER, GUARANTOR, AND DRAWER Individuals (i) Full name; (ii) Gender; (iii) Date of birth (iv) Residential address; (v) Identification documents (National identity card or Residential book orFamily record book, or Passport); and (vi) Taxpayer identification number. Legal Persons (i) Name of the entity; (ii) Organizational and legal form; (iii) Location; (iv) Number and date of registration as a legal entity (v) Taxpayer identification number;((vi) Full names of its Chief Executive Officer, Directors, and Shareholders; and Executive Officer, Directors	

		(vii) Taxpayer identification number of the Chief and Shareholders. B) CREDIT DATA (i) Date of credit provided and payment of principal and interest as agreed; (ii) Total amount of the loan or other facility granted to the consumer: (iii) Currency (iv) Current outstanding balance (v) Risk category classification of credit by the credit provider (vi) Date of the last payment activity (vii) Type of collateral securing the credit, if any; (viii) Type of credit (mortgage, consumer loan, overdraft etc.); (ix) Creditors name or creditors unique number (x) Dishonored checks (xi) Default credit, arrears balance (xii) Court judgments related to financial obligations; and (xiii) Other information as required by the NBC for banking supervision. In the case of a credit provider sells goods or offers services on a credit form or with delayed payment terms (i) The amount of the goods and services provided on a credit basis; together with contingent and possible obligations;((ii) The dates of services were provided; (iii) The agreed schedule of payment for the services; and (iv) Information on the composition and the types of collateral that secured the payment obligations.	
6	Law on Anti-Money Laundering and Combating the		

	Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017	Article 4 Definition Data refers to text, images, sounds, videos, or other notions that are created, used, and stored on a computer system.	
		Aticle 4 Definition Written letter means a letter in the form of a paper that contains or requires a signature or fingerprint, signature or fingerprint and name, signature or fingerprint and seal, name and stamp, or signature or fingerprint name And seals	
		Article 4 Definition A digital signature certificate refers to a record in a computer system issued by a digital signature authority to verify the identity of the owner of the digital signature certificate, the owner of the digital signature verification key.	
		Article 4 Definition E-mail refers to information that is created, transmitted, received or stored electronically in a computer system.	
		Article 4 Definition Digital signature refers to the	

		data attached to the e-mail to verify the identity of the digital signature and to verify the original status of the e-mail to which the digital signature is signed.	
12	Law on Cybercrime Draft V.1	Article 4 Terms and Definition 4. "computer data" are any representations of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can cause a computer system to perform a function.	
		Article 4 Terms and Definition 5. "Content" refers to electronic form including text, images, graphics, animation, symbols, voices, and video.	
		Article 4 Terms and Definition 7. "traffic data" are any computer data related to a communication by means of a computer system and generated by this, which represent a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, volume and duration, as well as the type of service used for communication.	
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code	Section II. Personal Rights 10. (Concept of personal rights) Personal rights include the rights to life, personal safety, health, freedom, identity, dignity, privacy, and other personal benefits or interests.	
15	The Criminal Code 2009 ('the Penal Code')		
16	The Code of Civil Procedure		

#	Regulation	Data handlers
		Classification/ distinction by responsibility (data processor, data controller)/ size of data, (national security) critical services, etc.

1	E-Commerce Law dated 2 November 2019	Annex Definition 25. Intermediary refers to a person who providing services, sending, receiving, transmitting or storing services, either on a temporary or permanent basis, of the electronic communication or provides other services relating to the electronic communication, including the following persons: 1. A person representing the sender, receiver, transmitter, or the custodian; 2. Telecommunication service providers; 3. Network service providers; 4. Internet service providers; 5. Search engines providers; 6. Online payment service providers; 7. Online auction service providers; 8. Online marketplaces service providers and internet commerce service provider.
		Annex Definition 32. Service provider refers to: (a) A person who provides an information and communication services including sending, receiving, storing or processing the electronic communication or providing of services through other electronic systems; (b) A person who owns, possesses, operates, manages or controls a public switched network or a person who provides telecommunication services; or (c) Any other person who processes or stores data for the use of electronic telecommunication service-oriented or users of such service.
2	Law on Consumer Protection No 1119_016 dated October 2019	
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021	
4	Law on Banking and Financial Institutions dated November 18, 1999	
5	Prakas on Credit Reporting dated June 26 2020	Article 3.- Definitions Authorized Users refers to any person that receives permission authorizing access to the database. It includes designated

		employees of Data Providers, employees of CRSPs, designated employees of the NBC, and other legal person approved by the NBC.
		Article 3.- Definitions Data Providers refers to covered entities and any institutions/other entities received permission from the NBC to provide information to the CRS.
		Article 3.- Definitions Credit Reporting System Service Providers (CRSPs) refers to any entities that conduct credit reporting activities and obtain license from the NBC.
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007	
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008	
8	Sub-Decree No. 61 on Physician's Code of Ethics	
9	Sub-Decree on Dental Ethics no 156	
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015	
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017	
12	Law on Cybercrime Draft V.1	Article 4 Terms and Definition 6. Serivce providers refer to: 1. any natural or legal person offering the users the possibility to communicate by means of a computer system; 2. any other natural or legal person processing or storing computer data for the persons mentioned in paragraph 1 and for the users of the services offered by these;
		Article 4 Terms and Definition 9. "competent authority" refers to the Secretariat of National

		Committee on Anti-Cybercrime or any competent authority in other countries.
13	The Constitution of the Kingdom of Cambodia 2008	
14	The Civil Code	
15	The Criminal Code 2009 ('the Penal Code')	
16	The Code of Civil Procedure	

Legal Basis

#	Regulation		
		consent	necessary for the performance of a contract
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020	Article 9.- Purposes of Credit Reporting Service The credit reporting service will be provided with following purposes: A. Evaluate the creditworthiness and indebtedness of consumer or guarantor when requesting for a loan; B. Support the NBC in	

		supervisory role to monitor credit flow in the financial system, to analyze data for producing financial stability reports, and to supervise banks and financial institutions; C. Evaluate credit risk, and/or review credit. D. Evaluate risks associated with the transaction of default payments or issuing dishonored check; E. Allow consumer or guarantor to confirm the accuracy of his or her information in a credit report; F. Evaluate or audit the efficiency and reliability of the CRS and compliance with any applicable laws and regulations; G. Support KYC including consumer identification pertaining to any activities of identity fraud, criminal, and money laundering and financing terrorism and H. Facilitate the consumer accessing financial service in both local and international. The information contained in the CRS shall not be used for different purposes other than the ones established under this article unless specific consumer's consent is obtained. Article 13.- Consumer Rights CRSPs and relevant parties shall ensure that: A. The rights of consumer, guarantor, and drawer of dishonored check regarding their data usage, distribution, loss, and leakage will be respected. In case of data loss or leakage, consumer, guarantor, and drawer of dishonored check shall be entitled to receipt of such information; B. The CRSPs shall establish a	

		dedicated unit with clear rules and procedures to handle claims and requests from individuals regarding their data: C. No data related to consumer's political tendency, beliefs, color, race, and personal private information will be collected and stored in the CRS: D. Data will be collected for the permissible purposes provided under the Article 9. Data collected or used for different purposes than the ones stated under the Article 9 will need unambiguous consent from consumer, guarantor, and drawer of dishonored check. Article 15.- Other Data Users and Providers 1. Non-covered entities shall contribute data and access data to the CRS once the NBC's permission and prior consumer's consent is obtained; 2. All authorized users and data providers whether regulated by the NB or not, will be subject to the same rules, obligations, and sanctions, as provided in this Prakas; 3. Under the rules of reciprocity, entities that do not report all required information, will not be able to access all information submitted to the CRS by other data providers; 4. The NBC can mandate the participation of new data providers when their activity in Cambodian credit market is perceived to be significant by the NBC	
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007	Article 15. Prohibition of Tipping Off In no circumstance shall persons required to disclose the information and submit reports referred to in Article 13, or any other individual having	

		knowledge thereof, communicate such information or reports to any natural or legal persons other than the Financial Intelligence Unit, except where so authorized by the Financial Intelligence Unit.	
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics	Article 43: Physician shall keep issue a medical record for each patient. The medical record should be kept as confidential document and to be used to record daily all information that are beneficial for diagnosis and treatment. In every case, physician shall be taking care of the records. On request or with the consent of patient, physician shall provide necessary information and documents to other physicians who shall involve or continue to provide treatment to the patient or physician who is going to be selected for further treatment. Article 55: Physician when consult with patient who received previous medical treatment from another colleague shall: - Respect the patient's interest and provide special treatment for urgent situation only, - Respect the rights of the patient for choosing another physician, With the patient's consent, a consulted physician shall report any finding and decisions to the treating physician. In case that the patient refuses, the consulting physician shall inform the patient about consequences that might occur due to the patient's	

		refusal. Article 70: Physician shall keep confidentiality of medical records and information of the patient under his or her medical care or treatment regardless of either the content or benefits of those documents. When physician need to use his or her experience or documents of scientific text in the purpose of publication or education, shall have to protect the patient's identity or otherwise shall seek the patient's consent.	
9	Sub-Decree on Dental Ethics no 156	Article 12: Dentists who are invited to examine or treat the patient who loses freedom, shall not cause or collude to cause harm on the body, mind, or honor of the patient either directly or indirectly. In case the person is ill-treated by any means, the dentists shall inform relevant competent authorities after receiving the consent from the person-himself. Article 42: Dentists shall keep a dental record for each patient. The dental record should be kept as confidential document and to be used to record daily all information that are beneficial for diagnosis and treatment. In every case, dentists shall be responsible in taking care of the records. On request or with the consent of patient, dentists shall provide necessary information and documents to other dentists who shall involve or continue to provide treatment to the patient or dentist who is going to be selected for further treatment. Article 69: Dentist shall keep confidentiality of dental records and information of the patient	

		under his or her dental care or treatment regardless of either the content or benefits of those documents. When dentist needs to use his or her experience or documents in the purpose of scientific promotion or teaching, dentist shall protect the patient's identity or otherwise shall seek the patient's consent.	
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017	Article 12: It is strictly forbidden to share the digital signature creation tips of others. It is prohibited to store or use anyone else's digital signature creation key without the written permission of the digital signature certificate holder.	
12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		
15	The Criminal Code 2009 ('the Penal Code')	Article 301: Listening or Recording Private Speeches The acts of listening or recording the privately announced or confidential speeches without the consent of the concerned person, is punishable, except for the cases where it is authorized by law, by an imprisonment of between 1 (one) month and 1 (one) year and a fine of between 100,000 (one hundred thousand) and 2,000,000 (two million) Riels. If the affected person is informed of the listening or the recording and he did not oppose to it, his consent is therefore presumed	

		Article 302: Infringement on the Right of Private Picture The acts of taking picture of a person in a private place without the consent of the latter, is punishable, except for the cases where it is authorized by law, by an imprisonment of between 1 (one) month and 1 (one) year and a fine of between 100,000 (one hundred thousand) and 2,000,000 (two million) Riels. If the affected person is informed of the picture taking and he/she did not oppose to it, his/her consent is therefore presumed	
16	The Code of Civil Procedure		

#	Regulation		
		necessary for compliance with a legal obligation	necessary in order to protect the vital interests
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999	Article 47 No person who participates in any capacity in the administration, direction management, internal control, or external audit of a covered entity, and no employee of the latter, may provide to any person any confidential information pertaining to statements, facts, acts, figures ot the contents of accounting or administrative	

		documents of which he might have become aware through hus functions. Any person who fails to observe this obligation of professional secrecy shall be liable to the sanctions laid down in Article 55 of this law. However the obligation of professional secrecy may not be used as a ground for nondisclosure vis-s-vis the supervisory authority, auditors, provisional administrators, liquidators, or a court dealing with criminal proceedings.	
5	Prakas on Credit Reporting dated June 26 2020	Article 24.- Confidentiality A. The credit information and dishonored check information is confidential and shall only be used for the permissible purposes set forth in the Article 9 of this Prakas. CRSPs, data providers, and authorized users shall strictly keep credit information or dishonored check information confidentially and shall not sell or otherwise provide such information to any third party. B. Only the NBC, the CRSPs, and the authorized users can access the information and always for the strict performance of their duties. C. The CRSPs shall take all necessary measures to ensure that CRS's directors, management, and employees regularly maintain the confidentiality of credit information and shall take all reasonable measures to prevent unauthorized access to information, and shall establish and enforce security policies and procedures to govern the access to the credit information and dishonored check information. D. The NBC shall have free access to the CRS to obtain	

		credit information for its oversight functions of covered entities, as well as other information pertaining to the non-covered entities to monitor the overall financial stability. E. The NBC shall have access to the CRS in order to fulfill its oversight functions to maintain the efficient, transparent, fair and legal operations of the CRS. F. Directors and employees of CRSPs, authorized users and employees of data providers shall sign confidentiality agreements prior to gaining access to credit information of the CRS.	
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007	Article 6. Banking and Professional Secrecy Banking or professional secrecy shall not inhibit the implementation of the present Law and may not be invoked as a ground for refusal to provide information to the Financial Intelligence Unit and supervisory authority, whether for domestic or for international cooperation purposes, or as required in connection with an investigation which relates to money laundering or financing of terrorism ordered by or carried out under the supervision of a judicial authority. Article 11. Record-keeping by Reporting Entities Reporting entities referred to an Article 4 of the present Law shall maintain, at least for 5 years after the account has been closed or the business relations with the customer have ended, and shall hold at the disposal of the competent authorities any records of customer identification and records of transactions conducted by customers in a manner that they are sufficient to permit the	

		reconstruction of individual transactions, including the amounts and types of currency involved if any, so as to provide, if appropriate, evidence for the prosecution of offense	
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008	Article 22- Record keeping 22.1 Banks and financial institutions should keep all records, documents and copies of documents involved in all forms of transactions for at least 5 years after the date of the transaction. All identification data, files, records, documents, business correspondence and copies of documents obtained on a customer must be maintained for at least 5 years after the accounts have been closed or the business relations with the customer have ended. 22.2 Where the records are subjected to an on-going investigation or suspicious transaction report submitted, they shall be reained beyond the stipulated retention period until it is confirmed by the relevant authority that such records are no longer needed	
8	Sub-Decree No. 61 on Physician's Code of Ethics	Article 12: Physicians must support preventive and educational activities of all relevant competent authorities. Listing, analysis and transmission of information of names either direct or indirect shall be done only within the law permit. Article 44: In any cases, the sustainability of nursing care must be guaranteed. Except in case of emergency and a physician's humanitarian obligation cannot be fulfilled, a physician has the right to refuse to provide medical care due to problem of professionalism or personal reason. If physician refuses this mission, the	Article 56: Physician when invited to immediately consult with patient, if the patient need to receive re-examination by treating physician or by another physician, the consulting physician should write a report about his or her intervention and treatment or send to colleague directly after informing the patient. Consulting physician shall keep a copy of the report. Article 61: When there are more physicians collaborated to provide examination and treatment of patients, those physicians shall share information to each other. Each physician shall assume responsibility individually and

		physician shall inform the patient and send necessary information to the other physician that selected by the patient to continue treatment.	shall keep monitor the development of the patient. Each physician can refuse to participate or discontinue cooperation on condition when the refusal to participate or discontinuity will not cause any harm to the patient and this information must inform all colleagues.
9	Sub-Decree on Dental Ethics no 156		Article 55: Dentist when invited to immediately consult with a patient, if the patient need to receive re-examination by treating dentist or by another dentist, the consulting dentist should write a report about his or her intervention and treatment or send to colleague directly after informing the patient. Consulting dentist shall keep a copy of the report. Article 58: Consulting dentist shall not initiate or re-examine the patient without prior informing the treating dentist except in case of emergencies. Consulting dentist shall not continue to provide dental care when the dental care is under the competency of the treating dentist except that it is the patient's will, then the consulting dentist shall provide all necessary information to the treating dentist for continuing treatment of the patient.
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017	Article 22 In the event that the digital signature license is revoked, the digital signature authority shall notify the owner of the digital signature certificate and shall	

		transfer the digital signature certificate to another digital signature authority in accordance with the proclamation of the PTA. ሸ. ሀ. ፮. The conditions and procedures for the transfer of a digital signature certificate must be determined in case the digital signature license is revoked.	
12	Law on Cybercrime Draft V.1	Article 17: Preservation of Computer Data and Traffic Data 1. In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered. 2. During the criminal investigation, the preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or exofficio, and during the trial, by the court order. 3. The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days. 4. The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions. 5. In case the data referring to the traffic data is under the possession of several service	

		providers, the service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to identify the other service providers in order to know all the elements in the communication chain used. 6. Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved. Article 18: Copying Data 1. Within the term provided for at art. 17 paragraph (3), the prosecutor, on the basis of the motivated authorisation of the prosecutor specially assigned by the general prosecutor of the office related to the Court of Appeal or, as appropriate, by the general prosecutor of the office related to the Supreme Court, or the court orders on 10the seizing of the objects containing computer data, traffic data or data regarding the users, from the person or service provider possessing them, in view of making copies that can serve as evidence. 2. If the objects containing computer data referring to the data for the legal bodies in order to make copies, the prosecutor mentioned in paragraph (1) or court orders the forced seizure. During the trial, the forced seizure order is communicated to the prosecutor, who takes measures to fulfil it, through the criminal investigation body. 3. The copies mentioned in paragraph (1) are achieved by the technical means and the proper procedures to provide the	

		integrity of the information contained by them. Article 19: Searching and Seizing Computer Data 1. Whenever for the purpose of discovering or gathering evidence it is necessary to investigate a computer system or a computer data storage medium, the prosecutor or court can order a search. 2. If the criminal investigation body or the court considers that seizing the objects that contain the data referred to at paragraph (1) would severely affect the activities performed by the persons possessing these objects, it can order performing copies that would serve as evidence and that are achieved according to art. 18, paragraph (3). 3. When, on the occasion of investigating a computer system or a computer data storage medium it is found out that the computer data searched for are included on another computer system or another computer data storage medium and are accessible from the initial system or medium, it can be ordered immediately to authorize performing the search in order to investigate all the computer systems or computer data storage medium searched for Article 20: Condition and Safeguard 1. The access to a computer system, as well as the interception or recording of communications carried out by means of computer systems are performed when useful to find the truth and the facts or identification of the doers cannot be achieved on the basis of other	

		evidence. 2. The measures referred to at paragraph (1) are performed by motivated authorisation of the prosecutor specially assigned by the general prosecutor related to the Court of Appeal or, as appropriate, of the general prosecutor of the office related to the Supreme Court, and for the corruption offences, of the general prosecutor of the National Anti-Corruption Office, by the criminal investigation bodies with the help of specialised persons, who are obliged to keep the confidentiality of the operation performed. 3. The authorisation referred to at paragraph (2) is given for 30 days at the most, with the extension possibility under the same conditions, for duly justified reasons, each extension not exceeding 30 days. The maximum duration of these measures is 4 10months. 4. Until the end of the criminal investigation, the prosecutor is obliged to inform, in writing, the persons against whom the measures referred to in paragraph (1) are taken. 5. The procedures of the Criminal procedure Code regarding the audio or video recordings are applied accordingly	
13	The Constitution of the Kingdom of Cambodia 2008	Article 40: The freedom of citizens to travel near and far and their right to legal settlement shall be respected. Khmer citizens shall have the right to settle abroad or return. The rights to privacy of residence, and to the confidentiality of correspondence by mail, telegram, fax, telex and telephone, shall be guaranteed. Any search of a house, personal	

		property or a person shall be in accordance with the law.	
14	The Civil Code		
15	The Criminal Code 2009 ('the Penal Code')		
16	The Code of Civil Procedure	Article 91 Searches The judicial police officer may conduct a search. In such case, the judicial police officer shall first obtain the authorization from the Royal Prosecutor, which is valid even if the authorization is verbal. The judicial police officer shall conduct a search in the presence of the occupant of the place to be searched. In the absence of such person, the search shall be done in the presence of two witnesses. The witnesses shall be appointed by the judicial police officers. The witnesses shall not be police or military police who are participating in the search operation. Judicial police officers may not conduct a search prior to 6:00 a.m. or after 6:00 p.m., – A search is conducted in cases provided for in Article 86 (Definition of Flagrant Felony or Misdemeanor) of this Code; – A search is conducted in cases provided for in Article 88 (Assimilation of Flagrant Felony or Misdemeanor) of this Code; – There is a call for help from inside a place; – A search is conducted at a place that is open to the public; – A search is conducted at a place where drugs are produced, stored, circulated, distributed or used. Judicial police officers shall establish a written record of the search, which shall include: – The authorization by the Royal Prosecutor, which shall include the date and time of such	Article 83 Confidentiality of Inquiry The inquiry is confidential. Persons who participate in the inquiry, especially Prosecutors, lawyers, court clerks, police and military police officers, civil servants, experts, interpreters/translators, medical doctors and other persons mentioned in Article 95 (Technical or Scientific Examination) of this Code, shall maintain professional confidentiality. However, such professional confidentiality may not be used as an obstacle to the right of self-defense. Moreover, the Royal Prosecutor is entitled to make a declaration in public if he considers that false information in a case has been published. A breach of confidentiality regarding an inquiry is an offense punishable under the Criminal Law in force.

		authorization; – The identity of the occupant or of any witnesses. Judicial police officers may not search the office of a lawyer. Only the Prosecutors or investigating judges who may conduct a search in the office of a lawyer, however only in the presence of the President of the Bar Association, or a delegate of the President of the Bar Association, or together with the lawyer concerned. Judicial police officers may conduct a search of any building of a newspaper, news reporting companies or news broadcasting companies only in the presence of a Prosecutor or an investigating judge who shall guarantee that the search does not affect the freedom of the press and does not improperly delay the news broadcasting or publishing.	

#	Regulation		
		necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	necessary for the purposes of the legitimate interests pursued by the controller or by a third party
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021	Article 6 Authorize the use of personal identification data stored and managed by the Ministry of Interior for the purpose of verifying or verifying or verifying personal identities to serve the public interest, improve the quality of service delivery and national development.	

4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020		
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017		
12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		
15	The Criminal Code 2009 ('the Penal Code')		
16	The Code of Civil Procedure		

#	Regulation		
		opt-out	others
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020		
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom		

	Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017		
12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		
15	The Criminal Code 2009 ('the Penal Code')		
16	The Code of Civil Procedure		

Rights of the data subject

#	Regulation		
		Right to be informed	Right of access
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020		Article 25.- Right over Information A. Consumers shall be entitled to

			request disclosure of any data pertaining to him/her once a year, per copy, and shall sufficiently identify themselves prior to making request. B. CRSPs shall provide report to the consumers within 5 (five) working days from the receipt of request. Report shall include the information of the consumer, name of data provider, and list of data providers within the last 6 (six) months. C. Consumers shall be entitled to request for report more than once a year but shall pay the assigned pricing rate of the CRSPs.
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017		

12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		
15	The Criminal Code 2009 ('the Penal Code')		
16	The Code of Civil Procedure		

#	Regulation	Right to rectification	Right to erasure
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020	D. The consumers shall be entitled to request for correction of any incorrect or incomplete information at any time. E. A detailed consumer rights procedure shall be made available at all data provider's premises and their respective websites or at the CRSPs premises and on their websites	
6	Law on Anti-Money		

	Laundering and Combating the Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017		
12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		
15	The Criminal Code 2009 ('the Penal Code')		
16	The Code of Civil Procedure		

#	Regulation		
		Right to restrict processing	Right to data portability
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No		

	1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020	Article 23.-Credit Reporting Suppression A. Consumer, guarantor, or drawer may request the CRSPs to suppress their credit reporting in case of fraud or identity theft of consumer, guarantor, or drawer. B. Consumer, guarantor, or drawer shall provide tangible evidence to CRSPS when requesting for credit reporting suppression within 5 (five) working days starting from the date of request. C. In case that the request is deemed suitable and sufficient, CRSPs shall notify the consumers, guarantors, or drawers of: 1. Suppression of credit reporting within 30 (thirty) days effective from the notice date. 2. In case that the suppression period is over, consumer, guarantor, or drawer can make extension request for a maximum period of 30 (thirty) days. This extension can be made only once. 3. In case that there is no extension request before the	

		expiration date of suppression or the extension request is refused, CRSPs can resume credit reporting starting from the expiration date of suppression. D. In case that consumer, guarantor, or drawer do not have or could not provide enough evidence to CRSPs within the timeframe provided when making suppression request, credit reporting can be operated as normal. E. If a consumer wishes to apply for credit from covered entities while their credit information is suppressed, they may request the CRSPs in writing to release the credit information to particular covered entities.	
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No		

	246 dated 29 December 2017		
12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		
15	The Criminal Code 2009 ('the Penal Code')		
16	The Code of Civil Procedure		

#	Regulation	Right to object	Right not to be subject to a decision based solely on automated processing
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020		
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007		

7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017		
12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		
15	The Criminal Code 2009 ('the Penal Code')		
16	The Code of Civil Procedure		

#	Regulation		
		Right to withdraw consent	others
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the		

	management, use, and protection of personal identification data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020		
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		Article 65 Subscribers shall have basic rights as follows: a- Rights to receive good quality of telecommunications services and related to information of the service; b- Rights to privacy, security and safety of using the telecommunications service, excepted otherwise determined by other specific law; c- Rights to participate in consultation related to the formulation of policies and regulations concerning the development of

			telecommunications sector; d- Rights to enquire to TRC concerning telecommunications sector; e- Rights to access depute settlement mechanism between subscribers and telecommunications operators, holders of permit or certificate as designated under this Law and other regulations; f- Right to indemnity for damages caused by telecommunications operators and related person in case of the breach of contract; g- Rights to association based on the Constitution and other regulations; and, h- Other rights prescribed by other regulations.
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017		
12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		
15	The Criminal Code 2009 ('the Penal Code')		
16	The Code of Civil Procedure		

Extraterritorial application

#	Regulation		
		applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction	applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction
1	E-Commerce Law dated 2 November 2019		

2	Law on Consumer Protection No 1119_016 dated October 2019	Article 3: Scope This law shall apply to any person who conduct a business, whether for a profit or for non-profit, including the sale of goods or services or real rights over immovable property, to consumers in the Kingdom of Cambodia unless otherwise provided by separate provisions.	
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020		
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156	Article 3: This Sub-decree covers on professional dentists and interned campus dental students who are capable for replacing the active dentists throughout the Kingdom of Cambodia.	

10	Law on Telecommunications (Telecom Law) enacted December 17, 2015	Article 3 This Law shall have the scope of applicability to all telecommunication operations in the Kingdom of Cambodia.	
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017	Article 3 This sub-decree applies to all transactions involving digital signatures in the Kingdom of Cambodia.	
12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		
15	The Criminal Code 2009 ('the Penal Code')		
17	The Code of Civil Procedure		

#	Regulation		
		applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction	applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019	Article 3: Scope This law shall apply to any person who conduct a business, whether for a profit or for non-profit, including the sale of goods or services or real rights over immovable property, to consumers in the Kingdom of Cambodia unless otherwise provided by separate provisions.	
3	Sub-Decree No,252 on the management, use, and protection of personal identification		

	data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020		
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156	Article 3: This Sub-decree covers on professional dentists and interned campus dental students who are capable for replacing the active dentists throughout the Kingdom of Cambodia.	
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015	Article 3 This Law shall have the scope of applicability to all telecommunication operations in the Kingdom of Cambodia.	
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017	Article 3 This sub-decree applies to all transactions involving digital signatures in the Kingdom of Cambodia.	
12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		

15	The Criminal Code 2009 ('the Penal Code')		
17	The Code of Civil Procedure		

#	Regulation		
		no express territorial scope, but would require some nexus to the jurisdiction	other
1	E-Commerce Law dated 2 November 2019	Article 45: Admissibility of Electronic Information from Foreign Countries In order to determine as to whether or not the information in the electronic form is admissible or admissible to a certain degree, it is not necessary to determine the place where such information was produced or used or where the place of business was established overseas as long as such electronic record can accessible and retrievable in the jurisdiction of the Kingdom of Cambodia	
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020		Article 2.- Scope This Prakas is applicable to Credit Reporting Service Providers (CRSPs), Data Providers, Authorized Users, and other Institutions/Companies,

			which obtained approval from the National Bank of Cambodia (NBC).
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017		
12	Law on Cybercrime Draft V.1	Article 3: Scope This law is applicable to all offenses in this law in the following situation: • Offense committed inside Kingdom of Cambodia or • Offense committed inside or outside Kingdom of Cambodia and effect to legal and natural person or interest of Kingdom of Cambodia.	
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		

15	The Criminal Code 2009 ('the Penal Code')		Article 13: Territorial Principles of the Application of Criminal Law As far as criminal acts are concerned, the Cambodian Penal Law is applicable to offences committed in the territory of the Kingdom of Cambodia. The territory of the Kingdom of Cambodia includes the airspace and the sea water territory which are bound to the territory of the Kingdom of Cambodia. Article 18: Application of Cambodian Criminal Law with Regards to the Commission of Acts which Started in Cambodia As far as criminal acts are concerned, the Cambodian Law is applicable to every person who is an instigator or an accomplice in the Cambodian territory of a felony or a misdemeanour committed abroad, if the following two conditions are fulfilled: 1. The offence is punished by the Cambodian law and by the foreign law; 2. The existence of offence has been verified by a final decision of the foreign court
17	The Code of Civil Procedure		

#	Regulation	Representatives of controllers or processors not established in the country
1	E-Commerce Law dated 2 November 2019	
2	Law on Consumer Protection No 1119_016 dated October 2019	
3	Sub-Decree No,252 on the management, use, and	

	protection of personal identification data dated 22 December 2021	
4	Law on Banking and Financial Institutions dated November 18, 1999	
5	Prakas on Credit Reporting dated June 26 2020	
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007	
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008	
8	Sub-Decree No. 61 on Physician's Code of Ethics	
9	Sub-Decree on Dental Ethics no 156	
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015	
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017	
12	Law on Cybercrime Draft V.1	
13	The Constitution of the Kingdom of Cambodia 2008	
14	The Civil Code	

15	The Criminal Code 2009 ('the Penal Code')		
17	The Code of Civil Procedure		

Notification obligation

#	Regulation	Data breach notification to authorities	Data breach notification to affected individuals
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020		Article 13.- Consumer Rights CRSPs and relevant parties shall ensure that: A. The rights of consumer, guarantor, and drawer of dishonored check regarding their data usage, distribution, loss, and leakage will be respected. In case of data loss or leakage, consumer, guarantor, and drawer of dishonored check shall be entitled to receipt of such information; B. The CRSPs shall establish a dedicated unit with clear rules and procedures to handle claims and requests from individuals

			regarding their data: C. No data related to consumer's political tendency, beliefs, color, race, and personal private information will be collected and stored in the CRS: D. Data will be collected for the permissible purposes provided under the Article 9. Data collected or used for different purposes than the ones stated under the Article 9 will need unambiguous consent from consumer, guarantor, and drawer of dishonored check.
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017	Article 28 ... The holder of a digital signature certificate has the following obligations: A. Keep the key to creating a digital signature confidential and secure B. Notify the Digital Signature Authority immediately and to the recipient of the data sent when the digital signature key is stolen	

		or exposed. C- Obligations determined by this sub-decree and other relevant provisions.	
12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		
15	The Criminal Code 2009 ('the Penal Code')		
16	The Code of Civil Procedure		

Obligations of Data Fiduciaries

#	Regulation	external	external
		Notification of data processing	registration of database
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019	Article 23: Information standard for consumers All persons conducting a business in the Kingdom of Cambodia shall disclose the minimum information to consumers in accordance with the information standard to be determined by Prakas of the competent regulators and subject to consultation with the National Committee for Consumer Protection if necessary.	
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		Article 7 Ministries, institutions, organizations in both the public and private sectors, or individuals wishing to use personal identification data, must apply for permission from the Ministry of Interior in accordance with the procedures and legal documents in force. Article 8

			Authorization of Ministries and Institutions in the public sector to use personal identification data to serve the provision of public services shall be made by an inter-ministerial prakas or a joint prakas between the Minister of Interior and the Minister or the head of the institution requesting it. Authorization of private sector entities to use personal identification data to provide public services shall be made by agreement or memorandum of understanding between the representative of the Ministry of Interior and the head or representative of the requested private sector entity. The procedure and procedure for requesting to confirm the identity of the person or confirm the authenticity requested by the person concerned shall be determined by a Prakas of the Minister of the Ministry of Interior. Procedures and procedures for requesting identification or authenticity for use in the field of justice, security, public order shall be determined by a Prakas of the Minister of Interior.
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020	Article 22.- Notification of Consumer Rights A. By way of a consent clause, data providers shall notify the consumer, guarantor, and drawer on any loan application, renewal or extension, or opening check account and purchasing check book of the relevant credit information and dishonored check information being submitted to the CRSPs. The	Article 19.- Access to Credit Reporting System A. All covered entities shall use the CRS to analyze the payment behavior of the consumers and guarantors whenever they receive any new loan application, or renewal or extension of an existing credit facility, regardless of the loan amount. 1. Access to the CRS shall be

		consent clause shall include but not limited to the followings: 1. Name of data provider 2. Credit information or dishonored check information collection purpose 3. Name and address of the CRSPs and 4. Means to access the credit information or dishonored check information if there is a need for correction or modification. B. Covered entities and non-covered entities, when become data providers, shall include notification of consumer rights in the loan application, opening check account application, and other services applications. C. When an adverse action against consumer and guarantor has taken place, as a result of a CRS enquiry, the data provider shall notify the consumer and guarantor accordingly within 5 (five) working days.	restricted to data providers or authorized users under the terms established in the code of conduct or other terms set by the NBC. 2. CRSPs shall establish processes, procedures and rules for determining authorized users to be authorized. B. Other non-regulated data providers shall submit credit information and access the CRS on a voluntary basis, subject to the rules of reciprocity and code of conduct. C. CRSPs shall ensure that the service is secure, stable and usable, and shall ensure that the CRS is fully capable of serving data providers and authorized users. D. CRSPs shall not be responsible for non-authorized access that occurs as a result of the sharing or disclosure access codes or passwords with third parties by any data providers or authorized users. E. All data providers and authorized users shall be subject to the procedures and security measures adopted and contained under the code of conduct.
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		

8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017		
12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		
15	The Criminal Code 2009 ('the Penal Code')		
16	The Code of Civil Procedure		

#	Regulation	external	external
		Data protection impact assessment	Others
1	E-Commerce Law dated 2 November 2019		Article 25: Liability for information or event 1. If an intermediary or an electronic commerce service provider is aware that that the information in an electronic record gives rise to civil or criminal liability, the intermediary or the electronic commerce service provider shall immediately take measure as bellow: a. Remove the information from any information system within the intermediaries or the electronic commerce service providers control and cease to provide services in respect of

			that information; b. Preserve the information as evidence and notify the Ministry of Posts and Telecommunications or relevant competent institutions about the facts and the identity of the suspected person. 2. In the event that an intermediary and an electronic commerce service provider is aware of any facts or circumstances which may lead to the civil or criminal liability, the intermediary and the electronic commerce service provider shall preserve the information evidence and notify the Ministry of Posts and Telecommunications or relevant competent ministriesinstitutions. 3. When it is acknowledged or notified in respect of any information of electronic record which may be subject to civil or criminal liability, the Ministry of Posts and Telecommunications and relevant competent ministries-institutions may give an instruction to the intermediary or electronic commerce service provider to perform any operation as follows: a. Remove the electronic record from the system which is under its control; b. Suspend or cease to provide services to the person; or c. Suspend or cease to provide services in respect of that electronic record. 4. An intermediary or an electronic commerce service provider is not liable on civil liability, whether in contract, outside of contract or in accordance with the law in respect of an activity performed in good faith as directed by the Ministry of Posts and Telecommunications or relevant

			competent ministries-institutions. 5. Any person who lodges a notification of unlawful activity with an intermediary or an electronic commerce service provider bout illegal activity knowing that the notification is false or misleading shall be subject to civil or criminal liability in respect of such offense.
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020		Article 14.- Covered Entities A. All Covered Entities are required to contribute all positive and negative credit information and dishonored check information to the CRS at a minimum of once per month. B. The consent of consumers, guarantors, and drawers of dishonored check shall be obtained for data collection and data access, and such consent shall remain valid for credit extension or review or even top-up until the termination of particular credit operation. The NBC will establish a standard consent form to be used by all covered entities. Covered entities may use other alternative consent forms as long as the

			meaning and content are clear and consistent with the NBC version. C. Data providers obtained permission from the NBC shall prepare procedure, process, and system in accordance with this Prakas within 3 (three) months from the date of permission receipt. D. There will be no discrimination between any data providers, and the CRSPs shall provide service under fair conditions to all participants Article 15.- Other Data Users and Providers 1. Non-covered entities shall contribute data and access data to the CRS once the NBC's permission and prior consumer's consent is obtained; 2. All authorized users and data providers whether regulated by the NB or not, will be subject to the same rules, obligations, and sanctions, as provided in this Prakas; 3. Under the rules of reciprocity, entities that do not report all required information, will not be able to access all information submitted to the CRS by other data providers; 4. The NBC can mandate the participation of new data providers when their activity in Cambodian credit market is perceived to be significant by the NBC Article 23.-Credit Reporting Suppression A. Consumer, guarantor, or drawer may request the CRSPs to suppress their credit reporting in case of fraud or identity theft of consumer, guarantor, or drawer.

			B. Consumer, guarantor, or drawer shall provide tangible evidence to CRSPS when requesting for credit reporting suppression within 5 (five) working days starting from the date of request. C. In case that the request is deemed suitable and sufficient, CRSPs shall notify the consumers, guarantors, or drawers of: 1. Suppression of credit reporting within 30 (thirty) days effective from the notice date. 2. In case that the suppression period is over, consumer, guarantor, or drawer can make extension request for a maximum period of 30 (thirty) days. This extension can be made only once. 3. In case that there is no extension request before the expiration date of suppression or the extension request is refused, CRSPs can resume credit reporting starting from the expiration date of suppression. D. In case that consumer, guarantor, or drawer do not have or could not provide enough evidence to CRSPs within the timeframe provided when making suppression request, credit reporting can be operated as normal. E. If a consumer wishes to apply for credit from covered entities while their credit information is suppressed, they may request the CRSPs in writing to release the credit information to particular covered entities.
6	Law on Anti-Money Laundering and		

	Combating the Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017		
12			
13	Law on Cybercrime Draft V.1		
14	The Constitution of the Kingdom of Cambodia 2008		
15	The Civil Code		
16	The Criminal Code 2009 ('the Penal Code')		
17	The Code of Civil Procedure		

#	Regulation	internal	internal
		technical and organisational measures	Purpose Limitation
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No		

	1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021	Article 4 The Ministry of Interior has the authority to collect, compile, store, manage and secure the identity data of individuals obtained from civil registration, identity card, Khmer nationality, statistics and residence management, passports, nationals and other registrations which are legal and regulatory documents. Yut handed over to the Ministry of Interior. The Ministry of Interior, which owns the original data, may authorize ministries, institutions, entities in both the public and private sectors or individuals to use the identity data in accordance with the procedures and procedures set forth in this sub-decree and other legal documents in force. Article 13 The Ministry of Interior shall protect the identity data of individuals under its control against risks and dangers such as data destruction, data loss or loss, data deletion, data correction or unauthorized access or disclosure of data. Public data. The Ministry of Interior shall establish a backup data storage system in a safe place other than the one where the original database is stored and properly maintained. Article 14: The Ministry of Interior, which owns the original data, and the ministries, institutions, entities, both public and private sectors that use the data, must ensure the protection of data security both during transmission and use, in accordance with high security technical requirements.	Article 11 Ministries, institutions, entities, both public and private, requesting the use of personally identifiable data must ensure that used data is not stored in its system and does not continue to share data with other parties or use data for purposes other than The request will not affect the security of public order.

		Article 15 ... Ministries, institutions, organizations, both public and private, which are data users, must ensure the security of data after use, in accordance with the highest technical safety standards. All data used or transmitted is still the data of the Ministry of Interior, regardless of the Ministry, institution, entity, both public and private sectors use that data in any form.	
4	Law on Banking and Financial Institutions dated November 18, 1999	Article 43. Under conditions prescribed by the supervisory authority, a covered entity must have an internal control system aiming particularly at: verifving that the operations carried out by a covered entity, as well as the organization and internal procedures, comply with the laws and regulations in force, professional and ethical standards and practices, and the policy of the executive body, 2. verifving that the limits laid down for risks. in particular counterparty, exchange-rate, interest-rate and other market risks, are strictly observed. 3. monitoring the quality of accounting and financial information, in particular the arrangements whereby this information is recorded, preserved, made available, and disclosed internally and externally	
5	Prakas on Credit Reporting dated June 26 2020	Article 10.- Obligations of Relevant Parties to Ensure Data Quality Credit Reporting System Service Providers (CRSPs) and data providers shall make all reasonable effort to ensure that the consumers' information collected, used, and disclosed is accurate, complete, and up-to date. The data shall be collected	Article 13.- Consumer Rights CRSPs and relevant parties shall ensure that: A. The rights of consumer, guarantor, and drawer of dishonored check regarding their data usage, distribution, loss, and leakage will be respected. In case of data loss or leakage, consumer, guarantor, and

		by fair and lawful means and shall include only necessary information such as valid identification, credit payment behavior, and dishonored check information. CRSPs and data providers shall be accountable for the followings: A. CRSPs shall: 1. Establish adequate procedures to ensure completeness and veracity of the information; 2. Ensure that data is updated regularly according to the code of conduct; 3. Establish adequate mechanisms for data correction and deletion ensuring that all users accessing incorrect data during the previous 3 (three) months are sufficiently informed and notified of the error and data correction according to the time frame as set out in the code of conduct and establish adequate mechanisms to ensure that all users that have access to the data in the previous3 (three) months are aware of such error and receive the correct information, and that a copy is also sent to the consumer; 4. Be accountable for any data errors to data providers, authorized users and consumers that have occurred during the processing or dissemination of credit information as a result of gross negligence or reckless behavior. CRSPs shall: a. Correct data promptly and establish adequate mechanisms to ensure that all users have access to data in the previous 3 (three) months are aware of such error and receive the correct information after being updated; b. Receive a copy of the updated report and provide the report to	drawer of dishonored check shall be entitled to receipt of such information; B. The CRSPs shall establish a dedicated unit with clear rules and procedures to handle claims and requests from individuals regarding their data: C. No data related to consumer's political tendency, beliefs, color, race, and personal private information will be collected and stored in the CRS: D. Data will be collected for the permissible purposes provided under the Article 9. Data collected or used for different purposes than the ones stated under the Article 9 will need unambiguous consent from consumer, guarantor, and drawer of dishonored check.

		consumer; c. Be responsible for any claims from the consumer that may result in a substantial damage of consumer's financial reputation because of gross negligence or reckless behavior; d. Make all reasonable efforts to mitigate damages which have effect on the consumer due to data errors. 5. Be responsible to data providers, authorized users, the NBC, or third party for any claims pertaining to delay, interruption or failing to provide credit information or statistical report, unless they are resulting from governmental orders, sabotages, riots, vandalism, internet service provider denial, or any other causes that are beyond the CRS's reasonable control; 6. Must not transfer, sell or rent any credit information submitted by data providers or authorized users, except as authorized under this Prakas; 7. Cross-border credit information can only be shared under a cooperation framework with prior consent from the NBC and shall take the following considerations: a. Consumer's privacy protection b. Conflict resolution and data correction c. Data security protection and d. Prior consent from the consumer. B. Data providers shall be responsible for: 1. Any incorrect information sent to CRSPs; 2. Any claims from the consumers regarding errors that are material to a substantial	

		damage of customer's financial reputation, as a consequence of gross negligence or reckless behavior in compliance with the decision made under the conflict resolution mechanisms provided in Article 28 of this Prakas and 3. Mitigating damages suffered by consumer for data errors by establishing all necessary policies and procedures. The credit information and other services provided by the CRSPs shall be considered as one of the tools for credit risk decision process, but the decision shall not be made solely based on the credit information obtained from the CRSPs. Each data provider shall have its own loan approval rules. Article 11.- Data Security CRSPs and data providers shall ensure the security and integrity of the database at all times. To prevent misuse or unauthorized access, data loss, or data corruption, all necessary steps must follow the following rules: A. CRSPs shall have systems, processes and procedures to ensure data recovery and disaster recovery plans to prevent data loss or data corruption; such as: 1. Access to the database will be restricted to authorized users; 2. Establish adequate mechanisms to ensure that data will be used only for permissible purposes or other lawful purposes with consumer's consent according to Article 9 of this Prakas. B. Data providers shall ensure the availability of adequate	

		procedures, policies and security measures. Policy and security measures for the operation of the CRS shall be approved by the Board of Directors of the CRSPs. The measures adopted should be reflected from a technical, organizational structure and technological view. C. In the event of any data loss or breach, the CRSPs or data provider is obliged to take measures to prevent such events and notify the NBC immediately Article 18.- Collection and Distribution A. CRSPs will collect, process, and store credit information and dishonored check information obtained from the data providers and other data sources according to the best possible knowledge, including operational guidelines to protect data from misuse, unauthorized access, loss, or system failure. CRSPs will introduce quality control procedures to ensure the continuity of the service. B. Data providers shall submit their complete loan portfolios and dishonored check information according to the layout and format established by the CRSPs in9agreement with the Advisory Council. The initial format will follow the layout indicated in ANNEX 1 (file layout). The format will include two parts, which first part containing identifiable information of the consumer, guarantor and drawer of the dishonored check and second part containing data of credit transaction and dishonored check. C. Data providers shall provide the first file within 90 (ninety) days, beginning from being notified the commencement	

		date. 1. The CRSPs shall load all relevant data that complies with the file layout received from the data providers within a period of 5 (five) working days since the receipt of data. 2. All data providers shall provide a complete update of their credit information and dishonored check information every month, no later than the fifth day of next month. 3. The file shall be provided in the format established by the Board of Directors and approved by the Advisory Council. D. CRSPs shall be responsible for the CRS database and shall provide the credit information services to covered entities, data providers and other authorized users under this Prakas, the code of conduct, or any applicable regulations of the NBC. E. CRSPs shall be responsible for data leakage as of a result of system failure or data misuse by its employees. F. Credit information and dishonored check information must not be sold or disclosed by any of the covered entities, data providers, or any users to a third party. Covered entities, data providers, or authorized users, shall not use the information obtained from the CRS to provide services to third parties or to conduct marketing campaigns, other than their existing customers. G. CRSPs may modify the terms and conditions of the service to guarantee or improve the performance of the service.	

		CRSPs shall send a notice to the data providers within 60 (sixty) days before the new conditions come into effect. Article 19.- Access to Credit Reporting System A. All covered entities shall use the CRS to analyze the payment behavior of the consumers and guarantors whenever they receive any new loan application, or renewal or extension of an existing credit facility, regardless of the loan amount. 1. Access to the CRS shall be restricted to data providers or authorized users under the terms established in the code of conduct or other terms set by the NBC. 2. CRSPs shall establish processes, procedures and rules for determining authorized users to be authorized. B. Other non-regulated data providers shall submit credit information and access the CRS on a voluntary basis, subject to the rules of reciprocity and code of conduct. C. CRSPs shall ensure that the service is secure, stable and usable, and shall ensure that the CRS is fully capable of serving data providers and authorized users. D. CRSPs shall not be responsible for non-authorized access that occurs as a result of the sharing or disclosure access codes or passwords with third parties by any data providers or authorized users. E. All data providers and authorized users shall be subject	

		to the procedures and security measures adopted and contained under the code of conduct. Article 24.- Confidentiality A. The credit information and dishonored check information is confidential and shall only be used for the permissible purposes set forth in the Article 9 of this Prakas. CRSPs, data providers, and authorized users shall strictly keep credit information or dishonored check information confidentially and shall not sell or otherwise provide such information to any third party. B. Only the NBC, the CRSPs, and the authorized users can access the information and always for the strict performance of their duties. C. The CRSPs shall take all necessary measures to ensure that CRS's directors, management, and employees regularly maintain the confidentiality of credit information and shall take all reasonable measures to prevent unauthorized access to information, and shall establish and enforce security policies and procedures to govern the access to the credit information and dishonored check information. D. The NBC shall have free access to the CRS to obtain credit information for its oversight functions of covered entities, as well as other information pertaining to the non-covered entities to monitor the overall financial stability. E. The NBC shall have access to the CRS in order to fulfill its oversight functions to maintain the efficient, transparent, fair and legal operations of the CRS. F. Directors and employees of CRSPs, authorized users and	

		employees of data providers shall sign confidentiality agreements prior to gaining access to credit information of the CRS.	
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007	Article 23. Obligation of Confidentiality The Financial Intelligence Unit Board and its permanent secretariat shall be required to keep confidential any information obtained within the scope of their duties, even after the cessation of those duties within the FIU. Such information may not be used for any purposes other than those provided for by the present Law	
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008	Article 24 - Record Format Banks and financial institutions should retain the relevant document as originals or copies, on microfilm or in electronic form, provided that such forms are secured and retrievable upon request and provided in an accurate and timely manner	
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017	Article 27 The digital signature authority has the following obligations: A. Protect and maintain security related to the issuance of digital signature certificates and the use of digital signatures in accordance with the provisions of the PTA. And other relevant provisions B. B- Do not keep the key to create the digital signature of the digital signature certificate	

		holder unless there is written consent. C. C- Do not use or disseminate the digital signature creation key of the digital signature certificate holder. D. D- Confidentiality of the digital signature of the owner of the digital signature certificate E. E- Keep the key to creating digital signatures confidentially and securely F. F. Maintain and manage secure digital signature certification records within 10 years after the expiration of the digital signature certificate G. G. Report immediately to the AEC. In the event of a malfunction of the data processing system or equipment, methods and authorization system within 24 (twenty-four) hours H. Provide the digital signature certificate holder with a device or means that allows the notification of theft, loss or disclosure of digital signature creation keys. I. Provide financial statements and non-financial information on a regular basis or at the request of the ECCC. J. Obligations determined by this sub-decree and other relevant provisions.	
12			
13	Law on Cybercrime Draft V.1		
14	The Constitution of the Kingdom of Cambodia 2008		
15	The Civil Code		
16	The Criminal Code 2009 ('the Penal Code')		
17	The Code of Civil Procedure		

#	Regulation	internal	internal
		Accuracy	Retention Limitation
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021	Article 10 ... The Ministry of Interior, which owns the original data, must ensure that all personal identification data is accurate, which can serve as a basis for official verification and use. In case of any correction of the identity data as stated in article 5 of this sub-decree, the Ministry of Interior shall update the data in its management system in accordance with the procedures and procedures in force.	
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020	Article 10.- Obligations of Relevant Parties to Ensure Data Quality Credit Reporting System Service Providers (CRSPs) and data providers shall make all reasonable effort to ensure that the consumers' information collected, used, and disclosed is accurate, complete, and up-to date. The data shall be collected by fair and lawful means and shall include only necessary information such as valid identification, credit payment behavior, and dishonored check information. CRSPs and data providers shall be accountable for the followings: A. CRSPs shall: 1. Establish adequate	Article12.- Data Retention Period A. Information collected by CRS will be maintained and disseminated among data providers for a period of 10 (ten) years from the payment or settlement deadline in case of positive information; B. CRSPs shall disclose the data as follows: 1) Positive information will be disclosed for a period of 10 (ten) years from the maturity date; 2) Negative information will be disclosed for a period of 3 (three) years from the maturity date; 3) Dishonored check information will be disclosed for a period of 2 (two) years from the date the dishonored check is returned to the institution;

		procedures to ensure completeness and veracity of the information; 2. Ensure that data is updated regularly according to the code of conduct; 3. Establish adequate mechanisms for data correction and deletion ensuring that all users accessing incorrect data during the previous 3 (three) months are sufficiently informed and notified of the error and data correction according to the time frame as set out in the code of conduct and establish adequate mechanisms to ensure that all users that have access to the data in the previous3 (three) months are aware of such error and receive the correct information, and that a copy is also sent to the consumer; 4. Be accountable for any data errors to data providers, authorized users and consumers that have occurred during the processing or dissemination of credit information as a result of gross negligence or reckless behavior. CRSPs shall: a. Correct data promptly and establish adequate mechanisms to ensure that all users have access to data in the previous 3 (three) months are aware of such error and receive the correct information after being updated; b. Receive a copy of the updated report and provide the report to consumer; c. Be responsible for any claims from the consumer that may result in a substantial damage of consumer's financial reputation because of gross negligence or reckless behavior; d. Make all reasonable efforts to mitigate damages which have effect on the consumer due to data errors.	4) Data on bankruptcy and liquidation of a legal entity will be disclosed for a period of 5 (five) years from the date of discharge: D. CRSPs shall archive data for a minimum period of 15 (fifteen) years.

		5. Be responsible to data providers, authorized users, the NBC, or third party for any claims pertaining to delay, interruption or failing to provide credit information or statistical report, unless they are resulting from governmental orders, sabotages, riots, vandalism, internet service provider denial, or any other causes that are beyond the CRS's reasonable control; 6. Must not transfer, sell or rent any credit information submitted by data providers or authorized users, except as authorized under this Prakas; 7. Cross-border credit information can only be shared under a cooperation framework with prior consent from the NBC and shall take the following considerations: a. Consumer's privacy protection b. Conflict resolution and data correction c. Data security protection and d. Prior consent from the consumer. B. Data providers shall be responsible for: 1. Any incorrect information sent to CRSPs; 2. Any claims from the consumers regarding errors that are material to a substantial damage of customer's financial reputation, as a consequence of gross negligence or reckless behavior in compliance with the decision made under the conflict resolution mechanisms provided in Article 28 of this Prakas and 3. Mitigating damages suffered by consumer for data errors by establishing all necessary policies and procedures.	

		The credit information and other services provided by the CRSPs shall be considered as one of the tools for credit risk decision process, but the decision shall not be made solely based on the credit information obtained from the CRSPs. Each data provider shall have its own loan approval rules. Article 28.- Conflict Resolution Mechanism A. Covered entities, non-covered entities, consumers, guarantors, and drawers shall submit any complaints regarding the accuracy of the credit information or dishonored check information to CRSPs for investigation. B. Once a complaint is received, CRSPs shall investigate the conflict and respond to the complainant within 15 (fifteen) working days from the receipt of complaint: 1. Any complaints related to accuracy or completeness of credit information or dishonored check information, CRSPs shall notify data providers within 5 (five) working days. Data providers shall review and correct the credit information or dishonored check information within 5 (five) working days upon receipt of otification. 2. CRSPs shall notify the complainant within 5 (five) working days upon receipt full response from data providers of the decision of complaint. C. Any complainant that is dissatisfied with the decision may appeal to the NBC within 10 (ten) working days upon receipt of decision.	

		D. If the complainant is not satisfied with the NBC's decision, further appeal may be made to the court	
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007		Article 11. Record-keeping by Reporting Entities Reporting entities referred to at Article 4 of the present Law shall maintain, at least for 5 years after the account has been closed or the business relations with the customer have ended, and shall hold at the disposal of the competent authorities any records of customer identification and records of transactions conducted by customers in a manner that they are sufficient to permit the reconstruction of individual transactions, including the amounts and types of currency involved if any, so as to provide, if appropriate, evidence for the prosecution of offense
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008	Article 24 - Record Format Banks and financial institutions should retain the relevant document as originals or copies, on microfilm or in electronic form, provided that such forms are secured and retrievable upon request and provided in an accurate and timely manner	Article 22- Record keeping 22.1 Banks and financial institutions should keep all records, documents and copies of documents involved in all forms of transactions for at least 5 years after the date of the transaction. All identification data, files, records, documents, business correspondence and copies of documents obtained on a customer must be maintained for at least 5 years after the accounts have been closed or the business relations with the customer have ended. 22.2 Where the records are subjected to an on-going investigation or suspicious transaction report submitted, they shall be reained beyond the stipulated retention period until it is confirmed by the relevant authority that such records are no longer needed

8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017		Article 27 The digital signature authority has the following obligations: A. Protect and maintain security related to the issuance of digital signature certificates and the use of digital signatures in accordance with the provisions of the PTA. And other relevant provisions B. B- Do not keep the key to create the digital signature of the digital signature certificate holder unless there is written consent. C. C- Do not use or disseminate the digital signature creation key of the digital signature certificate holder. D. D- Confidentiality of the digital signature of the owner of the digital signature certificate E. E- Keep the key to creating digital signatures confidentially and securely F. F. Maintain and manage secure digital signature certification records within 10 years after the expiration of the digital signature certificate G. G. Report immediately to the AEC. In the event of a malfunction of the data processing system or equipment, methods and authorization system within 24 (twenty-four) hours H. Provide the digital signature certificate holder with a device or means that allows the

			notification of theft, loss or disclosure of digital signature creation keys. I. Provide financial statements and non-financial information on a regular basis or at the request of the ECCC. J. Obligations determined by this sub-decree and other relevant provisions.
12			
13	Law on Cybercrime Draft V.1		
14	The Constitution of the Kingdom of Cambodia 2008		
15	The Civil Code		
16	The Criminal Code 2009 ('the Penal Code')		
17	The Code of Civil Procedure		

#	Regulation	internal	internal
		drawing up of codes of conduct	record of processing activities
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020	Article 10.- Obligations of Relevant Parties to Ensure Data Quality	

		Credit Reporting System Service Providers (CRSPs) and data providers shall make all reasonable effort to ensure that the consumers' information collected, used, and disclosed is accurate, complete, and up-to date. The data shall be collected by fair and lawful means and shall include only necessary information such as valid identification, credit payment behavior, and dishonored check information. CRSPs and data providers shall be accountable for the followings: A. CRSPs shall: 1. Establish adequate procedures to ensure completeness and veracity of the information; 2. Ensure that data is updated regularly according to the code of conduct; 3. Establish adequate mechanisms for data correction and deletion ensuring that all users accessing incorrect data during the previous 3 (three) months are sufficiently informed and notified of the error and data correction according to the time frame as set out in the code of conduct and establish adequate mechanisms to ensure that all users that have access to the data in the previous3 (three) months are aware of such error and receive the correct information, and that a copy is also sent to the consumer; 4. Be accountable for any data errors to data providers, authorized users and consumers that have occurred during the processing or dissemination of credit information as a result of gross negligence or reckless behavior. CRSPs shall: a. Correct data promptly and	

		establish adequate mechanisms to ensure that all users have access to data in the previous 3 (three) months are aware of such error and receive the correct information after being updated; b. Receive a copy of the updated report and provide the report to consumer; c. Be responsible for any claims from the consumer that may result in a substantial damage of consumer's financial reputation because of gross negligence or reckless behavior; d. Make all reasonable efforts to mitigate damages which have effect on the consumer due to data errors. 5. Be responsible to data providers, authorized users, the NBC, or third party for any claims pertaining to delay, interruption or failing to provide credit information or statistical report, unless they are resulting from governmental orders, sabotages, riots, vandalism, internet service provider denial, or any other causes that are beyond the CRS's reasonable control; 6. Must not transfer, sell or rent any credit information submitted by data providers or authorized users, except as authorized under this Prakas; 7. Cross-border credit information can only be shared under a cooperation framework with prior consent from the NBC and shall take the following considerations: a. Consumer's privacy protection b. Conflict resolution and data correction c. Data security protection and d. Prior consent from the consumer.	

		B. Data providers shall be responsible for: 1. Any incorrect information sent to CRSPs; 2. Any claims from the consumers regarding errors that are material to a substantial damage of customer's financial reputation, as a consequence of gross negligence or reckless behavior in compliance with the decision made under the conflict resolution mechanisms provided in Article 28 of this Prakas and 3. Mitigating damages suffered by consumer for data errors by establishing all necessary policies and procedures. The credit information and other services provided by the CRSPs shall be considered as one of the tools for credit risk decision process, but the decision shall not be made solely based on the credit information obtained from the CRSPs. Each data provider shall have its own loan approval rules. Article 24.- Confidentiality A. The credit information and dishonored check information is confidential and shall only be used for the permissible purposes set forth in the Article 9 of this Prakas. CRSPs, data providers, and authorized users shall strictly keep credit information or dishonored check information confidentially and shall not sell or otherwise provide such information to any third party. B. Only the NBC, the CRSPs, and the authorized users can access the information and always for the strict performance of their duties. C. The CRSPs shall take all necessary measures to ensure	

		that CRS's directors, management, and employees regularly maintain the confidentiality of credit information and shall take all reasonable measures to prevent unauthorized access to information, and shall establish and enforce security policies and procedures to govern the access to the credit information and dishonored check information. D. The NBC shall have free access to the CRS to obtain credit information for its oversight functions of covered entities, as well as other information pertaining to the non-covered entities to monitor the overall financial stability. E. The NBC shall have access to the CRS in order to fulfill its oversight functions to maintain the efficient, transparent, fair and legal operations of the CRS. F. Directors and employees of CRSPs, authorized users and employees of data providers shall sign confidentiality agreements prior to gaining access to credit information of the CRS.	
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		

10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017		
12			
13	Law on Cybercrime Draft V.1		
14	The Constitution of the Kingdom of Cambodia 2008		
15	The Civil Code		
16	The Criminal Code 2009 ('the Penal Code')		
17	The Code of Civil Procedure		

#	Regulation	Internal	Internal
		Designation of the data protection officer	Others
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		

4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020		
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007		
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017		
12			
13	Law on Cybercrime Draft V.1		
14	The Constitution of the Kingdom of Cambodia 2008		
15	The Civil Code		
16	The Criminal Code 2009 ('the Penal Code')		
17	The Code of Civil Procedure		

Data Cross Boarder Dist

#	Regulation	Cross-border data transfer & Exceptions	Data localization
		Provisions for Transborder Data Transfer. What are the exceptions? (e.g., sufficient authorization, transfers based on contracts equivalent to Standard Contract Clauses (SCC) or Binding Corporate Rules (BCR), transfers based on corporate certification, etc.), Transborder transfer assessment (TIA)	Presence or absence of provisions, stipulations regarding the types of data that must be stored in the country
1	E-Commerce Law dated 2 November 2019		
2	Law on Consumer Protection No 1119_016 dated October 2019		
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		
4	Law on Banking and Financial Institutions dated November 18, 1999		
5	Prakas on Credit Reporting dated June 26 2020	Article 10.- Obligations of Relevant Parties to Ensure Data Quality Credit Reporting System Service Providers (CRSPs) and data providers shall make all reasonable effort to ensure that the consumers' information collected, used, and disclosed is accurate, complete, and up-to date. The data shall be collected by fair and lawful means and shall include only necessary	

		information such as valid identification, credit payment behavior, and dishonored check information. CRSPs and data providers shall be accountable for the followings: A. CRSPs shall: 1. Establish adequate procedures to ensure completeness and veracity of the information; 2. Ensure that data is updated regularly according to the code of conduct; 3. Establish adequate mechanisms for data correction and deletion ensuring that all users accessing incorrect data during the previous 3 (three) months are sufficiently informed and notified of the error and data correction according to the time frame as set out in the code of conduct and establish adequate mechanisms to ensure that all users that have access to the data in the previous3 (three) months are aware of such error and receive the correct information, and that a copy is also sent to the consumer; 4. Be accountable for any data errors to data providers, authorized users and consumers that have occurred during the processing or dissemination of credit information as a result of gross negligence or reckless behavior. CRSPs shall: a. Correct data promptly and establish adequate mechanisms to ensure that all users have access to data in the previous 3 (three) months are aware of such error and receive the correct information after being updated; b. Receive a copy of the updated report and provide the report to consumer; c. Be responsible for any claims	

		from the consumer that may result in a substantial damage of consumer's financial reputation because of gross negligence or reckless behavior; d. Make all reasonable efforts to mitigate damages which have effect on the consumer due to data errors. 5. Be responsible to data providers, authorized users, the NBC, or third party for any claims pertaining to delay, interruption or failing to provide credit information or statistical report, unless they are resulting from governmental orders, sabotages, riots, vandalism, internet service provider denial, or any other causes that are beyond the CRS's reasonable control; 6. Must not transfer, sell or rent any credit information submitted by data providers or authorized users, except as authorized under this Prakas; 7. Cross-border credit information can only be shared under a cooperation framework with prior consent from the NBC and shall take the following considerations: a. Consumer's privacy protection b. Conflict resolution and data correction c. Data security protection and d. Prior consent from the consumer. B. Data providers shall be responsible for: 1. Any incorrect information sent to CRSPs; 2. Any claims from the consumers regarding errors that are material to a substantial damage of customer's financial reputation, as a consequence of gross negligence or reckless	

		behavior in compliance with the decision made under the conflict resolution mechanisms provided in Article 28 of this Prakas and 3. Mitigating damages suffered by consumer for data errors by establishing all necessary policies and procedures. The credit information and other services provided by the CRSPs shall be considered as one of the tools for credit risk decision process, but the decision shall not be made solely based on the credit information obtained from the CRSPs. Each data provider shall have its own loan approval rules.	
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007	Article 6. Banking and Professional Secrecy Banking or professional secrecy shall not inhibit the implementation of the present Law and may not be invoked as a ground for refusal to provide information to the Financial Intelligence Unit and supervisory authority, whether for domestic or for international cooperation purposes, or as required in connection with an investigation which relates to money laundering or financing of terrorism ordered by or carried out under the supervision of a judicial authority.	
		Article 25. Relationships with Foreign Financial Intelligence Unit 1. The Financial Intelligence Unit may, subject to a reciprocal arrangement, exchange information with foreign Financial Intelligence Unit provided that they are subject to similar requirements of confidentiality and irrespective of the nature of those units. It may, for that purpose, conclude cooperation agreements with such units.	

		2. Upon receipt of a request for information or transmission from a counterpart foreign Financial Intelligence Unit, it shall comply with that request within the scope of the powers conferred upon it by the present Law.	
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017		
12	Law on Cybercrime Draft V.1		
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		
15	The Criminal Code 2009 ('the Penal Code')		
16	The Code of Civil Procedure		

#	Regulation	Government Access
		National Security Law, Cybersecurity Law Provisions
1	E-Commerce Law dated 2 November 2019	

2	Law on Consumer Protection No 1119_016 dated October 2019	
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021	Article 4 The Ministry of Interior has the authority to collect, compile, store, manage and secure the identity data of individuals obtained from civil registration, identity card, Khmer nationality, statistics and residence management, passports, nationals and other registrations which are legal and regulatory documents. Yut handed over to the Ministry of Interior. The Ministry of Interior, which owns the original data, may authorize ministries, institutions, entities in both the public and private sectors or individuals to use the identity data in accordance with the procedures and procedures set forth in this sub-decree and other legal documents in force.
		Article 6 Authorize the use of personal identification data stored and managed by the Ministry of Interior for the purpose of verifying or verifying or verifying personal identities to serve the public interest, improve the quality of service delivery and national development.
		Article 7 Ministries, institutions, organizations in both the public and private sectors, or individuals wishing to use personal identification data, must apply for permission from the Ministry of Interior in accordance with the procedures and legal documents in force.
		Article 8 Authorization of Ministries and Institutions in the public sector to use personal identification data to serve the provision of public services shall be made by an inter-ministerial prakas or a joint prakas between the Minister of Interior and the Minister or the head of the institution requesting it. Authorization of private sector entities to use personal identification data to provide public services shall be made by agreement or memorandum of understanding between the representative of the Ministry of Interior and the head or representative of the requested private sector entity. The procedure and procedure for requesting to confirm the identity of the person or confirm the authenticity requested by the person concerned shall be determined by a Prakas of the Minister of the Ministry of Interior. Procedures and procedures for requesting identification or authenticity for use in the field of justice, security, public order shall be determined by a Prakas of the Minister of Interior.
4	Law on Banking and Financial Institutions dated November 18, 1999	
5	Prakas on Credit Reporting dated June 26 2020	Article 24.- Confidentiality A. The credit information and dishonored check information is confidential and shall only be used for the permissible purposes set

		forth in the Article 9 of this Prakas. CRSPs, data providers, and authorized users shall strictly keep credit information or dishonored check information confidentially and shall not sell or otherwise provide such information to any third party. B. Only the NBC, the CRSPs, and the authorized users can access the information and always for the strict performance of their duties. C. The CRSPs shall take all necessary measures to ensure that CRS's directors, management, and employees regularly maintain the confidentiality of credit information and shall take all reasonable measures to prevent unauthorized access to information, and shall establish and enforce security policies and procedures to govern the access to the credit information and dishonored check information. D. The NBC shall have free access to the CRS to obtain credit information for its oversight functions of covered entities, as well as other information pertaining to the non-covered entities to monitor the overall financial stability. E. The NBC shall have access to the CRS in order to fulfill its oversight functions to maintain the efficient, transparent, fair and legal operations of the CRS. F. Directors and employees of CRSPs, authorized users and employees of data providers shall sign confidentiality agreements prior to gaining access to credit information of the CRS.
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007	
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008	
8	Sub-Decree No. 61 on Physician's Code of Ethics	
9	Sub-Decree on Dental Ethics no 156	
10	Law on Telecommunications (Telecom Law) enacted December 17, 2015	
11	Sub-Decree on Digital Signatures No	

	246 dated 29 December 2017	
12	Law on Cybercrime Draft V.1	Article 20: Condition and Safeguard 1. The access to a computer system, as well as the interception or recording of communications carried out by means of computer systems are performed when useful to find the truth and the facts or identification of the doers cannot be achieved on the basis of other evidence. 2. The measures referred to at paragraph (1) are performed by motivated authorisation of the prosecutor specially assigned by the general prosecutor related to the Court of Appeal or, as appropriate, of the general prosecutor of the office related to the Supreme Court, and for the corruption offences, of the general prosecutor of the National Anti-Corruption Office, by the criminal investigation bodies with the help of specialised persons, who are obliged to keep the confidentiality of the operation performed. 3. The authorisation referred to at paragraph (2) is given for 30 days at the most, with the extension possibility under the same conditions, for duly justified reasons, each extension not exceeding 30 days. The maximum duration of these measures is 4 10months. 4. Until the end of the criminal investigation, the prosecutor is obliged to inform, in writing, the persons against whom the measures referred to in paragraph (1) are taken. 5. The procedures of the Criminal procedure Code regarding the audio or video recordings are applied accordingly
13	The Constitution of the Kingdom of Cambodia 2008	
14	The Civil Code	
15	The Criminal Code 2009 ('the Penal Code')	
16	The Code of Civil Procedure	

Penalty

#	Regulation	Corporate Punishments	Individual Punishments
		Forms of penalties (e.g., recommendations for corrective action, public penalties, fines, confiscation of assets and income, data deletion, data processing, business suspension, etc.)	Penalties (penalties, fines, demotion, etc.)
1	E-Commerce Law dated 2 November 2019	Article 54: Offence for Failure to Report of an Information or a Fact To be punishable by an imprisonment from 1 (one) month to 1 (one) year and a fine	Article 54: Offence for Failure to Report of an Information or a Fact To be punishable by an imprisonment from 1 (one) month to 1 (one) year and a fine

		from 100,000 (one hundred thousand) Riel to 2,000,000 (two million) Riel for the intermediary and the electronic commerce service providers who act in violation of the provisions of paragraph 1 and paragraph 2 of Article 25.	from 100,000 (one hundred thousand) Riel to 2,000,000 (two million) Riel for the intermediary and the electronic commerce service providers who act in violation of the provisions of paragraph 1 and paragraph 2 of Article 25.
		Article 55: Provision of False Information To be punishable by an imprisonment from 1 (one) month to 1 (one) year and a fine from 100,000 (one hundred thousand) Riel to 2,000,000 (two million) Riel for those who commit act as prescribed in the provision of paragraph 5 of Article 25.	Article 55: Provision of False Information To be punishable by an imprisonment from 1 (one) month to 1 (one) year and a fine from 100,000 (one hundred thousand) Riel to 2,000,000 (two million) Riel for those who commit act as prescribed in the provision of paragraph 5 of Article 25.
		Article 60: Offence for Failure to Comply with Data Protection Obligations To be punishable by an imprisonment from 1 (one) year to 2 (two) years and a fine from 2,000,000 (two million) Riel to 4,000,000 (four million) Riel for those who store information in an electronic form for a personal purpose, which is contrary to the provision of paragraph 1 of Article 32. To be punishable by an imprisonment from 1 (one) year to 2 (two) years and a fine from 2,000,000 (two million) Riel to 4,000,000 (four million) Riel for those who act in violation of the provision of paragraph 2 of Article 32.	Article 60: Offence for Failure to Comply with Data Protection Obligations To be punishable by an imprisonment from 1 (one) year to 2 (two) years and a fine from 2,000,000 (two million) Riel to 4,000,000 (four million) Riel for those who store information in an electronic form for a personal purpose, which is contrary to the provision of paragraph 1 of Article 32. To be punishable by an imprisonment from 1 (one) year to 2 (two) years and a fine from 2,000,000 (two million) Riel to 4,000,000 (four million) Riel for those who act in violation of the provision of paragraph 2 of Article 32.
2	Law on Consumer Protection No 1119_016 dated October 2019	Article 34: Decision to Disclose Information or to Re-Publish If the National Committee for Consumer Protection has found that the individual concerned has violated any provision of this law, the National Committee for Consumer Protection may issue the following decisions: 1. Requiring the person who failed to publish information or	Article 34: Decision to Disclose Information or to Re-Publish If the National Committee for Consumer Protection has found that the individual concerned has violated any provision of this law, the National Committee for Consumer Protection may issue the following decisions: 1. Requiring the person who failed to publish information or publishes insufficient

		publishes insufficient information to publish that information or any part thereof in a sufficient manner according to the procedures in this provision and to pay all the expenses on its own to any relevant public person or individual. 2. Requiring the person who published false or misleading information to make corrections according to the procedures stated in this provision and paying all the related expenses on its own.	information to publish that information or any part thereof in a sufficient manner according to the procedures in this provision and to pay all the expenses on its own to any relevant public person or individual. 2. Requiring the person who published false or misleading information to make corrections according to the procedures stated in this provision and paying all the related expenses on its own.
		Article 35: Decision on the Prohibition from Management Function The National Committee for Consumer Protection may render a decision to ban / prohibit any individual from holding a management function if: 1. That individual commits the offenses of the following with the occurrence of two times or more: - Act of dishonesty relating to goods and/or services - Misleading representation - Promise to offer gifts and prizes - Bait advertising - Dishonest sale by persuasion - The demand or acceptance of payments without the intention to supply goods or services as ordered - False or misleading representations of certain business activities - Physical coercion and mental threats - Pyramid selling scheme, or - Sale of goods attached with a false trade description. 2. That individual has committed the offenses of the following with the occurrence of at least two times within 5 years and the individual holds the position as	Article 35: Decision on the Prohibition from Management Function The National Committee for Consumer Protection may render a decision to ban / prohibit any individual from holding a management function if: 1. That individual commits the offenses of the following with the occurrence of two times or more: - Act of dishonesty relating to goods and/or services - Misleading representation - Promise to offer gifts and prizes - Bait advertising - Dishonest sale by persuasion - The demand or acceptance of payments without the intention to supply goods or services as ordered - False or misleading representations of certain business activities - Physical coercion and mental threats - Pyramid selling scheme, or - Sale of goods attached with a false trade description. 2. That individual has committed the offenses of the following with the occurrence of at least two times within 5 years and the individual holds the position as

		director or manager of a legal person: - Failure to disclose information standards for the consumers; - Failure to perform its obligations in complying with the information standards for consumers; or - Failure to provide a notification of the information standards for consumers. 3. Any individual who is prohibited by a foreign state with respect to consumer protection as stated in points 1 and 2.	director or manager of a legal person: - Failure to disclose information standards for the consumers; - Failure to perform its obligations in complying with the information standards for consumers; or - Failure to provide a notification of the information standards for consumers. 3. Any individual who is prohibited by a foreign state with respect to consumer protection as stated in points 1 and 2.
		Article 40: Sanctions and Interim Penalties The penalties under this law shall include written warnings, suspension or revocation or cancellation of the certificate of incorporation or license, an interim penalty/transitional fine, monetary fines and imprisonment. The written warning, suspension or revocation or cancellation of the certificate of incorporation or license shall fall within the competency of the National Committee for Consumer Protection. Imposing an interim penalty shall be the competency of the investigating officer. Payment of the transitional fine shall lead to the extinction of any related criminal actions of the offenses. In the case where the offender refuses to pay the interim penalty, the investigating officer may bring the case to a competent court. The procedure for interim penalties, the payment of fines, the management of payment receipts for fines issued, and the management of income from penalizing violators as stated in	Article 40: Sanctions and Interim Penalties The penalties under this law shall include written warnings, suspension or revocation or cancellation of the certificate of incorporation or license, an interim penalty/transitional fine, monetary fines and imprisonment. The written warning, suspension or revocation or cancellation of the certificate of incorporation or license shall fall within the competency of the National Committee for Consumer Protection. Imposing an interim penalty shall be the competency of the investigating officer. Payment of the transitional fine shall lead to the extinction of any related criminal actions of the offenses. In the case where the offender refuses to pay the interim penalty, the investigating officer may bring the case to a competent court. The procedure for interim penalties, the payment of fines, the management of payment receipts for fines issued, and the management of income from penalizing violators as stated in

		the provision of this law must be prescribed in an inter-ministerial Prakas between the Ministers of the Ministry of Commerce, the Ministry of Justice, and the Ministry of Economy and Finance.	the provision of this law must be prescribed in an inter-ministerial Prakas between the Ministers of the Ministry of Commerce, the Ministry of Justice, and the Ministry of Economy and Finance.
		Article 41: Dishonest Acts Relating to Goods, Services, or Misleading Claims A written warning shall be given to any individual who committed dishonest acts relating to goods, services, or misleading claims as stated in Article 9, Article, 10, Article 11, and Article 12. Where a written warning is already issued but there is still a violation under the first paragraph, the certificate of commercial registration or license shall be suspended, revoked, or voided. Violations of the first paragraph above relating to the quality and origin of the goods shall be punishable by an interim penalty of an amount not exceeding 20,000,000 (twenty million) Riels.	Article 41: Dishonest Acts Relating to Goods, Services, or Misleading Claims A written warning shall be given to any individual who committed dishonest acts relating to goods, services, or misleading claims as stated in Article 9, Article, 10, Article 11, and Article 12. Where a written warning is already issued but there is still a violation under the first paragraph, the certificate of commercial registration or license shall be suspended, revoked, or voided. Violations of the first paragraph above relating to the quality and origin of the goods shall be punishable by an interim penalty of an amount not exceeding 20,000,000 (twenty million) Riels.
		Article 42: Aggravating Circumstances of Dishonest Acts Relating to Goods, Services, or Misleading Claims that Affect Health and Safety Violations of the first paragraph of Article 41 in the case of severely affecting the health and safety of a consumer shall be punishable by imprisonment from 6 (six) months to 2 (two) years and fined from 1,000,000 (one million) to 4,000,000 (four million) Riels.	Article 42: Aggravating Circumstances of Dishonest Acts Relating to Goods, Services, or Misleading Claims that Affect Health and Safety Violations of the first paragraph of Article 41 in the case of severely affecting the health and safety of a consumer shall be punishable by imprisonment from 6 (six) months to 2 (two) years and fined from 1,000,000 (one million) to 4,000,000 (four million) Riels.
		Article 43: Aggravating Circumstances of Dishonest Acts Relating to Goods, Services, or Misleading Claims that Cause Disability or Death Violations of the first paragraph of Article 41 that causes permanent disability or death shall be punishable by imprisonment from 2 (two) years	Article 43: Aggravating Circumstances of Dishonest Acts Relating to Goods, Services, or Misleading Claims that Cause Disability or Death Violations of the first paragraph of Article 41 that causes permanent disability or death shall be punishable by imprisonment from 2 (two) years

		to 5 (five) years and fined from 4,000,000 (four million) Riels to 10,000,000 (ten million) Riels.	to 5 (five) years and fined from 4,000,000 (four million) Riels to 10,000,000 (ten million) Riels.
		Article 44: Acts Relating to Dishonest Practices Any individual who engages in bait advertisement, the demand or acceptance of payment without the intent to provide the goods or services as ordered, false or misleading representation about certain business activities, coercion by force or mental threat, shall be punished by an interim penalty not exceeding 50,000,000 (fifty million) Riels.	Article 44: Acts Relating to Dishonest Practices Any individual who engages in bait advertisement, the demand or acceptance of payment without the intent to provide the goods or services as ordered, false or misleading representation about certain business activities, coercion by force or mental threat, shall be punished by an interim penalty not exceeding 50,000,000 (fifty million) Riels.
		Article 48: Violations for Non-Compliance of the Provision on the Information Standards for Consumers Any individual who does not comply with the provision on the information standards for consumers shall be punishable by an interim penalty not exceeding 10,000,000 (ten million) Riels.	Article 48: Violations for Non-Compliance of the Provision on the Information Standards for Consumers Any individual who does not comply with the provision on the information standards for consumers shall be punishable by an interim penalty not exceeding 10,000,000 (ten million) Riels.
3	Sub-Decree No,252 on the management, use, and protection of personal identification data dated 22 December 2021		Article 17 Individuals who violate the provisions of this sub-decree, the Ministry of Interior may decide to impose any of the following disciplinary sanctions: A - Warning B. Blame C- Restrictions, suspension or cancellation of agreements or memoranda of understanding.
			Article 19 The competent official who exercises authority other than the purpose of this sub-decree or violates the provisions of this sub-decree shall be liable for the acts he has committed in accordance with the laws of the Kingdom of Cambodia.
4	Law on Banking and Financial Institutions dated	Article 55. In addition to the penalties provided for in case of violation of provisions of ordinary law or of the legal	Article 55. In addition to the penalties provided for in case of violation of provisions of ordinary law or of the legal

	November 18, 1999	statute of noncommercial societies, the following penalties may be applied under this law: Any person who, acting either for his own account or for the account t of a legal person, as his regular business and on behalf of the general public carries out banking operations without a license. shall be liable before the courts to imprisonment from 1 year to 5 years and a fine from 5 million to 250 million riels, or to either of these penalties, without prejudice to the closure of the concerned establishment. 2. Any person or entity who infringes any of the provisions of Articles 9. 11, 18. 19, 27, 30, and 47. shall be liable before the courts to the penalties provided for in Article 55-1 above. Any person, acting either for his own account or for the account of a legal person, shall be liable before the courts to imprisonment from one year to five years and a fine from 1 million to 10 million riels, or to either of these penalties: -if he infringes any of the provisions of Articles 8. 13. 23, 24, 28, 38. 39 44. 45, 46 and 51: - or if. after formal demand from the supervisory authority, he fails to respond to request for information provided for in Article 40-7: or if he knowingly provides the supervisory authority with inaccurate information: or if he hinders examinations implemented by the supervisory authority or by the external auditors of a covered entity or hinders the missions of a provisional administrator or of a	statute of noncommercial societies, the following penalties may be applied under this law: Any person who, acting either for his own account or for the account t of a legal person, as his regular business and on behalf of the general public carries out banking operations without a license. shall be liable before the courts to imprisonment from 1 year to 5 years and a fine from 5 million to 250 million riels, or to either of these penalties, without prejudice to the closure of the concerned establishment. 2. Any person or entity who infringes any of the provisions of Articles 9. 11, 18. 19, 27, 30, and 47. shall be liable before the courts to the penalties provided for in Article 55-1 above. Any person, acting either for his own account or for the account of a legal person, shall be liable before the courts to imprisonment from one year to five years and a fine from 1 million to 10 million riels, or to either of these penalties: -if he infringes any of the provisions of Articles 8. 13. 23, 24, 28, 38. 39 44. 45, 46 and 51: - or if. after formal demand from the supervisory authority, he fails to respond to request for information provided for in Article 40-7: or if he knowingly provides the supervisory authority with inaccurate information: or if he hinders examinations implemented by the supervisory authority or by the external auditors of a covered entity or hinders the missions of a provisional administrator or of a

		liquidator appointed by the supervisory authority	liquidator appointed by the supervisory authority
		Article 56. The penalties provided for in Article 55 shall be imposed by the courts, in particular after a prior complaint or action for damages by the supervisory authority or by the covered entities' professional association provided for in Article 72 hereafter.	Article 56. The penalties provided for in Article 55 shall be imposed by the courts, in particular after a prior complaint or action for damages by the supervisory authority or by the covered entities' professional association provided for in Article 72 hereafter.
5	Prakas on Credit Reporting dated June 26 2020	Article 30.-Transactional penalties Any person violates the provisions of this Prakas shall be liable for the transactional penalties as following: A. Any person who, acts either for his own account, or for the account of a natural or legal person, by carrying out the CRA without license, shall be liable for transactional penalties from KHR 5,000,000 (five million) to KHR 250,000,000 (two hundred and fifty million), without prejudice to the closure of the concerned establishment; B. Any person or data provider or authorized user, that uses the information obtained from the CRS for a different purposes other than the ones established under this Prakas shall be subject to transactional penalties from KHR 5,000,000 (five million) to KHR 250,000,000 (two hundred and fifty million); C. Covered entities and non-covered entities shall be liable for transactional penalties of KHR 10,000,000 (ten million) to KHR 50,000,000 (fifty million), following the cases of: 1. infringe any code of conduct 2. fail to provide complete and	Article 30.-Transactional penalties Any person violates the provisions of this Prakas shall be liable for the transactional penalties as following: A. Any person who, acts either for his own account, or for the account of a natural or legal person, by carrying out the CRA without license, shall be liable for transactional penalties from KHR 5,000,000 (five million) to KHR 250,000,000 (two hundred and fifty million), without prejudice to the closure of the concerned establishment; B. Any person or data provider or authorized user, that uses the information obtained from the CRS for a different purposes other than the ones established under this Prakas shall be subject to transactional penalties from KHR 5,000,000 (five million) to KHR 250,000,000 (two hundred and fifty million); C. Covered entities and non-covered entities shall be liable for transactional penalties of KHR 10,000,000 (ten million) to KHR 50,000,000 (fifty million), following the cases of: 1. infringe any code of conduct 2. fail to provide complete and

		accurate credit information and dishonored check information to the CRS; 3. fail to access the CRS for credit assessment; 4. fail to respond to request for information by the NBC within the timeframe specified; 5. knowingly provide the CRS with inaccurate or incomplete information regarding a consumer complaint; 6. fail to comply with the deadlines for consumers, guarantors, and drawers' rights; 7. fail to request for prior consent from consumers, guarantors, and drawers; 8. upload incorrect information or with carelessness causing financial defamation to consumers, guarantors, and drawers. D. In case CRSPs fail to follow this Prakas, CRSPs shall be liable for transactional penalties from KHR 5,000,000 (five million) to KHR 250,000,000 (two hundred and fifty million) E. Besides the above transactional penalties, any person infringes on the provision provided in this Prakas or the code of conduct shall be liable for disciplinary sanctions and penalties as provided in applicable law	accurate credit information and dishonored check information to the CRS; 3. fail to access the CRS for credit assessment; 4. fail to respond to request for information by the NBC within the timeframe specified; 5. knowingly provide the CRS with inaccurate or incomplete information regarding a consumer complaint; 6. fail to comply with the deadlines for consumers, guarantors, and drawers' rights; 7. fail to request for prior consent from consumers, guarantors, and drawers; 8. upload incorrect information or with carelessness causing financial defamation to consumers, guarantors, and drawers. D. In case CRSPs fail to follow this Prakas, CRSPs shall be liable for transactional penalties from KHR 5,000,000 (five million) to KHR 250,000,000 (two hundred and fifty million) E. Besides the above transactional penalties, any person infringes on the provision provided in this Prakas or the code of conduct shall be liable for disciplinary sanctions and penalties as provided in applicable law
6	Law on Anti-Money Laundering and Combating the Financing of Terrorism 2007	Article 29. Penal Sanctions Without taking into consideration of any offenses in the penal provisions of other law: • Any person who denies providing information to the FIU and the supervisory authorities as contrary to the provisions of Article 6 of the present Law will be sentenced to imprisonment from six days to one month and subject to a fine from 100,000 Riels up to 1,000,000 Riels or any one thereof.	Article 29. Penal Sanctions Without taking into consideration of any offenses in the penal provisions of other law: • Any person who denies providing information to the FIU and the supervisory authorities as contrary to the provisions of Article 6 of the present Law will be sentenced to imprisonment from six days to one month and subject to a fine from 100,000 Riels up to 1,000,000 Riels or any one thereof.

		• Any person who neglects to provide report on cash and suspicious transactions to the FIU as contrary to the provisions of Article 12 of the present Law will be sentenced to imprisonment from one month to one year, and will be subject to a fine from 1,000,000 Riels up to 5,000,000 Riels or any one thereof. • Any person required to disclose the information and submit reports referred to in Article 13, or any other individual having knowledge thereof, communicate such information or reports as the contrary to the provisions of prohibition of tipping off in Article 15 of the present Law will be sentenced to imprisonment from one month to one year, and will be subject to a fine from 1,000,000 Riels up to 5,000,000 Riels or any one thereof. • Any person who violates the obligations to keep professional secrecy as contrary to Article 23 of the present Law will be sentenced to imprisonment from one month to one year, and will be subject to a fine from 1,000,000 Riels up to 5,000,000 Riels or any one thereof.	• Any person who neglects to provide report on cash and suspicious transactions to the FIU as contrary to the provisions of Article 12 of the present Law will be sentenced to imprisonment from one month to one year, and will be subject to a fine from 1,000,000 Riels up to 5,000,000 Riels or any one thereof. • Any person required to disclose the information and submit reports referred to in Article 13, or any other individual having knowledge thereof, communicate such information or reports as the contrary to the provisions of prohibition of tipping off in Article 15 of the present Law will be sentenced to imprisonment from one month to one year, and will be subject to a fine from 1,000,000 Riels up to 5,000,000 Riels or any one thereof. • Any person who violates the obligations to keep professional secrecy as contrary to Article 23 of the present Law will be sentenced to imprisonment from one month to one year, and will be subject to a fine from 1,000,000 Riels up to 5,000,000 Riels or any one thereof.
7	Prakas on Anti-Money Laundering and Combating the Financing of Terroism dated September 10 2008		
8	Sub-Decree No. 61 on Physician's Code of Ethics		
9	Sub-Decree on Dental Ethics no 156		
10	Law on Telecommunications (Telecom Law) enacted		

	December 17, 2015		
11	Sub-Decree on Digital Signatures No 246 dated 29 December 2017	Article 29 In addition to criminal cases, all disputes related to digital signatures, including disputes between digital signatures and digital signatures, and between digital signatures and owners, digital signatures, and digital signatures. To reconcile. The conditions and procedures for conciliation shall be determined by a Prakas of the CPT. The fee for resolving disputes shall be determined by a joint proclamation between the DAC. And the Ministry of Economy and Finance	Article 29 In addition to criminal cases, all disputes related to digital signatures, including disputes between digital signatures and digital signatures, and between digital signatures and owners, digital signatures, and digital signatures. To reconcile. The conditions and procedures for conciliation shall be determined by a Prakas of the CPT. The fee for resolving disputes shall be determined by a joint proclamation between the DAC. And the Ministry of Economy and Finance
		Article 33 Dissemination of the key to creating a digital signature is subject to the following transaction penalties: Physical person: Amount from 3,000,000 (three million) Riels to 9,000,000 (nine million) Riels. Legal entity: Amount from 25,000,000 (twenty five million) Riels to 75,000,000 (seventy five million) Riels.	Article 33 Dissemination of the key to creating a digital signature is subject to the following transaction penalties: Physical person: Amount from 3,000,000 (three million) Riels to 9,000,000 (nine million) Riels. Legal entity: Amount from 25,000,000 (twenty five million) Riels to 75,000,000 (seventy five million) Riels.
		Article 39 The person who commits the offense as stated in Article 31, Article 32, Article 33, Article 34, Article 35, Article 36 and Article 37 of this sub-decree shall pay the transitional penalty within 30 (thirty) days from the date of receipt. Decided to fine. In case the offender does not pay the transaction penalty as prescribed in the first paragraph above. Must prepare a file to send to the prosecutor of the court. The form of penalties and the management of money derived from penalties shall be determined by a joint proclamation between the PPT. And the Ministry of Economy and Finance 90	Article 39 The person who commits the offense as stated in Article 31, Article 32, Article 33, Article 34, Article 35, Article 36 and Article 37 of this sub-decree shall pay the transitional penalty within 30 (thirty) days from the date of receipt. Decided to fine. In case the offender does not pay the transaction penalty as prescribed in the first paragraph above. Must prepare a file to send to the prosecutor of the court. The form of penalties and the management of money derived from penalties shall be determined by a joint proclamation between the PPT. And the Ministry of Economy and Finance 90

12	Law on Cybercrime Draft V.1	Article 21: Illegal Access 1. The access without right to a computer system is an offence shall be sentenced from 06 months to 03 years and fined from one million Riel (1,000,000) to six million Riel (6,000,000). 2. It is an offence where the act provided in paragraph (1) is committed with the intent of obtaining computer data, shall be sentenced from 06 months to 05 years and fined from one million Riel (1,000,000) to ten million Riel (10,000,000). 3. It is an offence where the act provided in paragraphs 1-2 is committed by infringing the security measures, shall be sentenced from 03 years to 12 years and fined from six million Riel (6,000,000) to twenty four million Riel (24,000,000)	Article 21: Illegal Access 1. The access without right to a computer system is an offence shall be sentenced from 06 months to 03 years and fined from one million Riel (1,000,000) to six million Riel (6,000,000). 2. It is an offence where the act provided in paragraph (1) is committed with the intent of obtaining computer data, shall be sentenced from 06 months to 05 years and fined from one million Riel (1,000,000) to ten million Riel (10,000,000). 3. It is an offence where the act provided in paragraphs 1-2 is committed by infringing the security measures, shall be sentenced from 03 years to 12 years and fined from six million Riel (6,000,000) to twenty four million Riel (24,000,000)
		Article 23: Illegal Interception The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data, shall be sentenced from 02 years to 07 years and fined from four million Riel (4,000,000) to fourteen million Riel (14,000,000)	Article 22: Data Espionage 1. Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access, shall be sentenced from 01 years to 03 years and fined from two million Riel (2,000,000) to six million Riel (6,000,000). 2. Data within the meaning of subsection 1 are only such as are stored or transmitted electronically or magnetically or in any form not directly visible.
		Article 24: Data Interference The alteration, deletion or deterioration of computer data or restriction to such data without right is an offence, shall be sentenced from 02 years to 07 years and fined from four million Riel (4,000,000) to fourteen million Riel (14,000,000)	Article 23: Illegal Interception The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data, shall be sentenced from 02 years to 07 years and fined from four million Riel (4,000,000) to fourteen million Riel (14,000,000)

		Article 25: Unauthorized Data Transfer The unauthorized data transfer from a computer system or by means of a computer data storage medium is an offence shall be sentenced from 03 years to 12 years and fined from six million Riel to twenty four million Riel (24,000,000).	Article 24: Data Interference The alteration, deletion or deterioration of computer data or restriction to such data without right is an offence, shall be sentenced from 02 years to 07 years and fined from four million Riel (4,000,000) to fourteen million Riel (14,000,000)
		Article 26: System Interference The act of causing serious hindering, without right, of the functioning of a computer system, by inputting, transmitting, altering, deleting or deteriorating computer data or by restricting the access to such data, shall be sentenced from 03 years to 15 years and fined from six million Riel to thirty million Riel	Article 25: Unauthorized Data Transfer The unauthorized data transfer from a computer system or by means of a computer data storage medium is an offence shall be sentenced from 03 years to 12 years and fined from six million Riel to twenty four million Riel (24,000,000).
			Article 26: System Interference The act of causing serious hindering, without right, of the functioning of a computer system, by inputting, transmitting, altering, deleting or deteriorating computer data or by restricting the access to such data, shall be sentenced from 03 years to 15 years and fined from six million Riel to thirty million Riel
			Article 28: Contents and Websites Any persons who engage in activities set forth in the followings: 1. Establishing contents that deemed to hinder the sovereignty and integrity of the Kingdom of Cambodia is a punishable offense of incarceration from one to three years and fined of 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels). 2. Publications that deemed to incite or instigate the general population that could cause one

			or many to generate anarchism is punishable of incarceration from one to three years and fined of 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels). 3. Publications or continuation of publication that deemed to generate insecurity, instability, and political cohesiveness is a punishable office of incarceration from one to three years and fined of 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels) 4. Publications or continuation of publication that deemed to be non-factual which slanders or undermined the integrity of any governmental agencies, ministries, not limited to departments, federal or local levels, is a punishable offense of incarceration from one to three years and fined of 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels). 5. Publications that deemed damaging to the moral and cultural values of the society as stated herein: a. Information that incites or instigates prejudice on race or clans, color, gender, language, religion, beliefs or political views, origin of race or nationality, and not limited to levels or class in society. b. Writings or pixilation that deemed to display inappropriate activities of persons, copulations between humans or animals, or devalue the moral of family values and pixilation that deemed to display domestic violence c. Manipulation, defamation, and slanders d. Drawings, pictorials, or

			pixilation that deemed to slander or defame human beings or commoners of the state performing activities unbecoming, with animals of any species is punishable of incarceration from one to three years and fined 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels) Publicizing with the intent to threatened and commit a crime not limited to one form of felonies or other felonies with the intent to interrupt a person or persons wellbeings is punishable of incarceration from one to three years and fined 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels). In the case of with the intent to threaten shall be treated as such law that is currently being enforced
			Article 30: Computer Related Fraud The causing of a loss of property to another person by inputting, altering or deleting of computer data, by restricting the access to such data or by any interference with the functioning of a computer system with the intent of procuring an economic benefit for oneself or for another shall be sentenced from 03 years to 12 years and fined from six million Riel (6,000,000) to twenty four million Riel (24,000,000)
			Article 31: Computer Related Forgery The input, alteration or deletion, without right, of computer data or the restriction, without right, of the access to such data, resulting in inauthentic data, with the intent to be used for legal purposes, is a criminal offence and shall be punished

			with 14 imprisonment from 2 to 7 years
			Article 33: Attempt Attempt to commit a misdemeanor as stated in Article 427 (Accessing or Maintaining Access to Automated Data Processing System), Article 428 (Act of Obstructing the Operations of Automated Data Processing System), Article 429 (Fraudulent Introduction, Deletion or Modification of Data), Article 430 (Participation in Group or a Agreement to prepare for the commission of Offences) of Criminal Code and Article 21 (Illegal Access), Article 22 (Data Espionage), Article 23 (Illegal Interception), Article 24 (Data Interference), Article 25 (Unauthorized Data Transfer), Article 26 (System Interference), Article 27 (Child Pornography), Article 28 (Contents and Websites), Article 29 (Intellectual Property Rights and Related Rights), Article 30 (Computer Related Fraud), Article 31 (Computer Related Forgery) and Article 32 (Misuse of Device) of this law shall face the same punishment as misdemeanor
13	The Constitution of the Kingdom of Cambodia 2008		
14	The Civil Code		
15	The Criminal Code 2009 ('the Penal Code')		Article 301: Listening or Recording Private Speeches The acts of listening or recording the privately announced or confidential speeches without the consent of the concerned person, is punishable, except for the cases where it is authorized by law, by an imprisonment of between 1 (one) month and 1 (one) year and a fine of between 100,000 (one hundred thousand) and 2,000,000 (two million) Riels. If the affected person is informed

			of the listening or the recording and he did not oppose to it, his consent is therefore presumed
			Article 302: Infringement on the Right of Private Picture The acts of taking picture of a person in a private place without the consent of the latter, is punishable, except for the cases where it is authorized by law, by an imprisonment of between 1 (one) month and 1 (one) year and a fine of between 100,000 (one hundred thousand) and 2,000,000 (two million) Riels. If the affected person is informed of the picture taking and he/she did not oppose to it, his/her consent is therefore presumed
			Article 314: Acts of Infringement on Professional Confidential Any person who holds, by reason of his/her position, profession, function or mission, an information of confidential nature, and if he/she has revealed the said information to an unauthorized person to know its content, is punishable by an imprisonment of between 1 (one) month and 1 (one) year and a fine of between 100,000 (one hundred thousand) Riels to 2,000,000 (two million) Riels. The offence does not constitute in the case where the law authorizes or imposes the revelation of the secrets.
			Article 318: Infringement on Secrecy of Telephone Conversation The act of listening or jamming the telephone conversations, in bad faith, is punishable by an imprisonment of between 1 (one) month and 1 (one) year and a fine of between 100,000 (one hundred thousand) Riels to 2,000,000 (two million) Riels. The act of intercepting or jamming the messages transmitted by means of

			telecommunications or by way of fraudulently acquiring knowledge of their content, in bad faith, is punishable by the same penalties.
			Article 427: Threats to Commit Destruction Followed by an Order The threat, by means whatsoever, to commit destruction, deterioration or damage is punishable by an imprisonment from 1 (one) year to 2 (two) years and a fine from 2,000,000 (two million) Riels to 4,000,000 (four million) Riels if the threat was followed by an order to perform or not to perform anything.
			Article 428: Falsification of Information The act of communicating or disclosing false information with intention to create an impression that destruction, deterioration or damage to persons be committed is punishable by an imprisonment from 1 (one) year to 2 (two) years and a fine from 2,000,000 (two million) Riels to 4,000,000 (four million) Riels
			Article 430: Accessing or Maintaining Access to Automated Data Processing Systems The acts of fraudulently having access to a system of automated data processing or maintaining access to it, is punishable by an imprisonment from 1 (one) month to 1 (one) year and a fine from 100,000 (one hundred thousand) Riels to 2,000,000 (two million) Riels. When the act has resulted in either deletion or modification of the data contained in the system, or an alteration of the functioning of the system, it is punishable by an imprisonment from 1 (one) year to 2 (two) years and a fine from 2,000,000 (two

			million) Riels to 4,000,000 (four million) Riels
			Article 431: Act of Obstructing the Operations of Automated Data Processing System Any act of obstructing the operations of the automated processing system of data is punishable by an imprisonment from 1 (one) year to 2 (two) years and a fine from 2,000,000 (two million) Riels to 4 (four million) Riels.
			Article 432: Fraudulent Introduction, Deletion or Modification of Data The fraudulent acts of introducing, deleting or modifying data in an automated processing system are punishable by an imprisonment from 1 (one) year to 2 (two) years and a fine from 2,000,000 (two million) Riels to 4,000,000 (four million) Riels.
			Article 433: Participation in a Group or a Agreement to Prepare for the Commission of Offences The participation in a group or in a knock-out agreement established in order to prepare for the commission of one or several offences specified in the present Chapter is punishable by an imprisonment from 1 (one) year to 2 (two) years and a fine from 2,000,000 (two million) Riels to 4,000,000 (four million) Riels.
16	The Code of Civil Procedure		

C) Indonesia

Legal system overview

#	Regulation	Translation	Purpose of the Legal System
			What purpose does the legal system serve? (e.g. cybersecurity)

		Google translation or Translation by certain organization	
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	Original	
2	Implementing regulation of PDP Law	Original	
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").	Original	it is necessary to make Law concerning Electronic Information and Transactions;
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")	Google translation	
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")	Original	
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)	Original	

7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")	Original	An Act to regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto.
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40	Google translation	
9	Information and Electronic Transaction Law No.19 of 2016	Google translation	
10	Law No. 7 of 1992 on Banking	Google translation	
11	Law No. 36 of 2009 on Health	Google translation	
12	Law No. 1 of 2023 on Criminal Code	Google translation	
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector	Google translation	
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")	Google translation	

15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection	Google translation	
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")	Google translation	
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services	Google translation	
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector	Google translation	
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation	Form of legal system	Target Business
		Is it introduced in accordance with government ordinances and guidelines? (Is it introduced in a format that ensures lead time?)	Does the law target specific industry or in general? Is it clearly stated in the regulations?
		Regulation level	Industry
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	Law	General

2	Implementing regulation of PDP Law	Subordinate Laws and Guidelines	General
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").	Law	Cybersecurity, E-commerce, Information Technology
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")	Subordinate Laws and Guidelines (Government)	Cybersecurity, E-commerce, Information Technology
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")	Subordinate Laws and Guidelines (Minister)	Cybersecurity, E-commerce, Information Technology
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		General
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the	Subordinate Laws and Guidelines (Minister)	General

	Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40	Law	Telecom
9	Information and Electronic Transaction Law No.19 of 2016	Subordinate Laws and Guidelines	General
10	Law No. 7 of 1992 on Banking	Law	Bank
11	Law No. 36 of 2009 on Health	Law	Health
12	Law No. 1 of 2023 on Criminal Code	Law	Criminal
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector	Subordinate Laws and Guidelines	Bank and Financial Services
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")	Subordinate Laws and Guidelines	Bank and Financial Services
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection	Subordinate Laws and Guidelines	Bank and Financial Services

16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")	Subordinate Laws and Guidelines	Bank and Financial Services
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services	Subordinate Laws and Guidelines	Bank and Financial Services
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector	Subordinate Laws and Guidelines	Bank and Financial Services
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation	Regulatory authority	Jurisdiction
		Which regulatory authority has jurisdiction over regulation?	Cyber security, data security, personal information protection, etc.
		Name of ministry/organization	Similar to purpose?
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	ational data protection authority ("Indonesian DPA")	personal information protection
2	Implementing regulation of PDP Law	Minister of Communication and Informatics ("MOCI")	personal information protection
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on		Cybersecurity

	Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")	Government	Cybersecurity
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")	Minister of Communication and Informatics ("MOCI")	Cybersecurity
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)	Minister of Communication and Informatics ("MOCI")	
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")	Minister of Communication and Informatics ("MOCI")	personal information protection
8	Law No. 36 of 1999 on Telecommunicati on (the	Government	personal information protection

	"Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016	Government	personal information protection
10	Law No. 7 of 1992 on Banking	Government	
11	Law No. 36 of 2009 on Health	Government	
12	Law No. 1 of 2023 on Criminal Code	Government	
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector	the Financial Services Authority ("OJK")	
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")	the Financial Services Authority ("OJK")	
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection	the Bank Indonesia ("BI")	
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer	the Bank Indonesia ("BI")	

	Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services	the Financial Services Authority ("OJK")	
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector	the Financial Services Authority ("OJK")	
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation	Status	Citation
		Legislation / Public Comment / Passage / Enforcement / Amendment, etc.	
		Status of the regulation: Draft = drafting (new regulation) published = published in the gazzette but not yet enacted Enact = published in the gazzette and already enacted Amendment = enacted regulation being on amending process	URL
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	Draft	https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022
2	Implementing regulation of PDP Law	Draft	
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on	Enforcement (Second Amendment)	http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4846_UU_11_2008_e.html

	Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")	Enforcement	https://jdih.kominfo.go.id/produk_hukum/view/id/695/t/peraturan+pemerintah+nomor+71+tahun+2019+tanggal+10+oktober+2019
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")	Enforcement	https://www.dataguidance.com/sites/default/files/data_privacy_english_-_permenkominfo_no_20_of_2016.pdf
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")	Enforcement	—
8	Law No. 36 of 1999 on Telecommunication (the	Enforcement	https://www.pdp.gov.my/ppdpv1/

	"Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016	Enforcement	
10	Law No. 7 of 1992 on Banking	Enforcement	
11	Law No. 36 of 2009 on Health	Enforcement	
12	Law No. 1 of 2023 on Criminal Code	Enforcement	
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer		

	Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

Definitions for basic items

#	Regulation	Type and Scope of Data	Data processing and handling
		Personal data, personal information/sensitive and important data/children and minors' data, etc. Is the scope of data clearly written in the regulations? What are the unclear points?	Processing, handling / disclosure, sharing, provision, transmission, outsourcing / use for advertising, etc.
		Specific type of data required to complied with the regulation	Provision for data processing
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	"Personal Data": Personal data means any data related to identified or identifiable individuals, separately or in combination with other information, directly or indirectly, through an electronic or non-electronic system. "Sensitive Personal Data": The PDP Law categorises personal data into general data and specific (sensitive) data, which includes:	"Processing": Processing includes activities of data acquisition, collection, analysis, storing, rectification, update, display, announcement, transfer, dissemination, disclosure, erasure and/or destruction. "Data Breach": Data breach means failure to protect a person's personal data in terms of confidentiality, integrity and availability of the personal data, including security breaches,

		a. health and information data; b. biometric data; c. genetic data; d. criminal records; e. children's data; f. personal financial data; and/or g. other data in accordance with provisions of laws and regulations.	whether intentional or unintentional, leading to destruction, loss, alteration, disclosure or unauthorised access to the data which are being transferred, stored or processed.
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").	Article 1 In this Law, what is meant by: 1. Electronic Information is one or a set of electronic data, including but not limited to text, sounds, images, maps, drafts, photographs, electronic data interchange (EDI), electronic mails, telegrams, telex, telecopy or the like, letters, signs, figures, Access Codes, symbols or perforations that have been processed for meaning or understandable to persons qualified to understand them. 2. Electronic Transaction is a legal act that is committed by the use of Computers, Computer networks, and/or other electronic media. 3. Information Technology is a technique to collect, prepare, store, process, announce, analyze, and/or disseminate information. 4. Electronic Document is any Electronic Information that is created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical form, or the like, visible, displayable and/or audible via Computers or Electronic Systems, including but not limited to writings, sounds, images, maps, drafts,	

		photographs or the like, letters, signs, figures, Access Codes, symbols or perforations having certain meaning or definition or understandable to persons qualified to understand them. 5. Electronic System is a set of electronic devices and procedures that serve to prepare, collect, process, analyze, store, display, announce, send, and/or disseminate Electronic Information. 6. Operation of Electronic System is Electronic System utilization by the state administrators, Persons, Business Entities, and/or the society. 7. Electronic System Network is interlinked network of two or more Electronic Systems, which are closed or open. 8. Electronic Agent is an automated electronic means that is used to initiate an action to certain Electronic Information, which is operated by Persons. 9. Electronic Certificate is a certificate in electronic nature that contains an Electronic Signature and identity, demonstrating a status of a legal subject of parties to an Electronic Transaction issued by Certification Service Providers. 10. Electronic Certification Service Provider is a legal entity that acts as a reliable party, issues and audits Electronic Certificates. 11. Reliability Certification Institute is an independent institution that is formed by professionals acknowledged,	

		certified, and supervised by the Government, whose authority is to audit and issue reliability certificates for Electronic Transactions. 12. Electronic Signature is a signature that contains Electronic Information that is attached to, associated or linked with other Electronic Information that is used for means of verification and authentication. 13. Signatory/Signer i a legal subject associated or linked with an Electronic Signature. 14. Computer i an electronic, magnetic, optical data processing device, or a system that performs logic, arithmetic, and storage functions. 15. Access is an activity to make interaction with independent or network Electronic Systems. 16. Access Code is a figure, letter, symbol, other character or a combination thereof, which is a key to enable Access to Computers and/or other Electronic Systems. 17. Electronic Contract is an agreement of parties entered into by means of Electronic Systems. 18. Sender/Originator is a legal subject that sends Electronic Information and/or Electronic Documents. 19. Recipient/Addressee is a legal subject that receives Electronic Information and/or Electronic Documents from Senders. 20. Domain Name is an internet	

		address of a state administrator, Person, Business Entity, and/or the society that can be used for communication over the internet, in the form of unique character code or set to identify a certain location on the internet. 21. Person is an individual, whether an Indonesian citizen, foreign citizen, or legal entity. 22. Business Entity is a sole proprietorship or partnership of both legal entity and non-legal entity. 23. Government is a Minister or other official appointed by the President.	
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")	29. Personal Data means any data about a person which is identified and/or is identifiable either separately or when combined with other information, either directly or indirectly through an Electronic System and/or non-electronic system. 30. Electronic Data means data in electronic form that is not limited to texts, sounds, images, maps, designs, photographs, electronic data interchange (EDI), electronic mails, telegrams, telexes, telecopies or the like, letters, signs, numbers, Access codes, symbols, or perforations. "Strategic Electronic Data" are: energy, transportation, financial, healthcare, ICT, food, defense, and any other sectors stipulated by the Government.	
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic		

	Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		

14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure		

	('PR No. 82/2022')		

#	Regulation	Data handlers
		Classification/ distinction by responsibility (data processor, data controller)/ size of data, (national security) critical services, etc.
		Provision on type of data handler
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	"Controller": Controller means any person or corporation, public institution and international organisation acting individually or jointly that determine the purposes and have control over personal data processing activities. "Processor": Processor means any person or corporation, public institution and international organisation acting individually or jointly in processing personal data on behalf of the Controller. "Data Subject": Data subject means an individual whose data are associated with.
2	Implementing regulation of PDP Law	
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").	
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")	
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI	

	Regulation 20/2016")	
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)	
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")	
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40	
9	Information and Electronic Transaction Law No.19 of 2016	
10	Law No. 7 of 1992 on Banking	
11	Law No. 36 of 2009 on Health	
12	Law No. 1 of 2023 on Criminal Code	
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector	

14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")	
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection	
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")	
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services	
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector	
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure	

	('PR No. 82/2022')	

Legal Basis

#	Regulation		
		consent	necessary for the performance of a contract
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	In obtaining the consent of the data subject, Article 21 of the PDPL requires the controller to provide the following information: confirmation that the personal data processing shall be carried out for lawful purposes; the purpose of the personal data processing; the type and relevance of the personal data to be processed; the retention period for documents containing personal data; details regarding the information collected; how long the processing of the personal data will be carried out; and the rights of the personal data subject.	
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the		

	Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		

12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital		

	Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation	necessary for compliance with a legal obligation	necessary in order to protect the vital interests
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)		
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in		

	Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the		

	Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information		

	Infrastructure ('PR No. 82/2022')		

#	Regulation		
		necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	necessary for the purposes of the legitimate interests pursued by the controller or by a third party
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)		
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		

6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/20		

	14 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation		
		opt-out	others
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)		
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators		

	(Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer		

	Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

Rights of the data subject

#	Regulation	Right to be informed	Right of access
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	Right to obtain information : The data subject is entitled to obtain information on the identity, legal basis, purpose of request and use of personal data, and accountability of the party requesting the personal data.	Right to access data or copies of data: The data subject is entitled to access and obtain a copy of their personal data, in accordance with the applicable laws and regulations.
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic		

	System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK		

	Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation	Right to rectification	Right to erasure
1	Law No. 27 of 2022 on Personal	Right to complete, update and/or rectify errors or inaccuracies:	Right to terminate the processing, deletion or disposal

	Data Protection (PDP Law)	The data subject is entitled to complete, update and/or rectify errors or inaccuracies of their personal data in accordance with the purpose of data processing.	of data: The data subject is entitled to delete or destroy their personal data in accordance with the applicable laws and regulations.
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		

7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		

15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation	Right to restrict processing	Right to data portability
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	Right to restrict processing: The data subject is entitled to postpone or restrict data processing proportional to the purpose of data processing.	Right to obtain, use or transfer their data: The data subject is entitled to obtain, utilise and transfer their personal data to another Controller, insofar as the system may communicate safely in accordance with the principles provided under the PDP Law.

2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the		

	Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		

16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation	Right to object	Right not to be subject to a decision based solely on automated processing
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	Right to file a lawsuit: The data subject is entitled to file a lawsuit and receive compensation over the violation of their processed personal data. Right to complain to the relevant data protection authority(ies): The data subject is entitled to complain to the relevant authority in respect of a data protection violation.	Right to object against automated decision-making: The data subject is entitled to object to automated decision-making and profiling that has legal or significant effects on them.

2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the		

	Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		

16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation	
		Right to withdraw consent
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	Right to withdraw consent: The data subject is entitled to withdraw their submitted consent to the data processing.
2	Implementing regulation of PDP Law	
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic	

	Information and Transactions ("EIT Law") ("Second Amendment Law").	
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")	
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")	
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)	
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")	
8	Law No. 36 of 1999 on Telecommunicati on (the "Telecommunicat	

	ion Law") Section 40	
9	Information and Electronic Transaction Law No.19 of 2016	
10	Law No. 7 of 1992 on Banking	
11	Law No. 36 of 2009 on Health	
12	Law No. 1 of 2023 on Criminal Code	
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector	
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")	
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection	
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")	

17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services	
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector	
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')	

Extraterritorial application

#	Regulation	applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction	applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)		
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second	Article 2 This Law shall apply to any Person to take legal acts as governed by this Law, both within jurisdiction of Indonesia and outside jurisdiction of Indonesia, which has legal effect within jurisdiction of Indonesia and/or outside jurisdiction of	Article 2 This Law shall apply to any Person to take legal acts as governed by this Law, both within jurisdiction of Indonesia and outside jurisdiction of Indonesia, which has legal effect within jurisdiction of Indonesia and/or outside jurisdiction of

	Amendment Law").	Indonesia and detrimental to the interest of Indonesia.	Indonesia and detrimental to the interest of Indonesia.
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic		

	Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information		

	Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation		
		no express territorial scope, but would require some nexus to the jurisdiction	other
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)		
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and		

	Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		

12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No.		

	13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation	Representatives of controllers or processors not established in the country
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	
2	Implementing regulation of PDP Law	
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").	
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")	
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")	
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)	
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")	
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40	
9	Information and Electronic Transaction Law No.19 of 2016	
10	Law No. 7 of 1992 on Banking	
11	Law No. 36 of 2009 on Health	
12	Law No. 1 of 2023 on Criminal Code	

13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector	
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")	
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection	
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")	
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services	
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector	
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')	

Notification obligation

#	Regulation	Data breach notification to authorities	Data breach notification to affected individuals
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	In the event that a data breach occurs, the Controller is required to submit a written notification to the affected data subjects and the Indonesian DPA no later than three days from the occurrence of the data breach, pursuant to Article 46 of PDP Law. In certain circumstances, the data breach shall also be notified to the public if it disturbs public services and/or has a material impact on the public interest. Pursuant to Article 46(2) of PDP Law, the notification shall contain the following items: a. the disclosed data; b. the time and reason of the breach; and c. the remedy measure carried out by the Controller. Under the PDPL the notification to the data protection authority must be done within 72 hours (Article 46(1) of the PDPL).	In the event that a data breach occurs, the Controller is required to submit a written notification to the affected data subjects and the Indonesian DPA no later than three days from the occurrence of the data breach, pursuant to Article 46 of PDP Law. In certain circumstances, the data breach shall also be notified to the public if it disturbs public services and/or has a material impact on the public interest. Pursuant to Article 46(2) of PDP Law, the notification shall contain the following items: a. the disclosed data; b. the time and reason of the breach; and c. the remedy measure carried out by the Controller. Under the PDPL the notification to the data protection authority must be done within 72 hours (Article 46(1) of the PDPL).

2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")	there is a requirement for the ESO to notify any security incident to the law enforcement authorities and relevant ministry or supervisory, pursuant to Article 24(3) of GR 71/2019.	
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")	the ESO may electronically notify the data subject upon their consent, pursuant to Article 28 letter c of the MOCI Reg. 20/2016. Under MOCI Regulation 20, the data breach notification must be sent to the data subjects within 14 days after the data breach becomes known to the electronic system operator (Article 28(c)(4) of MOCI Regulation 20).	
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the		

	Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		

16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

Obligations of Data Fiduciaries

#	Regulation	Notification of data processing	registration of database
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	Article 46 (1) In the event of a failure to protect Personal Data, Mandatory Personal Data Controller written notification no later than 3 x 24 (three times twenty four) hours to: a. Personal Data Subject; And b. institution. (2) Written notification as referred to in paragraph (1) contains at a minimum:	※In general, the PDP Law does not require organisations to register or notify any governmental body for the processing activities of personal data. However, if an organisation (Indonesian or offshore) processes personal data through an electronic system (i.e., website or application), such organisation can be considered

		Personal Data disclosed; when and how Personal Data is disclosed; And handling and recovery efforts disclosure of Personal Data by the Data Controller Personal. (3) In certain cases, the Personal Data Controller is obliged inform the public about failure to protect personal data. Article 48 (1) The Personal Data Controller is a legal entity merge, split, takeover, amalgamation, or dissolution of a body legal mandatory notification transfer of Personal Data to Personal Data Subjects. (2) Notification of transfer of Personal Data as follows referred to in paragraph (1) is carried out before and after a merger, separation, takeover, consolidation, or dissolution of a legal entity. (3) In the event that the Personal Data Controller is an entity the law carries out dissolution or dissolution, storage, transfer, Destruction of Personal Data is carried out in accordance with the provisions of the legislation. (4) Storage, transfer, deletion, or the destruction of Personal Data as intended in paragraph (3) shall be notified to the Data Subject Personal. (5) Further provisions regarding procedures notification as intended in paragraph (l), paragraph (21, and paragraph (4) are regulated in the Regulations Government.	as an ESO – and accordingly, is subject to obtain an ESO registration certificate under the EIT regulatory framework. Failure to conduct this registration is subject to an administrative sanction in the form of blocking access to the electronic system by the MOCI. The ESO registration certificate process is completed online through an Online Single Submission ("OSS") system, an integrated electronic system for the implementation of licensing in Indonesia.
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on		

	Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunicati on (the		

	"Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer		

	Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation	Data protection impact assessment	Others
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)		Under the PDP Law, the processing of children's personal data requires the consent of their parent or guardian.
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		

4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		

10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective		

	Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation		
		technical and organisational measures	Purpose Limitation
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	Article 39 (1) Personal Data Controllers are obliged to prevent Personal Data accessed unauthorizedly. (2) Prevention as intended in paragraph (1) carried out with a security system regarding Personal Data that is processed and/or processing system Personal Data electronics reliably, safely and responsibly answer. (3) Prevention as intended in paragraph (21 carried out in accordance with regulatory provisions legislation.	
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second		

	Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic		

	Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information		

	Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation		
		Accuracy	Retention Limitation
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)		
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and		

	Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		

12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No.		

	13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation	drawing up of codes of conduct	record of processing activities
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)		Article 31 Personal Data Controllers are required to carry out recording regarding all Personal Data processing activities.
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on		

	Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public		

	Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of		

	Vital Information Infrastructure ('PR No. 82/2022')		

#	Regulation	Designation of the data protection officer	Others
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	An organisation is required to appoint a DPO if the following conditions apply: a. the data processing is carried out for the interest of public services; b. the nature, scope and/or purpose of the Controller's core activities require regular and systematic monitoring of personal data on a large-scale basis; and c. the core activities of the Controller consist of large-scale processing activities of sensitive personal data and/or personal data relating to criminal activities. An organisation may appoint the DPO from within or outside of the organisation, such as a consultant or lawyer, as long as such appointment is made based on professional qualities, expert knowledge, practice of personal data protection and the ability to fulfil the tasks. based on the MOCI Handbook of PDP Programme for DPOs issued in 2022 ("DPO Handbook"), the to-be-issued PDP Law's implementing regulation on the DPO will regulate a required certification for a DPO. Pursuant to Article 54 of the PDP Law, a DPO is responsible for: a. informing and providing advice to the Controller or the Processor in order to comply with the provisions of the PDP	

		Law; b. monitoring and ensuring compliance with the PDP Law and the policies of the Controller and Processor; c. providing advice on assessing the impact of personal data protection and monitoring the performance of the Controller and the Processor; and d. coordinating and acting as a liaison for issues related to the processing of personal data.	
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").		
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics		

	Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of		

	Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')		

Data Cross Boarder Dist

#	Regulation	Cross-border data transfer & Exceptions	Data localization

		Provisions for Transborder Data Transfer. What are the exceptions? (e.g., sufficient authorization, transfers based on contracts equivalent to Standard Contract Clauses (SCC) or Binding Corporate Rules (BCR), transfers based on corporate certification, etc.), Transborder transfer assessment (TIA)	Presence or absence of provisions, stipulations regarding the types of data that must be stored in the country
		Provisions for cross boarder data transfer	Provisions on requirement of localization; and Type of data required for localization
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	Article 56 of the PDP Law: 1. the sending party must ensure the recipient party's country/state has a personal data protection level that is equal to or higher than the provisions in the PDP Law (Article 56(2)); 2. if the requirement in 1. is not met, the sending party must ensure the existence of adequate and binding data protection (Article 56(3)); and 3. if the requirements in 1. and 2. are not met, the last option is to obtain consent from the data subject before conducting the cross-border transfer. However, the PDP Law exempts certain rights of the data subject in the interests of: national defense and security, law enforcement, state administration, supervision of the financial services sector, monetary sector, payment systems and financial system stability; or statistical and scientific research.	–
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions	Article 18A of the Second Amendment introduces a new article stating that an international electronic contract governing an electronic system provided by an ESO, which includes standardised clauses (klausula baku), must be	

	("EIT Law") ("Second Amendment Law").	governed by Indonesian law if one or all of the following conditions is satisfied: 1. the user of the electronic system comes from Indonesia and gives his/her consent within the Indonesian jurisdiction; 2. the electronic system is accessed from Indonesia; and/or 3. the ESO has a place of business or carries out business activities in the Indonesian territory (i.e., ESOs that actively targets the Indonesian market).	
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")	a. before the collection or transfer of personal data, an electronic system operator must obtain written consent of the personal data owner (i.e. data subject) for the purpose of processing3 his/her personal data; and b. all transfer of personal data outside Indonesia must be coordinated with MOCI by: (i) reporting to MOCI("MOCI Regulation 20/2016") the plan of transfer of personal data4, (ii) requesting advocacy from the government (e.g. having a consultation with the government)5, if required; and (iii) reporting to MOCI the implementation of such transfer.	Article 99 of GR 71 states that institutions holding "Strategic Electronic Data" must hold archives and must be connected to a specific data center (presumably one that is managed by the Government). Included in sectors stipulated as holder of "Strategic Electronic Data" are: energy, transportation, financial, healthcare, ICT, food, defense, and any other sectors stipulated by the Government. Article 99 (1) The Government determines Agencies or institutions that have strategic Electronic Data that must be protected. (2) Agencies or institutions that have strategic Electronic Data that must be protected as referred to in section (1) include those in: a. government administration sector; b. energy and mineral resources sector; c. transportation sector; d. financial sector; e. health sector; f. information and communication technology sector; g. food sector; h. defense sector; and i. other sectors as stipulated by

			the President. (3) Agencies or institutions that have strategic Electronic Data as referred to in section (1) shall make Electronic Documents and their electronic backup and connect them to certain data centers for data security purposes. (4) Further provisions regarding the obligation to make Electronic Documents and the electronic backup and to connect them to certain data centers as referred to in section (3) are regulated by a regulation of the head of the government agency in charge of cyber security affairs. •public bodies (such as central and regional executive, legislative, judicative bodies and any other bodies established pursuant to a statutory mandate); and (b) entities appointed by public bodies to operate electronic systems on their behalf. •A private ESO may manage, process and/or store electronic data or electronic system outside of Indonesia, pursuant to GR 71 and its implementing regulation, i.e. Regulation of Minister of Communication and Informatics No. 5 of 2020 on Private Electronic System Operators (Regulation 5).
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")	1. a report on the planned personal data transfer, listing the destination country, the recipient's name, the transfer date, and the purpose of the transfer (a form for this is provided by the MOCI); 2. an advocacy request to the government, such as consultation, if necessary; and 3. a report on the implementation of the personal	

		data transfer (a form for this is provided by the Ministry).	
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector		

14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure		

	('PR No. 82/2022')		

#	Regulation	Government Access
		National Security Law, Cybersecurity Law Provisions
		Provision allowed govt to access regulated data/to not comply to data regulation
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)	
2	Implementing regulation of PDP Law	
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").	Article 42 Investigation of criminal acts as intended by this Law shall be made under the provisions of the Law of Criminal Procedure and the provisions of this Law. Article 43 (1) In addition to Investigators of the State Police of the Republic of Indonesia, certain Civil Service Officials within the Government whose scope of duties and responsibilities is in the field of Information Technology and Electronic Transactions shall be granted special authority as investigators as intended by the Law of Criminal Procedure to make investigation of criminal acts of Information Technology and Electronic Transactions. (2) Investigation of Information Technology and Electronic Transactions as intended by paragraph (1) shall be made with due regard to privacy protection, secrecy, smooth public services, data integrity, or data entirety in accordance with provisions of Rules. (3) Searches and/or seizures of electronic systems suspiciously involved in criminal acts must be carried out with the permission of the local chief justice of the district court. (4) In carrying out searches and/or seizures as intended by paragraph (3), investigators are required to maintain the public service interests. (5) Civil Service Investigators as intended by paragraph (1) shall have the authority: a. to receive reports or complaints from Persons of the occurrence of criminal acts under the provisions of this Law; b. to summons any Person or other party for hearing and/or examination as suspects or witnesses in connection with suspected criminal acts in the field related to the provisions of this Law; c. to make examination of the truth of reports or inquiries into criminal acts under the provisions of this Law; d. to make examination of Persons and/or Business Entities that

		should be suspected of having committed criminal acts under this Law; e. to make inspection of equipment and/or facilities in connection with the activities of Information Technology suspected of having been used to commit criminal acts under this Law; f. to search certain places suspected of having been used as the place to commit criminal acts under the provisions of this Law; g. to seal and seize equipment and/or facilities of Information Technology activities suspected of having been used in a manner departing from provisions of Rules; h. to solicit assistance of experts necessary for investigation of criminal acts under this Law; and/or i. to cease investigation of criminal acts under this Law in accordance with the provisions of the prevailing law of criminal procedure. (6) To make arrest and detention, investigators through public prosecutors are required to seek order of the local chief justice of the district court within a period of twenty-four hours. (7) Civil Service Investigators as intended by paragraph (1) shall coordinate with Investigators of the State Police of the Republic of Indonesia to notify the commencement of investigation and deliver the results thereof to public prosecutors. (8) In the framework to uncover criminal acts of Electronic Information and Electronic Transactions, investigators may cooperate with investigators of other countries to share information and means of proof.
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")	Under GR 71 and Regulation 5, Indonesian regulators have the authority to request a private ESO (including foreign private ESOs) to grant the Ministry of Communications and Informatics (MOCI) access to the ESO's electronic systems and electronic data which relate to Indonesian citizens or legal entities.
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MOCI Regulation 20/2016")	
6	Regulation of the Minister of Communication and Informatics	

	Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)	
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")	Under GR 71 and Regulation 5, Indonesian regulators have the authority to request a private ESO (including foreign private ESOs) to grant the Ministry of Communications and Informatics (MOCI) access to the ESO's electronic systems and electronic data which relate to Indonesian citizens or legal entities.
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40	
9	Information and Electronic Transaction Law No.19 of 2016	
10	Law No. 7 of 1992 on Banking	
11	Law No. 36 of 2009 on Health	
12	Law No. 1 of 2023 on Criminal Code	
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector	
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of	

	Financial Products and/or Services ("OJK Consumer Protection Regulations")	
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection	
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")	
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services	
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector	
19	President Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure ('PR No. 82/2022')	

Penalties

#	Regulation	Corporate Punishments	Individual Punishments
		Forms of penalties (e.g., recommendations for corrective	Penalties (penalties, fines, demotion, etc.)

		action, public penalties, fines, confiscation of assets and income, data deletion, data processing, business suspension, etc.)	
		Forms of penalties on corporate	Forms of penalties on individual
1	Law No. 27 of 2022 on Personal Data Protection (PDP Law)		
2	Implementing regulation of PDP Law		
3	Law No. 1/2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law") ("Second Amendment Law").	Article 52 (4) Criminal acts as intended by Article 27 through Article 37 committed by corporations shall be sentenced to the basic sentence plus two-thirds.	Article 45 (1) Any Person who satisfies the elements as intended by Article 27 paragraphs (1), (2), (3), or (4) shall be sentenced to imprisonment not exceeding 6 (six) years and/or a fine not exceeding Rp1,000,000,000 (one billion rupiah). (2) Any Person who satisfies the elements as intended by Article 28 paragraph (1) or paragraph (2) shall be sentenced to imprisonment not exceeding 6 (six) years and/or a fine not exceeding Rp1,000,000,000,- (one billion rupiah). (3) Any Person who satisfies the elements as intended by Article 29 shall be sentenced to imprisonment not exceeding 12 (twelve) years and/or a fine not exceeding Rp2,000,000,000 (two billion rupiah). Article 46 (1) Any Person who satisfies the elements as intended by Article 30 paragraph (1) shall be sentenced to imprisonment not exceeding 6 (six) years and/or a fine not exceeding Rp600,000,000 (six hundred million rupiah). (2) Any Person who satisfies the elements as intended by Article

			30 paragraph (2) shall be sentenced to imprisonment not exceeding 7 (seven) years and/or a fine not exceeding Rp700,000,000 (seven hundred million rupiah). (3) Any Person who satisfies the elements as intended by Article 30 paragraph (3) shall be sentenced to imprisonment not exceeding 8 (eight) years and/or a fine not exceeding Rp800,000,000 (eight hundred million rupiah). Article 47 Any Person who satisfies the elements as intended by Article 31 paragraph (1) or paragraph (2) shall be sentenced to imprisonment not exceeding 10 (ten) years and/or a fine not exceeding Rp800,000,000 (eight hundred million rupiah). Article 48 (1) Any Person who satisfies the elements as intended by Article 32 paragraph (1) shall be sentenced to imprisonment not exceeding 8 (eight) years and/or a fine not exceeding Rp2,000,000,000 (two billion rupiah). (2) Any Person who satisfies the elements as intended by Article 32 paragraph (2) shall be sentenced to imprisonment not exceeding 9 (nine) years and/or a fine not exceeding Rp3,000,000,000 (three billion rupiah). (3) Any Person who satisfies the elements as intended by Article 32 paragraph (3) shall be sentenced to imprisonment not exceeding 10 (ten) years and/or a fine not exceeding Rp5,000,000,000 (five billion

			rupiah). Article 49 Any Person who satisfies the elements as intended by Article 33 shall be sentenced to imprisonment not exceeding 10 (ten) years and/or a fine not exceeding Rp10,000,000,000 (ten billion rupiah). Article 50 Any Person who satisfies the elements as intended by Article 34 paragraph (1) shall be sentenced to imprisonment not exceeding 10 (ten) years and/or a fine not exceeding Rp10,000,000,000 (ten billion rupiah). Article 51 (1) Any Person who satisfies the elements as intended by Article 35 shall be sentenced to imprisonment not exceeding 12 (twelve) years and/or a fine not exceeding Rp12,000,000,000 (twelve billion rupiah). (2) Any Person who satisfies the elements as intended by Article 36 shall be sentenced to imprisonment not exceeding 12 (twelve) years and/or a fine not exceeding Rp12,000,000,000 (twelve billion rupiah).
4	Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("GR 71/2019")		
5	Minister of Communication and Informatics ("MOCI") Regulation No. 20 of 2016 on Personal Data		

	Protection in Electronic Systems ("MOCI Regulation 20/2016")		
6	Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)		
7	MOCI Regulation No. 5 of 2020 on Electronic System Organizers ("ESO") in the Private Sector ("MOCI Regulation 5/2020")		
8	Law No. 36 of 1999 on Telecommunication (the "Telecommunication Law") Section 40		
9	Information and Electronic Transaction Law No.19 of 2016		
10	Law No. 7 of 1992 on Banking		
11	Law No. 36 of 2009 on Health		
12	Law No. 1 of 2023 on Criminal Code		
13	the Financial Services Authority ("OJK") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the		

	Financial Services Sector		
14	OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services ("OJK Consumer Protection Regulations")		
15	the Bank Indonesia ("BI") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection		
16	BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection ("BI Consumer Protection Regulations")		
17	the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services		
18	the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector		
19	President Regulation No. 82 of 2022 on the Protection of Vital Information		

	Infrastructure ('PR No. 82/2022')		

D) Lao PDR

Legal system overview

#	Regulation	Translation	Purpose of the Legal System
			What purpose does the legal system serve? (e.g. cybersecurity)
		Google translation or Translation by certain organization	
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	Translation by certain organization	Article 1 Purpose The law on Electronic Data Protection defines the principles, regulations and measures regarding to the administration, monitoring, inspection and activation of Electronic Data Protection in order to ensure the collection, accessing, usage, and disclosing of data are safe and correct. It is also focused on the protection of rights and benefits of the state, individual, legal entities or organizations; and it aims to contribute in Socio-Economic Development of the nation, ensures the stability of the nation, peace and orderliness of the society.
			Article 4 Government Policies on Electronic Data Protection The government considers Electronic Data Protection as one of the most important tasks in order to ensure the use of data are in security and limit of taking individual, legal entities or organizations data to use and disclose in public without permission. The government supports and promotes Electronic Data Protection by facilitating, providing budget, building infrastructure, human resource

			development, researching and using modern technology for efficient and effective performance. The government supports and enhances domestic and international individual, legal entities or organizations to contribute and investment on Electronic Data Protection.
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015	Translation by certain organization	Article 1 Objectives This Law determines the principles, regulations and measures regarding the management, monitoring of cybercrime resistance and prevention activities in order to enable the effectiveness of such activities with the aim to resist, prevent, restrain and eliminate the crime, to protect database system, server system, computer data and to guarantee the security of the nation, the peace and orderliness of the society, the ability to link with regional and international network, and to contribute in the protection and development of the national socio-economic in a progressive and sustainable manner.
			Article 2 Cybercrime Resistance and Prevention Cybercrime is a wrongful act in the computer system that cause the loss to the state, individuals, legal entities, organizations and society based on the behavior specified in Article 8 of this Law. Cybercrime resistance and prevention is an activity to restrain, eliminate, suppression of individuals, legal entities and organizations that have direct rights and duties in finding out and implementing the cybercrime resistance and prevention activities as specified in Article 19 and 24 of this law.
			Article 4 Government Policy on Cybercrime Resistance and

			Prevention Activities The state encourages the computerized system to be used in a safe, convenient, quick and fair manner as well as to protect the legitimate rights and interests of service provider, service users of computerized system and computer data in accordance with the laws and regulations. The state sets condition and facilitates the implementation of the cybercrime resistance and prevention activities through the provision of budget, builds and recruits personnel, vehicles, equipment, study and apply modern technology, build infrastructure to enable the effectiveness of such activities. The state considers cybercrime resistance and prevention as main activities and problem solving as significant tasks. The state encourages and promotes individuals, legal entities and organizations (both domestic and foreign) to invest in the production in terms of technique and technology as well as to participate in cybercrime resistance and prevention activities.
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018	Google translation	Chapter 1 Purpose This guideline expands and recommends the implementation of some clauses in some articles of the Law on the Protection of Electronic Information, No. 25/NPC, dated May 12, 2017 in order to make the content of the law more detailed and clear by further explaining the technical technical content as well as giving examples to make it easy to understand in use, aiming to make the implementation of the law easy, efficient, effective and uniform throughout the country.

4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018	Google translation	Chapter 1 Purpose This guide expands and recommends the implementation of some articles of the Law on Combating and Suppressing Cybercrime, No. 61/SPO, dated July 15, 2015 in order to make the content of the said law more detailed and clear by further explaining the content of technical and technical characteristics, behavior that is systematic crime as well as giving examples to make the computer easy to understand in order to make the implementation of the law accurate, efficient, effective and uniform. in the entire country.
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018	Google translation	Article 1 Objective This law defines the principles, regulations and measures regarding the management and monitoring of electronic work in order to make such work accurate, up-to-date, modern, safe and fast, with the aim of protecting the rights and interests of the state, individuals, legal entities and organizations, ensuring national security, peace and social order, being able to link with the region and internationally to contribute to the socio-economic development of the nation
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012	Translation by certain organization	Article 1 Purpos This Law defines the principles, regulationsand measures for the formation, use, recognition, management and inspection of electronic transactions to create reliability and confidence in electronic transactions aiming atprotecting the legitimate rights and interests ofthose who are doingelectronic commerce, and ensure the use, promotion of electronic transactions, modernization, regional and

			international integration contributing to socio-economic development while preserving national stability, social peace, order and justice.
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017	Translation by certain organization	Article 1 Objectives This Decision determines the principles of fine measures as set forth in article 60, under the Law On Resistance and Prevention of Cybercrime, involves with deleting data in computerized system, providing incorrect computer data, failing to provide computer data and other behaviors that impede, and not cooperate with, police officers on investigation. Aiming to build the peace and orderliness of the society, and contribute to the national socio-economic development in a progressive manner.
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017 / Instruction on Computer Safety	Translation by certain organization	Objectives. This instruction is aimed to roll out the content in article 24 of the Law on the Prevention and Defense of Cybercrime that relating to the specific measures on governing computer safety in order for the creation, prevention, management, surveillance and monitor on computer safety are united throughout the country.
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014	Translation by certain organization	Article 1: Function of the Decree This decree defines the principles, regulations and measures for managing information on the Internet to promote national stability, peace and social order. It is focused on protecting the integrity of and benefits to be derived by service providers, service users, and society in order to contribute to national development.
10		Google translation	Article 1 Objective This decree defines the

	Decree on E-commerce No. 296/GOV		principles, regulations and measures regarding the management, monitoring and inspection of electronic wording work in order to make such work developed, modern, safe and reliable, aimed at protecting the rights and legitimate interests of customers and electronic merchants, able to link with the region and internationally, to contribute to the economic-social development of the nation,
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020	Google translation	Article 1 Objective This decree defines the principles, regulations and measures regarding the management and inspection of financial service users' protection in order to make financial services quality, accurate, transparent and fair with the aim of building confidence in the financial system and contributing to the socio- economic development of the nation.
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012	Translation by certain organization	Article 1. Objective This Decision determines the rules and principles on the credit information activities of the Bank of the Lao PDR, commercial banks and financial institutions to maintain, report the customer's credit information in order to provide such information to the members of the Information Center which is aimed at reducing and limit the potential risk in providing loan of commercial banks and financial institution.
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018	Translation by certain organization	Article 1 Objectives This Decision determines principles, regulations, [and] management methods and facilitation toward providing the

			credit information in order to make a user able to access to the credit information systematically, conveniently and safety.
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020	Google translation	Article 1 Purpose This agreement defines the principles, regulations and measures regarding the management of services, the use of electronic signatures to promote business operations to be orderly, correct, standardized, modern, safe and fast, aimed at protecting the rights and interests of the state, individuals, legal entities and organizations, ensuring national security, peace and social order, and contributing to the socio-economic development of the nation.
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016	Google translation	Article 1 Objective This decree defines the principles, regulations and measures in the creation, use, maintenance, development and management of information centers through the Internet in order to develop such work in a systematic, efficient, effective, economical, modern and connected manner with the aim of contributing to the development of the economy and society.
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020	Google translation	Article 1 Purpose This agreement defines the principles, regulations and measures related to the management, monitoring, inspection, activity of protection of service users in order to make telecommunication and internet services of quality, standard, transparent, fair, convenient, fast, aiming to guarantee the rights and benefits of service users, to make society peaceful and contribute to socio-economic development.

17	Decree on Credit Information No 224/GOV dated July 19, 2019	Google translation	Article 1 Objective This decree defines the principles, regulations and measures related to the management, monitoring and inspection of credit information activities in order to make the work efficient and effective, to ensure the reduction of credit risk of financial institutions, to promote access to sources of capital aimed at maintaining financial stability and the implementation of monetary policy to be stable and contribute to the socio-economic development of the nation.
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016	Google translation	Article 1 Objective This law defines the principles, regulations and measures related to management. Monitor the use and development of information communication technology to ensure that the work is developed in a systematic, quality, modern, fast, safe manner and promote this work in all sectors to be effective in order to protect the rights and benefits of the state, individuals, legal entities and organizations, the nation is stable, the society is peaceful, orderly and fair, able to link with the region and internationally to contribute to the socio-economic development of the nation.
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021	Google translation	Article 1 (Amendment) Purpose This law defines the principles, regulations and measures regarding the management and monitoring and inspection of telecommunication work so that the work is efficient, quality, universal, convenient, fair, continuously developed and modernized with the aim of ensuring the stability and security of the nation, able to link with the region and internationally to contribute to

			the socio-economic development of the nation.
20	The Penal Code No.26/NA datd May 17, 2017	Translation by certain organization	Article 1 Role of the Penal Code The Penal Code intends to safeguard the political, economic and social regimes of the Lao PDR, to protect interests of the State, the legitimate rights and interests of citizens, the life, health, dignity, rights and freedom of Lao people, national security and social order; to prevent and counter offences; and to teach all citizens to be aware of the laws. In order to fulfill this role, the Penal Code defines certain acts which endanger the public as criminal offences and establishes penalties for the perpetrator(s).

#	Regulation	Form of legal system	Target Business
		Is it introduced in accordance with government ordinances and guidelines? (Is it introduced in a format that ensures lead time?)	Does the law target specific industry or in general? Is it clearly stated in the regulations?
		Regulation level	Industry
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	Law	General
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015	Law	Telecommunication
3	Guideline on the implementation of the Law on Electronic Data Protection no.	Guideline	General

	2126/MPT, dated 8 August 2018		
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018	Guideline	Telecommunication
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018	Law	General
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012	Decree	General
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017	Decision	Telecommunication
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017 / Instruction on Computer Safety	Guidelines	Telecommunication
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014	Decree	Telecommunication
10	Decree on E-commerce No. 296/GOV	Decree	Commerce
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020	Decree	Finance

12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012	Decision	Finance
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018	Decision	Finance
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020	Decision	General
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016	Decree	Telecommunication
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020	Decision	Telecommunication
17	Decree on Credit Information No 224/GOV dated July 19, 2019	Decree	Finance
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016	Law	Telecommunication
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021	Law	Telecommunication

20	The Penal Code No.26/NA datd May 17, 2017	Law	General

#	Regulation	Regulatory authority	Jurisdiction
		Which regulatory authority has jurisdiction over regulation?	Cyber security, data security, personal information protection, etc.
		Name of ministry/organization	Similar to purpose?
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	Article 40 Administration Organization of Electronic Data Protection The government is an administration center of Electronic Data Protection and unity throughout the country which the Ministry of Posts and Telecommunication is a key person in responsible and coordination with line ministries, Government Organizations equivalence to the ministry, Local Authorities, and other relevant sectors are implemented. The Electronic Data Protection Administration Organizations comprise of: 1. Ministry of Posts and Telecommunication; 2. Provincial, and Capital Department of Posts and Telecommunication; 3. Posts and Telecommunication Office of District, Municipality, City.	Data security
		Article 41 Rights and Duties of Ministry of Posts and Telecommunication Regarding to the administration of Electronic Data Protection, the Ministry of Posts and Telecommunication has the following rights and duties: 1. Research, create policy, strategy plan, laws and regulations regarding to the Electronic Data Protection in order to propose to the government for consideration; 2. Develop policy, strategy plan, and laws to be a plan, scheme	

		and project that relating to Electronic Data Protection and implement; 3. Advertise, disseminate, and educate laws and regulations that relating to Electronic Data Protection throughout the country; 4. Guide, administrate, monitor, and inspect the administration; implementation of Laws and regulations that relating to Electronic Data Protection; 5. Research, create, and use the technical standard of data security; 6. Administrate certification system of national electronic security code; 7. Inspect the gap regarding to data security system; 8. Create, upgrade, and develop human resource regarding to Electronic Data Protection; 9. Consider and solve the proposals that relating to electronic data; 10. Coordinate with line ministries that relating to electronic data protection; 11. Relate and coordinate with foreign countries, regional and international regarding to Electronic Data Protection; 12. Regularly summarize and report Electronic Data Protection activities to the government; 13. Apply other rights and duties as specified in the law.	
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015	Article 48 Management Authority The Government is in charge of managing the cybercrime resistance and prevention activities in a centralized and uniformed manner throughout the country by assigning the Ministry of Post and Telecommunication to directly responsible for and to take initiative in collaborating with the Ministry of National Defense, Ministry of Public Security,	Cybercrime.

		Ministry of Information, Culture and Tourism, Ministry of Sciences and Technology, other ministries and local administration concerned. The Authority in charge of the management of cybercrime resistance and prevention activities comprises of: 1. Ministry of Post and Telecommunication; 2. Division of Post and Telecommunication of provincial, city level; 3. Office of Post and Telecommunication at district, municipality level.	
		Article 49 Rights and Duties of the Ministry of Post and Telecommunication In the management of cybercrime prevention activities, the Ministry of Post and Telecommunication shall have the rights and duties as follows: 1. To study, build strategic plan, policy, law related to cybercrime resistance and prevention activities in order to propose to the Government for consideration; 2. To propagate, disseminate the laws and regulations relating to cybercrime resistance and prevention activities across the country; 3. To guide capacity building, training, upgrading and development of personnel on the safety of the computerized system; 4. To guide the safeguarding, monitoring, inspect, advise, warn and response to computerized system emergencies; 5. To coordinate with ministries, authority concerned in performing activities related to cybercrime resistance and prevention; 6. To contact, cooperate with foreign countries, regional and	

		international levels about cybercrime resistance and prevention; 7. To brief and report its activities to the Government on a regular basis; 8. To exercise such other rights and to perform such other duties as specified in the laws and regulations.	
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018	Ministry of Posts and Telecommunications	Data protection
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018	Ministry of Posts and Telecommunications	Cybercrime
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018	Article 68 Organizations for the management of items such as electronics The government is in charge of electronic affairs in a centralized and uniform way throughout the country by assigning the Ministry of Posts, Telecommunications and Communications to be directly responsible and to coordinate with relevant ministries, agencies and local government agencies. Electronic signature management organization consists of: 1. Ministry of Posts, Telecommunications and Communications; 2. Department of post, telecommunication and communication of the province, capital.	Personal data protection
		Article 69 Rights and duties of the Ministry of Posts, Telecommunications and Communications	

		In managing electronic signatures, the Ministry of Posts, Telecommunications and Communications has the following rights and duties: 1. Research and create policies, strategies and laws on electronic signature work to present to the government for consideration; 2. Develop policies, strategies and laws related to electronic work as plans, programs, projects and implementation; 3. Advertise, publish and educate about policies, strategies, laws about work Electronic signature events in the country; 4. Research and set technical standards, issue regulations on management and service of issuing electronic signature certificates; 5. Create, train and upgrade personnel related to electronic signature work: 6. Investigate and consider issuing, renewing, suspending or revoking business licenses to provide electronic signature certification services; 7. Manage, evaluate and inspect the issuance and use of electronic signature certificates nationwide; 8. Proposing to suspend or cancel the electronic signature certificate; 9. Provide advice and guidance on the issuance and use of electronic signature certificates of state organization. 10. Receive and consider and correct proposals regarding electronic signature work; 11. Coordinating with relevant ministries, organizations and local governments in organizing Set up electronic signature tasks, 12. Interact and cooperate with foreign countries on electronic signature work;	

		13. Summarize and report activities such as electronics to the government regularly; 14. Use the rights and perform other duties as defined in the law.	
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012	Article 46 Management Organizations The Government shall centrally and uniformly manage electronic transactions throughout the country by designating the Ministry of Science and Technology to be responsible for [its] management by coordinating with other relevant sectors and relevant local administrations under their jurisdictions. The management organizations are as follows: 1. The Ministry of Science and Technology; 2. Provincial [and] Capital Departments of Science and Technology; 3. The District [and] Municipal Offices of Science and Technology; 4. Village Units of Science and Technology.	Personal Data Protection / data protection?
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017	Ministry of Posts and Telecommunications	Cyber crime
		Article 47 Rights and Duties of the Ministry of Science and Technology For the purpose of managing electronic transactions, the Ministry of Science and Technology shall have the following rights and duties: 1. to establish policies, strategic plans, programs and plans regarding the development of electronic transaction activities to propose to the government for approval; 2. to conduct research, develop and amend laws, regulations and other legislation concerning electronic transaction activities;	

		3. to disseminate laws and relevant legislation with regard to electronic transaction activities; 4. to issue, suspend and withdraw permits and maintain a list of digital signature certificate providers according to its responsibility; 5. to consider and resolve proposals with regard to the electronic transaction activities according to its responsibility; 6. to upgrade and improve capacity of personnel of both public and private sectors involved in electronic transactions; 7. to consider standards and methods for the protection and resolving of problems that may occur in electronic transactions according to the proposal of the Provincial [and] Capital Departments of Science and Technology; 8. to supervise [and] monitor the implementation of electronic transaction activities throughout the country; 9. to maintain confidentiality of data messages and electronic records that give rise to damage to national stability, security and social order; 10.to coordinate with other ministries or organizations and local administrations involving the implementation of electronic transaction activities; 11.to carry out international relations activities regarding electronic transaction; 12.to regularly summarize and report activities regarding electronic transaction to the Government; 13.to implement other rights and duties as defined in the laws and regulations.	
8	Guidelines on Computer	Ministry of Posts and Telecommunications	Cyber crime

	Systems Security No. 3623, dated 11 December 2017 / Instruction on Computer Safety		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014	Ministry of Posts and Telecommunications. Article 18: The Responsibilities of Post, Telecommunication, and Communication Sector Regarding information management on the Internet, the Post, Telecommunication, and Communication Sector shall have the following responsibilities: 1. Publicize and disseminate policies, strategic plans, regulations and laws on the management of information on the Internet; 2. Monitor and inspect the service of Internet service providers, and the dissemination of information of Internet service users; 3. Issue orders to Internet service providers to restrain accessing information, temporarily or permanently suspend connection of those who violate this decree or other related regulations and laws; 4. Receive and consider the requests from service provider, service users, and societies about dissemination of information on the Internet; 5. Collaborate with concerned officers in following us and searching for people who disseminate information that violates this decree or other related regulations and laws; 6. Summarize and report the results of implementing this decree to the government regularly.	Shared information on social media
10		Article 50 Electronic Commerce Management Agency	Data protection

	Decree on E-commerce No. 296/GOV	The Ministry of Industry and Trade, the Ministry of Technology and Communications, the Bank of Lao PDR and the Ministry of Finance are responsible for the implementation of this decree in coordination with the Ministry, equivalent state agencies and relevant local government agencies to manage and implement the work of electronic communications.	
		Article 51 Rights and duties of the Ministry of Industry and Trade In the management of electronic commerce, the Ministry of Industry and Trade has the right and the following duties: 1. Research, create policies, strategic plans, development plans, legislation and measures on electronic commerce to present to the government for consideration; 2. Develop policies, strategic plans, development plans, legislation and measures related to electronic commerce and implementation; 3. Advertise, publish policies, strategies, development plans, legislation and measures related to electronic commerce to the relevant parties and society in general to: 4. Consider issuing business licenses and certificates of recognition, suspension or termination of operations conduct electronic commerce business; 5. Develop, improve and maintain the electronic trade database system; 6. Receive and consider resolving proposals regarding electronic commerce disputes; 7. Encourage and promote the use of electronic communication; 8. Coordinate with related organizations to encourage the establishment of electronic commerce associations in Lao	

		PDR; 9. Summarize the collection of electronic wording statistics; 10. To be a point of coordination, cooperation and negotiation of electronic trade with foreign countries; 11. Coordinate with ministries, government agencies equivalent to ministries, and local government agencies to organize work related to electronic commerce; 12. Divide the responsibilities, direct and monitor the implementation of electronic commerce according to their vertical lines throughout the country; 13. Summarize and report the implementation of electronic commerce work to the top on a regular basis; 14. Use rights and perform other duties according to laws and regulations.	
		Article 52 Rights and duties of the Ministry of Technology and Communication In the management of electronic commerce, the Ministry of Technology and Communication has the right and the following duties: 1. Research, create policies, strategic plans, development plans, legislation and measures on electronic commerce within the scope of their role to present to the government for consideration; 2. Research, create policies, strategic plans, development plans, legislation and measures related to ICT, telecommunications and digital work such as electronic signatures, electronic data protection and computer crime prevention to ensure a safe environment for conducting electronic business transactions; 3. Promote and develop postal, telecommunication and modern information technology products and services conducive to the growth of electronic commerce;	

		4. Consider issuing, suspending or revoking technical standards certificates of electronic commerce channels; 5. Coordinate with the Ministry of Industry and Trade and other related sectors to promote and encourage business units to use electronic commerce; 6. Coordinating with the Ministry of Industry and Trade and other related sectors to consider resolving electronic trade disputes, compiling electronic trade statistics and implementing cooperation with foreign countries in the framework of electronic trade; 7. Use rights and perform other duties according to laws and regulations.	
		Article 53 Rights and duties of the Bank of the Lao PDR In the management of electronic commerce, the Bank of Lao PDR has the right and Duties as follows: 1. Research, create policies, development plans, legislation and measures on the work of the payment system to support electronic commerce to present to the government for consideration; 2. Promote and develop a modern payment system to facilitate the growth of electronic commerce; 3. Propose to the Ministry of Industry and Trade to suspend or cancel the business license or recognition certificate of merchants who do not use payment tools or payment media of payment service providers that are not authorized by the Bank of Lao PDR to pay for goods and services; 4. Coordinate with the Ministry of Industry and Trade and other related sectors to collect statistics, resolve disputes, cooperate with foreign countries and monitor payment activities that provide services	

		for electronic commerce; 5. Use rights and perform other duties as defined in regulations and laws	
		Article 54 Rights and duties of the Ministry of Finance In managing electronic commerce, the Ministry of Finance has the following rights and duties: 1. Research, create, update, strategy, legislation on electronic commerce within the scope of its role to present to the government for consideration; 2. Develop policies, strategies and legislation on electronic commerce to become plans, programs or projects and implement them on the basis of coordination with the Ministry of Industry and Trade and related parties; 3. Manage, monitor, inspect the implementation of tax obligations and taxes according to laws and regulations; 4. Propose to the Ministry of Industry and Trade to suspend or cancel the business license or recognition certificate of those who do not fulfill tax obligations or other obligations as stipulated in the law on taxes; 5. Use the rights and perform other duties as stipulated in the law and regulations.	
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020	Article 30 Management and Inspection Agency for the Protection of Financial Service Users The Bank of Lao PDR is directly responsible and in charge of coordinating with the Ministry, equivalent state agencies, local government agencies and other related parties in managing and organizing the protection of financial service users.	Personal data protection
		Article 31 Rights and duties of the Bank of the Lao PDR In managing and supervising the protection of financial service users, the Bank of Lao PDR has	

		the following rights and duties: 1. Research and create strategic plans, legislation on the protection of users of financial services; 2. Create and implement a plan to protect users of financial services as well publicity to inform the public; 3. Create mechanisms and methods to resolve user suggestions; 4. Collect information, monitor, inspect and evaluate the implementation of financial service user protection; 5. Request service providers to report or provide information in the event of any incident or condition that occurs related to the protection of financial service users; 6. Publish a report on the results of the protection of users of technical services money; 7. Provide financial knowledge to the society with appropriate forms including providing information about it with financial services; 8. Inspect the protection of financial service users, including the activities of the units or employees responsible for the protection of financial service users of service providers; 9. Notify the service provider to improve the service or wrong actions: 10. Use measures against violators according to relevant laws and regulations; 11. Coordinate with relevant parties on the protection of financial service users; 12. Summarize and report the activity of protection of users of financial services to the government on a regular basis; 13. Exercising rights and performing other duties according to law.	
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated	Article 22. The Implementation The CIC of the Bank of the Lao PDR and its members shall strictly implement this Decision.	Credit information

	20 September 2012		
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018	Bank of the Lao PDR	Credit information
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020	Article 57 Rights and duties of the Ministry of Posts, Telecommunications and Communications In the management of electronic activities, the Ministry of Posts, Telecommunications, and Communications has the following rights and duties: 1. Publish laws and regulations on electronic signatures; 2. Consider approving, renewing, changing, suspending and revoking the electronic signature certification service license; 3. Monitor and inspect the implementation of conditions, standards, quality and regulations according to the agreement This version: 4. Warn, educate or fine those who violate laws and other related regulations; 5. Consider modifying the proposal regarding electronic signature services such as quality provision of services and services; 6. Collect fees and service charges for issuing licenses to provide electronic signature certificates Tonics and other service charges according to laws and regulations; 7. Perform other duties as prescribed by laws and regulations	Data security / Data proection
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016	Article 28 Preventing and solving security problems of information centers through Internet The Ministry of Posts, Telecommunications and Communications is the center to coordinate with the relevant parties in surveillance,	Data center

		monitoring, inspection, warning and solving problems that occur with the information center through the Internet and electronic information in both the public and private sectors. Individuals, legal entities or organizations to cooperate and facilitate the prevention and resolution of information center security issues through the Internet and electronic information	
		Article 54 Rights and duties of the Ministry of Posts, Telecommunications and Communications The Ministry of Posts, Telecommunications and Communications has the following rights and duties: 1. Research policies, strategic plans and legislation on information center work through the Internet to propose to the government for consideration; 2. Organize and develop policies, strategic plans and legislation on data center work Information through the Internet is a detailed plan, program and project as well as implementation; 3. Advertise, disseminate policies, strategic plans, legislation and plans regarding the work of the Information Center through the Internet widely; 4. Manage the creation and use of information centers through the Internet throughout the country; 5. To be a point of coordination with government organizations in creating, using and developing information centers Internet news; 6. Investigate issuing, extending, suspending, changing and revoking the license to operate in the private sector Internet Information Center;	

		7. Research and set standards, issue guidelines and regulations regarding the management and service of information centers through the Internet; 8. Evaluate and inspect the creation and use of public and private Internet information centers; 9. Provide advice and guidance on the creation and use of information centers through the Internet, the implementation of plans for the creation and development of information centers through the Internet and the use of technology in Loci to communicate information of government organizations; 10. Advise and lead the implementation of computer system information security protection; 11. Coordinating with relevant ministries, organizations and local government agencies in the organization and implementation of information centers through the Internet; 12. Summarize and report the activities of the information center through the Internet to the government regularly; 13. Use rights and perform other duties as defined in laws and regulations.	
16	Decision on consumer protection for telecommunicati on and Internet service No. 1061/MPT, dated 25 May 2020	Article 12 Postal, telecommunications and communication sectors The Telecommunications Regulatory Agency, Department of Posts, Telecommunications and Communications of the province, the capital will receive and consider the proposals regarding the protection of users of telecommunications services and the Internet according to the rules and procedures set forth in this agreement. Post Office, Telecommunication and Communication District,	consumer protection in telecommunication service. (not data protection)

		Municipality is the recipient of proposals regarding the protection of users of telecommunication and Internet services to the Department of Post, Telecommunication and Communication to consider and amend the rules and procedures set forth in this agreement	
		Article 13 Rights and duties of the Ministry of Posts, Telecommunications and Communications In managing the protection of service users, the Ministry of Posts, Telecommunications and Communications has the following rights and duties: 1. Research, create and update various legislations on the protection of service users to suit the The state of economic-social development from time to time; 2. Receive and consider to modify the proposals regarding the protection of service users: 3. Advertise, publish and train about the protection of service users; 4. Organize a seminar, discuss and exchange opinions on the protection of service users 5. Supervise the Department of Posts, Telecommunications and Communications in the province and capital regarding the protection of service users; 6. Liaise and cooperate with foreign countries on the protection of service users; 7. Summarize and report the implementation of service user protection work to the government; 8. Live use and perform other functions as defined in the law and regulations.	
17	Decree on Credit Information No 224/GOV dated July 19, 2019	Article 43 Rights and duties of the Bank of the Lao PDR In managing credit information, the Bank of Lao PDR has the	Credit information

		following rights and duties: 1. Approve the strategic plan, policy on credit information management and credit information system development plan; 2. Research, create and issue legislation on credit information work; 3. Monitor and inspect the activities of credit information companies; 4. Coordinating with relevant parties to promote the activities of information and moral work believe; 5. Summarize and report credit information activities to the government normal; 6. Use rights and perform other duties according to the law.	
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016	Article 56 Rights and duties of the Ministry of Posts, Telecommunications and Communications In managing information and communication technology, the Ministry of Posts, Telecommunications and Communications has the following rights and duties: 1. Research, create strategic plans, policies and laws regarding information and communication technology work to present to the government for consideration: 2. Develop strategic plans, policies and laws into plans, programs and projects for implementation; 3. Advertise, disseminate laws, regulations and guidelines on information and communication technology throughout the country; 4. Create, upgrade, develop human resources in media technology work Information Court; 5. Investigate issuing, extending, suspending, changing, withdrawing and canceling business licenses related to information communication technology; 6. Permission to use	Information communication technology. Data disclosure

		telecommunications resources such as Internet numbers; 7. Inspect, verify technical standards	
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021	Ministry of Posts, Telecommunications and Communications Not releated to data processing	Telecommunication in general. Not releated to data processing
20	The Penal Code No.26/NA datd May 17, 2017	Article 424 Implementation The Government of the Lao PDR, the People's Supreme Court, the Office of the Supreme People's Prosecutor and other relevant authorities are to implement this Penal Code.	Cybercrime, Data security

#	Regulation	Status	Citation
		Legislation / Public Comment / Passage / Enforcement / Amendment, etc.	
		Status of the regulation: Draft = drafting (new regulation) published = published in the gazzette but not yet enacted Enact = published in the gazzette and already enacted Amendment = enacted regulation being on amending process	URL
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	Enact	http://lsp.moic.gov.la/?r=site%2Fdisplaylegal&id=289
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015	Enact	http://lsp.moic.gov.la/index.php?r=site%2Fdisplaylegal&id=216
3	Guideline on the implementation of the Law on	Enact	https://laoofficialgazette.gov.la/kcfinder/upload/files/Introduction%20on%20Implementation%20of

	Electronic Data Protection no. 2126/MPT, dated 8 August 2018		%20Data%20Protection%20Law.pdf, http://lsp.moic.gov.la/index.php?r=site%2Fdisplaylegal&id=371
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018	Enact	http://lsp.moic.gov.la/index.php?r=site%2Fdisplaylegal&id=372
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018	Enact	http://lsp.moic.gov.la/index.php?r=site%2Fdisplaylegal&id=424
			—
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012	Enact	http://lsp.moic.gov.la/index.php?r=site%2Fdisplaylegal&id=39
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017	Enact	http://lsp.moic.gov.la/index.php?r=site%2Fdisplaylegal&id=296
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017 / Instruction on Computer Safety	Enact	http://lsp.moic.gov.la/index.php?r=site%2Fdisplaylegal&id=293
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014	Enact	http://lsp.moic.gov.la/index.php?r=site%2Fdisplaylegal&id=56
10	Decree on E-commerce No. 296/GOV	Enact	https://laoofficialgazette.gov.la/kcfinder/upload/files/Decree%20on%20Electronic%20Commerce%20No.296%20-%20Reduced.pdf
11	Decree on consumer protection in financial services No. 225/GO,	Enact	http://www.lsp.moic.gov.la/index.php?r=site%2Fdisplaylegal&id=505

	dated 06 April 2020		
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012	Enact	http://www.lsp.moic.gov.la/index.php?r=site%2Fdisplaylegal&id=133
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018	Enact	http://www.lsp.moic.gov.la/index.php?r=site%2Fdisplaylegal&id=324
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020	Enact	http://lsp.moic.gov.la/index.php?r=site%2Fdisplaylegal&id=517
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016	Enact	https://mpt.gov.la/index.php?r=site/contents&id=5
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020	Enact	http://lsp.moic.gov.la/index.php?r=site%2Fdisplaylegal&id=515
17	Decree on Credit Information No 224/GOV dated July 19, 2019	Enact	https://laoofficialgazette.gov.la/index.php?r=site/display&id=1534
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016	Enact	https://laoofficialgazette.gov.la/index.php?r=site/display&id=1136
19	Law on Telecommunications (Revised Version) No. 05,	Enact	https://mpt.gov.la/index.php?r=site%2Fdetail&id=822

	dated November 16, 2021		
20	The Penal Code No.26/NA datd May 17, 2017	Enact	https://laoofficialgazette.gov.la/index.php?r=site%2Fsearchtip&s=penal+code

Definitions for basic items

#	Regulation	Type and Scope of Data	Data processing and handling
		Personal data, personal information/sensitive and important data/children and minors' data, etc. Is the scope of data clearly written in the regulations? What are the unclear points?	Processing, handling / disclosure, sharing, provision, transmission, outsourcing / use for advertising, etc.
		Specific type of data required to complied with the regulation	Provision for data processing
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	Article 2 Electronic Data Protection Electronic Data is digits, letters, motion- picture, non-motion picture, audio, video and others that keep in electronic form. Electronic Data protection is the methods and measures to secure the data that have been administrated and stored in electronic form from accessing, using, disclosing, editing, sending, transferring and destroying without permission.	Article 3 Definitions 13. Electronic Data Administration means the administrative and management of data including saving, copying, sending, receiving, maintaining and destroying the electronic data.
		Article 3 Definitions 1. Data means the digits, letters or other symbols that can be processed by computer; 2. Electronic means things that relating to the technology by using electricity, digital, magnetic system, wireless system, fiber light, magnetic electric and other similarities; 11. Official Data means data or data technology that relating to the activation or administration of the government; 12. Personal Data means electronic data of individual, legal entities or organizations;	Article 11 Electronic Data Protection Tasks Electronic Data Protection Tasks are as following: 1. Data collection; 2. Inspection of electronic data; 3. Depositing of electronic data; 4. Maintenance of electronic data; 5. Using or disclosing of electronic data; 6. Sending or transferring of electronic data; 7. Accessing of electronic data; 8. Updating or editing electronic data; 9. Deleting of electronic data.
		Article 9 General Data General data is the data of	

		individual, legal entities or organizations which able to access, use and disclose, and must indicate sources of data correctly	
		Article 10 Specific Data Specific data is the data that not allow individual, legal entities or organizations to access, use or disclose without permission from the owner or relevant organizations. Specific data includes official data and personal data. Data Security must be ranked in official data and the procedure of accessing, using and disclosing as specified in the Article 22 in this law.	
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015	Article 3 Definition of Terms 4. Computer Data refers to any data, messages, programs or database system, personal data, computerized traffic data in the form that can be processed and enable the operation of the computerized system; 5. Database System refers to data being saved in electronic file that can be manageable, improvable and usable; 6. Personal Data refers to data related to or referred directly to the character or ....., activity of individuals, legal entities or organizations in a direct or indirect way; Data Traffic through Computerized System refers to computer data relating to the communication through computerized system which being created by the computer system that is a part of the communication chain which indicate the sender, starting point, mediums, road, destination, date, time, size, duration of communication, type of services and others that are related to the communication through such computerized	Article 3 Definition of Terms 9. Data Processing in Automatic Form refers to the process of data calculation and processing in the computerized system through the computer program;

		system. 15. User Data refers to any data sending to the user, such as postal address, electronic address, geographical address, Internet code number, telephone no. or others that being used in the computerized system;	
			Article 8 Cybercrime-Prone Behaviour The cybercrime-prone behaviour includes: 1. Disclosure of safeguarding measures for accessing computerized system; 2. Unauthorized accessibility to computerized system; 3. Censoring of content, photos, moving pictures, sound and video without authorization; 4. Stealing data in the computerized system without authorization; 5. Causing the losses through online social media; 6. Dissemination of pornography through computerized system; 7. Interference of computerized system; 8. Forgery of computer data; 9. Destruction of computer data; 10. Business operation related to computerized system cybercrime tools.
			Article 9 Disclosure of Safeguarding Measures for Accessing Computerized System Disclosure of safeguarding measures for accessing computerized system is to bring special safeguarding measures for disclosure without authorization which causes damage to the state, individuals, legal entities, organizations and society.
			Article 10 Unauthorized Accessibility to Computerized SystemThe unauthorized accessibility to computerized system is the use of electronic apparatus in the computerized

			system with special safeguarding measures or to steal commercial, financial data, confidentiality and other data of individuals, legal entities and organizations.
			Article 12 Stealing Data in the Computerized System without Authorization Stealing data in the computerized system without authorization is to catch up data being received or transferred through the computerized system by using electronic apparatus.
			Article 16 Falsification of Computerized System The falsification of computerized system is the use of computer or computerized system and electronic apparatus in order to change the computer data through the following action: 1. Input data, changing data, falsifying electronic address or deleting data in the computerized system that cause any computerized data being changed from the original data on purpose; 2. Input and change data relating to financial transaction, trade, confidentiality and other data of individuals, legal entities, organizations without authorization; 3. Setting fake website in order to cheat, a deception to push the users of computerized system or the internet to provide the deposit account information, credit card code, internet application code, code for internet user and other data.
			Article 17 Demolition of Computer Data Demolition of computer data is to erase, edit and/or the changes in the computer data or data in the computerized system in order to make such data or such

			computerized system damages and differ from the original data.
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018	Chapter 2 1. Article 8 Electronic data is digital text, letters, moving images, still images, sound, video, etc. stored in electronic form, including information of individuals, legal entities, organizations, confidentiality, security, copyright information and other information. This information includes both information that can be disclosed, called general information, and information that cannot be disclosed, called specific information. Therefore, in the Law on the Protection of Electronic Information, it was unanimously agreed with all sectors to include two types: general information and specific information.	Chapter 2 4. Article 11 Electronic data protection is the use of methods and measures to prevent information managed and stored in electronic form from being accessed, used, disclosed, modified, sent, transferred or destroyed without permission.
		Chapter 2 2. Article 9 General information is the information of individuals, legal entities or organizations that can be accessed, used and disclosed but must state the source of the information correctly. For example: Personal information such as name, title, address, phone number, email address, organizational information, general statistical information, technical publications, etc.	Chapter 2 5. Article 12 Data collection is the collection of data in a data warehouse or database for easy access, inspection and safe use on the basis of a unanimous agreement between the data manager and the data owner, which both parties benefit from. For example: a bank wants to collect financial transaction account information of Mr. Khe, the bank must inform Mr. Khe about the purpose, the details of the information to be collected such as name and surname, date of birth, gender, residence,
		Chapter 3 3. Article 10 Specific information is information that does not allow individuals, legal entities or organizations to access, use or disclose without permission from the owner of the information or related organizations. For example: customer information, financial information, personal biography,	Chapter 2 6. Article 13 Electronic data inspection is the inspection of various details of the data to ensure that the data is correct, reliable, not against the law and regulations as well as to ensure that it can be used in accordance with the circumstances, such as the data obtained must be correct, complete, correct,

		health treatment history, race, religion, project plans, budget plans, official secrets, etc.	without modification, change, forgery, loss, partial or total damage and be newly created. For example: If you want to deposit information in a data deposit service center, you must identify and check your information in detail before giving it to the data manager to verify that it is correct according to the rules and conditions of the deposit procedure.
			Chapter 2 7. Article 14 Depositing electronic data is to bring data in electronic form such as numbers, letters, moving images, still images, audio, video, etc. to be deposited with the data manager by complying with the agreement of both parties to ensure that the data is safe, accurate and in accordance with the Law on the Protection of Electronic Data.
			Chapter 2 8. Article 15 Electronic data storage is the management and maintenance of data to ensure that the data is safe, not lost, damaged as well as to facilitate quick access and Use. Data managers must define measures and methods of safe storage, such as creating an archive Maintain electronic information that can be easily checked, information security level, authorization Data access, data retention period, data backup, etc. For example: any information service center must keep your information, such as phone history or sending information via electronic mail, for at least 90 days, after the deadline, your information may be deleted, block access or comply with the agreement of both parties.
			Chapter 2 9. Article 16 Using or disclosing

			electronic information is bringing information out for use or disclosure to a third party to meet the requirements of the work which must be approved by the owner of the information unless it is proposed by the relevant government organization. For example: He also committed the crime of defrauding citizens by making false calls to other people to pay him, which caused other people to suffer. In such a case, if there is a request for phone call information from the government organization with relevant authority to request Mr. Khe's information, the data manager must provide the information as proposed without the need to notify Mr. Khe.
			Chapter 2 10. Article 17 Sending or transferring electronic information is sending information from the source to the destination Defined through electronic devices or computers in a transfer such as data transmission Internet network, data recording equipment, etc. in accordance with the conditions agreed between Recipients and senders to ensure that the information is safe, correct and does not violate the law. Example 1: Sun provides a data deposit service and wants to transfer Mr. Khe's information to Mr. Khe Sun. If he wants to provide the service to receive such information, he must obtain permission from Mr. Khe before he can send or transfer the information. Example 2: You want to send important information such as financial transaction information, banking, investment and accounting via electronic mail (email) to You to ensure that the information is

			safe, correct and complete. You must encrypt the data security before sending it to You.
			Chapter 2 11. Article 18 Access to electronic information is access to general information or specific information to use and disclose according to work requirements. In the case of individuals, legal entities or organizations with the purpose of accessing specific information, they must submit to the relevant data manager for research, consideration according to laws and regulations
			Chapter 2 12. Article 19 Updating or correcting electronic data is modifying or changing from the original data to make the data correct and consistent according to the data owner's proposal. For example: You want to update or correct your information such as address, phone number, size of information, etc. He must propose to the data manager to consider correcting or provide methods for him to be able to update and correct the information himself,
			Chapter 2 13. Article 20 Deletion of electronic data is the destruction of data from electronic devices or database systems, for example: if you want to delete information that you do not want to use, you must propose to the data manager to delete or delete it. Its information is out of the database system. In the event that the data has expired, the data manager has the right to delete or Destroy the information from the database system but must notify the owner of the information. In the event that your information affects national security, peace, harmony The

			order of society, culture and the good customs of the nation or information that defames others. The data manager must delete or destroy the information according to the proposal of the authorities or related persons.
			Chapter 2 14. Article 21 electronic data protection measures are the determination of specific methods, requirements and regulations in the protection of electronic data to ensure data security, such as the level of official data security, storage, access, security encryption and response to data intrusion.
			Chapter 2 16. Article 24 Security in accessing information is to comply with measures, regulations or policies to access information safely, such as determining rights, procedures, methods of access and recording the history of entering and exiting the system in detail. In the event that the information is changed, corrected, lost or damaged, it must be possible to check it again quickly and according to the situation. Also, the owner of the information must ensure that his password is not leaked so that others do not use it.
			Chapter 2 17. Article 25 Security encryption is to maintain the confidentiality of information by encoding information to prevent information from being accessed, read, destroyed, used, disclosed, sent, transferred, updated, deleted, changed and other actions that cause damage. For example: Data managers must use the electronic certificate (Certificate Authority) on the system to provide information services, encryption

			in PGP (Pretty Good Privacy) format when sending or transferring important electronic data through electronic mail (email), encryption of electronic data in normal format and other formats to be correct according to security standards. For data security encryption, details are provided in the Computer Security Guidelines,
			Chapter 2 18. Article 26 Response to data intrusion is to check and collect information, evidence about the intrusion as well as coordinate with relevant parties to stop and solve the incident in a timely manner. In the case of receiving a notification from an individual, legal entity or organization, the data manager must quickly check, analyze, manage, correct, notify and define various protection methods to prevent data intrusion again. Data managers must report emergencies to the Computer Emergency Prevention and Resolution Center of the Ministry of Posts, Telecommunications and Communications in order to collect information, coordinate and take corrective actions in a timely manner.
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		Chapter 2 1. Article 9 Disclosure of measures to prevent access to computer systems is to bring specific measures to be disclosed without permission such as passwords, loopholes, penetration methods, methods of attacking computer systems and other methods that cause damage to the state, individuals, legal entities, organizations and society. For example: He brought passwords, vulnerabilities, penetration methods and methods of attacking the computer system of an

			organization to reveal to other people without permission, causing damage to the computer system of the organization
			Chapter 2 2. Article 10 Unauthorized access to computer systems is the use of electronic devices or tools such as computer programs, malicious programs, data recording devices and other devices to access computer systems that have specific protective measures to steal commercial, financial, confidential and other information of individuals, legal entities, and organizations. For example: He used a data recording device with a virus to connect to the computer system of any organization without permission to steal data, falsify data, change data or do other actions that caused damage to the computer system of the organization.
			Chapter 2 4. Article 12 Unauthorized computer data interception is the interception of information being received or sent through the computer system, such as the interception of data through electronic mail (Email), telephone calls, text conversations and other forms using electronic tools. For example: Mr. Kum sent an electronic letter to Mr. Kum that he would transfer one billion kip for the goods by sending it to Mr. Kum's account, but Mr. Kol used electronic tools to capture the information of the conversation between Mr. Kum and Mr. Kum, which information may cause damage to Mr. Kum and Mr. Kum.
			Chapter 2 5. Article 13 Creating damage through online social media is

			manifested by the following actions: Example 1: He took the information that is defamatory, defamatory, using vulgar words and posted it on Facebook, WhatsApp, LINE, Twitter, YouTube and through other means; Example 2: You bring information that is characterized by violence, mushroom information, deceptive information, and untrue information published on Facebook, WhatsApp, LINE, Twitter, YouTube and through other means; Example 3: He brings information that destroys national security, peace and stability Social order, culture and good customs of the nation published on Facebook (Facebook), WhatsApp, LINE, Twitter, YouTube and through another way; Example 4: He brings information that is propaganda, incites and encourages people to oppose the government or divide unity and publish it on Facebook, WhatsApp, LINE, Twitter, YouTube and through other means; Example 5: Mr. Kum advertises selling drugs, chemical weapons, chemical weapons, human trafficking, prostitution, prostitution and other illegal things posted on Facebook, WhatsApp, LINE, Twitter (Twitter), YouTube (YouTube) and through other means; Example 6: You publish or transmit information as defined in Articles 11 and 14 of the Law on Combating and Suppressing Computer Crimes including 1, 2, 3, 4 and Article 5 of Article 13.
			Chapter 2 7. Article 15 Interfering with the computer system is the following action: a. 7.1. Using computer programs,

			viruses or other tools to disrupt or destroy the operation of computer systems. For example: He has attacked the computer system of an organization by sending a large amount of data (DDoS Attack) to block or make the operation of the computer system abnormal or unusable or to attack with the use of viruses to delete and destroy important data files in the computer system, causing damage to the organization; b. 7.2. Sending computer system information or electronic mail by concealing the sender's address or source, such as sending fake electronic mail, sending propaganda messages and other forms to disrupt and/or destroy the operation of computer systems, For example: He faked an Internet address (IP Address) and sent a large number of e-mails to Ms. Qo by concealing the source, which interfered with the operation of Ms. Qo's computer system until processing was delayed or damaged, causing the computer to crash.
			Chapter 2 8. Article 16 Falsification of computer data is the use of computers or computer systems and electronic devices to change computer data by the following actions: Example 1: He stole access to a computer system of a university with the purpose of changing information, deleting his or other person's education information such as exam scores (from 0 to 9), Grade point average (F to A), attendance history (from missing many hours of class to coming to class normal) and other information; Example 2: He hacked into a bank's computer system to enter and change financial, commercial and confidential

			transaction information, such as changing account balances, customer payments, money transfer information or falsifying bank confidential electronic documents and other information; Example 3: He created a fake website of a bank such as the real bank website is www.123abc- bank.la to become a fake website www.123cba-bank.la with the purpose of deceiving or lying to other people to get deposit account information, credit card code, internet access code and other information.
			Chapter 2 9. Article 17 Destruction of computer data is the deletion, modification and/or modification of computer data or data in a computer system to make the data or computer system damaged and different from the original data. For example: He hacked into a company's computer system to delete or destroy financial information, customer information, project information and other important information from the company's computer system, causing the company's information to be destroyed and lost.
			Chapter 2 10. Article 18. Proceedings on computer crime tools are creation Specially developing, manufacturing, importing, possessing, trading, distributing, advertising or introducing such tools as computer programs or designing computer data to commit computer crimes. For example: He has been operating on signal cutting tools, communication control tools, eavesdropping, data interception, traffic data falsification and modification, coordinate capture, computer data penetration tools,

			etc. to commit computer system crimes.
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018	Article 2 items such as electronics An electronic signature (Electronic Signature) is a letter, mark, symbol, number, sound or other thing created in electronic form attached to electronic data to indicate and verify the identity of the signer and the authenticity of the said data.	Article 3 Definition of Terms 5. Keeping data confidential (Data Confidential) means protecting any person, legal entity or organization from accessing any information or document;
		Article 8 Types of electronic signatures There are two types of electronic signatures: 1. Electronic signature restored; 2. Digital signature.	Article 3 Definition of Terms 6. Data Integrity (Data Integrity) means verifying any data or document as being complete, accurate and true to the actual data;
		Article 9 items such as basic electronics A basic electronic signature is information created in an electronic form that is used to indicate and verify the identity of the signer using an electronic program or tool without using a security code infrastructure to recognize each other between the originator of the communication and the recipient of the communication.	
		Article 10 Digital signature A digital signature is information created in an electronic form that is used to indicate and verify the identity of the signer who uses a program or electronic tool using a security code infrastructure to recognize each other between the originator of the communication and the recipient of the communication.	
		Article 12 Digital seal A digital seal is information created by a legal entity or organization in electronic form using a technical system that is used along with a digital signature to verify that there is a link between the signer and the document.	

		Article 18 Electronic data Electronic data is text that is letters, numbers, images, sounds, signs or symbols in the form of information or documents that are created, sent, received, stored or processed by electronic means. Electronic data with digital signature and digital seal have legal effect as defined in Article 15 of this Law.	
		Article 23 Certificate of electronic signature An electronic signature certificate is any electronic data that is used to create a digital signature or digital seal issued by an electronic signature certificate issuer for identity verification, data confidentiality, data accuracy and non-repudiation using security code infrastructure technology. For the basic electronic signature there is no electronic signature certificate	
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012	Article 2 Electronic Transaction An electronic transaction is an act of making a contract, and the provision and use of electronic government services that are conducted wholly or partly by electronic means, which includes the use of Automatic Teller Machines (ATMs), payments over the Internet, and other similar interactions.	
		Article 3 Definition 7. An Electronic Document means any document, record, or information that are recorded or stored on any medium by an electronic information system and that can be read using a display, print-out and other output;	
		Article 3 Definition 9. An Electronic Record is any document or data that is required by law or regulation to	

		be stored when electronic storage means are used.	
		Article 3 Definition 10.Electronic Information System means a system used for creating, sending, receiving, and storing data or other processing of data messages;	
		Article 3 Definition 14.Signature means an electronic method used to identify a person who is the owner of the signature and to indicate the intention of that person regarding the information contained in an electronic document;	
		Article 3 Definition 3. Electronic Communication means any statement made, sent or received in electronic form;	
		Article 3 Definition 4. A Data Message means information in the form of alphabetical letters, text, numbers, sound, codes, computer programs, software, and databases or other formats that is generated, sent, received or stored by electronic, optical, or magnetic means;	
		Article 8 Formation of Electronic Contracts The formation of an electronic contract using electronic means isas follows. 1. An offer and the acceptance of an offer to enter into a contract. 2. A declaration of intent or other statement by an originator or addressee of a data message or electronic document; 3. An agreement by the parties to an electronic transaction to select the technological means, electronic communications modes, and electronic signature rules. Contracts formed electronically can be amended electronically unless the contract definesotherwise.	

		In addition to the above provisions, the formation of each type of an electronic contract shall be applied according to the Law on Contracts and Torts.	
		Article 19 Types of Electronic Signature There are three types of electronic signatures: 1. Basic electronic signature; 2. Basic digital signature; and 3. Secure digital signature.	
		Article 20 Basic Electronic Signature Basic electronic signature means data in electronic format that are in, affixed to, or technically associated with a data message, which identifies the signatory and indicates the signatory's intention in respect of the information contained in the data message.	
		Article 21 Basic Digital Signature Basic digital signature means a type of electronic signature that is uniquely linked to the signatory, capable of identifying the signatory, created using means that the signatory can maintain under his sole control, and any subsequent change of the data is detectable.	
		Article 22 Secure Digital Signature Secure digital signature means a type of digital signature created using technical methods that protect against the forgery of that signature by using available technology to ensure that the signature creation-data used to generate that signature can practically be used only once and can be reliably protected by the legitimate signatory against its use or discovery by others.	
		Article 31 Forms of Electronic Transaction Used by State Organizations Electronic transactions by state organizations are divided into	

		three forms as follows: 1. Electronic transactions within a state organization; 2. Electronic transactions between State organizations; and 3. Electronic transactions between a state organization and individuals, legal entities, and other organizations. The rules and standards that will apply to the use of each type of electronic transaction by State organizationsshall be stipulated inspecific regulations.	
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017	Article 3 Definition of Terms The terms applied in this Law shall have the meaning as follows: 1. Crime refers to an offence as stipulated in the Law on Criminal Procedures and other laws of which prescribed criminal punishment;	
		Article 3 Definition of Terms 3. Computer Data refers to any data, messages, programs or database system, personal data, computerized traffic data in the form that can be processed and enable the operation of the computerized system;	
		Article 3 Definition of Terms 4. Personal Data refers to data related to or referred directly to the character or nature, activity of individuals, legal entities or organizations in a direct or indirect way;	
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014	Article 2: Information Management on the Internet Information management on the Internet refers to the monitoring, reviewing, resisting and suppressing the use of information on the Internet,	Article 6: Dissemination of Information through the Internet The dissemination of information through the Internet refers to the posting of messages, animations, photos, voices, and videos on the website in order to

		which threatens society, and stability of the nation.	present, comment, share, send, and forward messages to one or many people.
		Article 3: Definition In this Decree: 1. Information means messages written in numbers, words, animations, photos, voices and videos, among others;	
10	Decree on E-commerce No. 296/GOV	Article 2 Electronic commerce Electronic commerce is buying and selling, exchanging goods or services between merchants and customers using electronic channels.	
		Article 3 Definition of Terms 5. Online Ordering Function means an order that is installed in an electronic trading channel or any data receiving and sending device connected to the electronic trading channel to enable the buyer to initiate an electronic trading contract according to the conditions specified in the electronic trading channel;	
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020	Article 2 Protection of users of financial services Protection of users of financial services is the use of various measures to protect the property, rights and legitimate interests of users due to the effects of using financial services.	
		Article 3 Definition of Terms The words used in this decree have the following meanings: 1. Users means individuals, legal entities or organizations both domestic and foreign that use financial services;	
		Article 13 Maintenance of user information User information is personal information, financial information, passwords such as ATM card code, e-view code, mobile bank code. The service provider must keep the user's information and not disclose it to	

		other unauthorized persons or Organizations that do not have relevant authority. User information can be stored in paper and electronic form. service provider It is necessary to notify and advise users how to store passwords. In the event that users' password information is leaked or disclosed without permission, the service provider must record and notify the affected users immediately. In the event that the leak or disclosure creates a serious or widespread impact, the service provider must record and report to the management and inspection organization to protect financial service users urgently. The service provider will be able to disclose the user's information to a third party after receiving written consent from the user. In the case of disclosure of information to the competent authority must act according to the relevant law. 5	
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012	Article 2. Definition of Terms 4. Credit Information refers to general information about the customer, information on the status of credit, including the guarantee, financial status and other information as determined by the Credit Information Center, the Bank of the Lao PDR;	Article 2. Definition of Terms Activities Regarding Credit Information refers to the collection, modification and analysis of information, classification of business, customer, exchange of credit information, service, supply and development of credit information, production creation, service development, prepare new and modern technology to serve the credit information service;
		Article 2. Definition of Terms 6. Consent refers to the customer's written authorization allowing the Credit Information Center to disclose personal information, financial status information which can be exchanged in the Credit Information Center with other parties;	

		Article 2. Definition of Terms 7. Credit Information Product refers to the determination of personal information, credit information provided by the Bank of the Lao PDR, as follows: • Standard form of credit information report • Products the Credit Information Center provided to its members; • Standard from of financial institution report; • Standard form for reporting and other statistic.	
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018	Article 2 Credit Information Access The credit information access is the credit information services through the information searching and providing of the credit information center.	
		Article 3 Definitions The terms used in this decision shall have the following meaning: 1. "Credit information" refers to credit information or other information concerning loaning.	
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020	Article 2 Electronic signature service An electronic signature is a letter, sign, numerical symbol, sound or other thing created in electronic form attached to electronic data to indicate and verify the identity of the signatory and the authenticity of said data. The operation of electronic signatures is the management of electronic signature verification, service provision and use of electronic signatures of individuals, legal entities and organizations.	
15	Decree on Internet Information Center / Decree on data center pass though	Article 2 Internet Information Center Internet Information Center is a system that integrates technical infrastructure to provide information services such as servers, databases, programs,	

	internet No 412 November 2016	websites and provide various information through the Internet.	
		Article 3 Definition of terms The terms used in this decree have the following meanings: 1. Internet Data Center refers to the technical infrastructure system that includes equipment systems necessary to provide equipment installation space, server space, server space, server space, software, database, data storage, etc.;	
		Article 3 Definition of terms 2. Internet Content Center (Intermet Content Center) means a center that provides various information services in electronic form such as online social media, video, images, audio, music, and books via the Internet;	
		Article 3 Definition of terms 6. Information Security (Information Security) refers to technical security and management of information systems to maintain, protect and recover information systems and services from accidents, attacks or other hazards.	
		Article 3 Definition of terms 7. Personal data (Personal Data) refers to information related to or indicating the character, identity, activity of a person, legal entity or organization directly or indirectly;	
		Article 3 Definition of terms 3. Database (Data Base) means a place to store information in electronic form in a systematic way that can be managed, updated and used;	
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020	Article 2 Protection of service users Protection of service users against telecommunication and Internet is the use of relevant measures to protect the property, rights and interests of service users who are affected	

		by the use of services or the use of telecommunication and Internet products, such as charging for the use of telephone and Internet services, cutting illegal data packages, receiving phone calls or disturbing messages, etc.	
17	Decree on Credit Information No 224/GOV dated July 19, 2019	Article 3 Definition of Terms 2. Wrong information refers to credit information that is incorrect according to the printed form of credit information report or is factually incorrect;	Article 2 Credit information work Credit information work is the activity of collecting, checking, storing, creating products, providing and correcting credit information.
		Article 3. Credit information Credit information is information on loans, financial obligations and other related information of customers to financial institutions, other legal entities and organizations in which the customer has an obligation to pay debts to financial institutions, legal entities and organizations. Credit information includes the following: 1. Individual customer information such as identity cards and census records or passports; 2. Customer information that is a legal entity, such as the company registration card and the tax's identification number; 3. Loan or credit card information such as approved amount, contract signing date, contract expiration date, loan period, interest rate, outstanding balance, loan type, loan classification and loan status; 4. Guarantee contract information such as buildings, land and houses, money in accounts, valuable documents, machinery and equipment, projects, vehicles, guarantors who are individuals, legal entities or organizations, insurance; 5. Information on financial	Article 10 Data collection Credit Information Company of Lao PDR collects credit information from members and stakeholders according to the prescribed format. After collecting information or receiving credit information The Credit Information Company of Lao PDR must check the information using technology and technical techniques to filter, edit the information to be accurate and complete, and record it in the database. Members and stakeholders are responsible for providing information to the Credit Information Company of the Lao PDR from time to time or as requested by the Credit Information Company of the Lao PDR.

		statements such as financial statements, operating results statements, cash flow statements; 6. Public utility information such as electricity, water, telephone, insurance; 7. Other information as determined by the Bank of the Lao PDR from time to time.	
			Article 13 Provision of credit information Providing credit information is the provision of credit information products as defined in Article 12 of this decree to members or individuals, legal entities or organizations as proposed. The provision of information must comply with the regulations issued by the Bank of the Lao PDR.
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016	Article 2 Information communication technology Information communication technology is a technology used to create information as an electronic system, calculation, classification, storage and exchange of information through communication networks such as computers, telephones, communication devices, broadcasting equipment. Television, network and other electronic devices including related services.	
		Article 3 Definition of Terms The terms used in this law have the following meanings: 1. Information communication technology products mean software, hardware and information related to information communication;	
		Article 3 Definition of Terms 8. Electronic data refers to data recorded or stored in digital form which can be read by a display system, printed or in other formats:	

		Article 3 Definition of Terms 9. Database (Data Base) refers to a place to store information in electronic form in a systematic way that can be managed, updated and used; left	
		Article 3 Definition of Terms 10. Information center (Data and ContentCenter) refers to a system that integrates technical infrastructure to provide information services such as server services, databases, programs, websites and provide various information through the Internet;	
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA dated May 17, 2017		

#	Regulation	Data handlers
		Classification/ distinction by responsibility (data processor, data controller)/ size of data, (national security) critical services, etc.
		Provision on type of data handler
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	Article 3 Definitions 10. Data Owner means individual, legal entities or organizations that own the electronic data; 14. Electronic Data Administration Authorities means individual, legal entities or organizations that responsible for administrating the electronic data which mainly are Ministries, Data Center through internet, telecommunication service providers, banks; 18. Computer Emergency Interception and Resolution Center means an organization of the Ministry of Posts and Telecommunication which its roles to intercept and resolve computer emergency.
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No.	Article 3 Definitions of Terms 8. Service Provider refers to a person who provide a service in the field of communicating the information through the computerized system and/or computer data maintenance service provider;

	61/NA, dated 15 July 2015	
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018	
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018	Article 3 Definition of Terms 9. Initiator of communication (Addresser) refers to the person who creates, sends or converts information or documents any;
		Article 3 Definition of Terms 10. Communication recipient (Addressee) refers to the recipient of sending, sharing information or any document of the initiator of communication;
		Article 3 Definition of Terms 11. Owner of information (Originator) means the person who has the right and/or duty to use, access or arbitrate any information or document;
		Article 3 Definition of Terms 12. Representative (Representing Person) means a person who is authorized or assigned by the owner of the information to initiate communication instead;
		Article 3 Definition of Terms 13. Data collection system means the technical system of the certificate issuer such as electronic Nick used to collect information about the issuance and cancellation of electronic signature certificates so that the holder of electronic signature certificates or other related persons can access such information;
		Article 3 Definition of Terms 14. The holder of electronic certificates means individuals, legal entities and organizations Obtain an electronic signature certificate from an electronic signature certificate issuer:
		Article 28 Electronic signature certificate issuer There are two levels of electronic signature certificate issuers as follows: 1. National Root Certificate Authority: 2. Sub-Certificate Authority.
		Article 29 National electronic signature certificate issuer The National Electronic Signature Certificate Issuer is a department under the Ministry of Posts, Telecommunications and Communications that provides electronic signature certificate issuing services to the electronic signature certificate issuers.
		Article 30 Electronic signature certificate issuer There are four types of electronic signature certificate issuers as follows: 1. Public Certificate Authority (Public Certificate Authority); 2. Government electronic signature certificate issuer (Government Certificate Authority);

		3. Private Certificate Authority (Private Certificate Authority); 4. The foreign electronic signature certificate issuer (Foreigner Public Certificate Authority.
		Article 31 General electronic signature certificate issuers General electronic certificate issuers are legal entities authorized by national electronic certificate issuers to provide electronic signature certificate services to individuals, legal entities or organizations both domestically and internationally.
		Article 40 Public sector electronic signature certificate issuers The public sector electronic signature certificate issuer is a state organization that has registered and requests permission to issue electronic signature certificate services from the national electronic signature certificate issuer to provide services to civil servants and state organizations
		Article 42 Issuer of a specific electronic signature certificate A specific electronic signature certificate issuer is a legal entity or organization that has registered with the national electronic signature certificate issuer to provide services for issuing electronic signature certificates to employees and organizations within their organizations.
		Article 43 Service of the issuer of the electronic signature certificate The electronic signature certificate issuer can only provide services within its organization and must be responsible for all its technical systems as well as comply with the technical conditions and standards set by the national electronic signature certificate issuer.
		Article 44 Foreign electronic signature certificate issuers Foreign electronic signature certificate issuers are electronic signature certificate issuers with offices abroad that have been certified by the national electronic signature certificate issuers to provide electronic signature certificate services to individuals, legal entities and organizations in the Lao PDR.
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012	Article 3 Definition 15.Signature Owner means a natural person, or the authorized representative of a legal entity, who uses an electronic signature creation device in order to generate electronic signatures;
		Article 3 Definition 13.Certification Service Provider means a legal entity or organization authorized by the Science and Technology Sector to issue secure digital signature certificates and provide related services;
		Article 3 Definition 5. The Originator of an electronic communication is the party who generates or sends an electronic communication, or the party on whose behalf it is generated or sent, which does not include an intermediary;
		Article 3 Definition 6. The Addressee is the party that is intended to receive electronic information sent by the originator, which does not include an intermediary;
		Article 33 Intermediary Intermediary means an individual or legal entity that

		provides services to others for sending, receiving or storing data messages, or hosting temporarily, providing access to a communication system and providing other services for handling data messages and electronic documents.
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017	
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017	
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014	9. Internet service user means the individual who connects to the Internet in different forms in order to read, write, send, and forward information on the Internet.
10	Decree on E-commerce No. 296/GOV	
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020	
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012	Article 2. Definition of Terms The terms used in this Decision have the definitions as follows: 1. Member refers to commercial banks, branches of foreign commercial banks located in the Lao PDR and financial institutions as agreed by the Bank of the Lao PDR;
		Article 2. Definition of Terms 2. Customer refers to individuals or legal entities having credit connection with the member;
		Article 2. Definition of Terms 3. Credit Information Center abbreviated as "CIC" refers to the place for accumulating the credit information from commercial banks and financial institutions and to provide credit to commercial banks and financial institution to be used as reference in the consideration for providing credit;
		Article 5. Position and Role of the Credit Information Center3 The CIC is a part of the organizational structure of the Department of Commercial Bank Management of the Bank of the Lao PDR, has the role as a logistical arm to the Department Director in order to conduct the credit information tasks.

		Article 7. Membership The commercial bank and financial institution accepting the deposit or releasing credit must be a member of CID. To apply for a membership, the following documentation shall be prepared: 1. Application for a membership; 2. Copy of a License for bank establishment 3. Copy of an Enterprise Registration Certificate. For financial institution under the management of the Bank of Lao PDR, specific regulation concerning the membership shall be applied.
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018	Article 3 Definitions 2. A member" refers to a commercial bank and a financial institution under the management of the Bank of Lao PDR which is the member of the credit information center.
		Article 3 Definitions "An information owner" refers to a borrower that their information has been retained in the credit information database.
		Article 3 Definitions "A non-information owner" refers to individual, legal entity, and organization that require the credit information.
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020	Article 3 Definition of Terms The terms used in this agreement have the following meanings: 1. Service user or electronic signature certificate holder (Subscriber) refers to individuals, legal entities and organizations that use electronic signature services;
		Article 3 Definition of Terms 7. Registration Authority (Registration Authority) refers to the Registration Authority (RA) who coordinates with the registration service provider when there is a request to use the service or make an electronic notification through checking and verifying the accuracy of the information provided by the service user;
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016	Article 13 Information center through private sector internet Private internet information center is an internet information center of a legal entity or a private organization created and developed to serve its work or to provide services to business and social entities both domestically and abroad.
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020	Article 3 Definition of terms The terms used in this agreement have the following meanings: 1. Service provider means the provider of telecommunications and internet services;
		Article 3 Definition of terms 2. Service users mean individuals, legal entities or organizations that use telecommunication and Internet services;
17	Decree on Credit Information No 224/GOV dated July 19, 2019	Article 3 Definition of Terms The words used in this decree have the following meanings: 1. Financial institutions mean commercial banks, micro-finance institutions, credit and savings cooperatives, credit leasing

		companies and other financial institutions under the management of the Bank of the Lao PDR according to relevant laws and regulations;
		Article 3 Definition of Terms 3. Customer refers to a person, legal entity or organization that has a credit relationship with a financial institution or uses public utility services;
		Article 29 Membership Financial institutions under the management of the Bank of the Lao PDR must become members of the Credit Information Company of the Lao PDR, for legal entities or other organizations can apply for membership according to the conditions set by the Credit Information Company of the Lao PDR from time to time,
		Article 32 Stakeholders Stakeholders are data owners, state organizations, legal entities or related organizations that have information related to credit information as defined in Article 8 of this decree. Article 33 Owner of information The credit information owner is a person, legal entity or organization that is a customer or service user whose member, legal entity or organization has reported their credit information to the Credit Information Company of Lao PDR. Article 34 State organizations State organizations are sectors and organizations that have information related to the credit information work defined in Article 8 of this decree to compare with the information received from members. Article 35 Legal entities and organizations A legal entity or organization is a person authorized to provide public utility services such as electricity, water, telecommunications, and insurance.
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016	
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021	
20	The Penal Code No.26/NA dated May 17, 2017	

Legal Basis

#	Regulation	consent	necessary for the performance of a contract
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	Article 12 Data Collection Individual, legal entities or organizations who would like to collect data must inform the purpose and detail of the data collection to the data owner, and data administration authorities. The collection of data must be approved by data owner and must not dissimulate or use other methods that causing misunderstanding of propose and detail of data collection. Article 15 Maintenance of Electronic Data Data administration authority can maintain electronic data when necessary from the collection purpose and other purposes. Following by the personal data may be deleted or blocked from accessing, except the law specified in others. Data administration authority must create a list of electronic data maintenance which can be easily check and the maintenance measures and methods must be safe. Data administration authority is able to handover electronic data to other authorities and shall be agreed from the data owner. Article 17 Sending or Transferring of Electronic Data Sending or transferring of electronic data shall comply as following: 1. Have permission from the data owner and ensure the receiver is able to secure those data; 2. Input data security for the important data which mainly are financial, banking, investment and accounting data; 3. Do not falsify data sources	

		that have been sent and transferred; 4. Consistent with the agreement between sender and receiver; 5. Stop sending or transferring data when the receiver denies. Individual, legal entities or organizations cannot send or transfer personal data and official data outside the Lao PDR without permission from the data owner or if contradicts with the law. Article 31 General Prohibition Individual, legal entities or organizations are prohibited to act as follow: 1. Accessing, collecting, using, disclosing, destroying, blocking, editing, falsifying, providing electronic data that is the confidential of the state, individual, legal entities or organizations without permission; 2. Sending or transferring electronic data without permission from data owner; 3. Sending electronic data without sources, dangerous program, virus; 4. Creating the falsification of electronic data or dangerous data which causing the damage to others; 5. Use the gap or weakness of data system to access, collect, use and disclose the electronic data; and 6. Other acts that violate the law.	
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No.	Article 40 Prohibitions for Service Providers Service providers shall be prohibited from the following behaviors: 1. Delete any data circulated through the computerized system prior to ninety days in connecting case and before three hundred sixty-five days in non-connecting case;	

	61/NA, dated 15 July 2015	2. Delete data of computerized system user which cause the loss before ninety days; 3. Provide incorrect data to officials and relevant staffs; 4. Disclose the information of service users without authorization; 5. Build condition or facilitate the cybercrime activities; 6. Have other behaviors that violate the laws and regulations.	
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018	Chapter 2 9. Article 16 Using or disclosing electronic information is bringing information out for use or disclosure to a third party to meet the requirements of the work which must be approved by the owner of the information unless it is proposed by the relevant government organization. For example: He also committed the crime of defrauding citizens by making false calls to other people to pay him, which caused other people to suffer. In such a case, if there is a request for phone call information from the government organization with relevant authority to request Mr. Khe's information, the data manager must provide the information as proposed without the need to notify Mr. Khe. 10. Article 17 Sending or transferring electronic information is sending information from the source to the destination Defined through electronic devices or computers in a transfer such as data transmission Internet network, data recording equipment, etc. in accordance with the conditions agreed between Recipients and senders to ensure that the information is safe, correct and does not violate the law. Example 1: Sun provides a data	

		deposit service and wants to transfer Mr. Khe's information to Mr. Khe Sun. If he wants to provide the service to receive such information, he must obtain permission from Mr. Khe before he can send or transfer the information. Example 2: You want to send important information such as financial transaction information, banking, investment and accounting via electronic mail (email) to You to ensure that the information is safe, correct and complete. You must encrypt the data security before sending it to You.	
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018	Article 59 General prohibitions It is forbidden for individuals, legal entities or organizations to behave as follows: 1. Destroy, block, obstruct the operation of the electronic signature certificate issuing system; 2. Forge electronic signature certificates; 3. Provide false information; 4. Claiming to be a service agent; 5. Use someone else's electronic signature certificate without permission; 6. Have other behavior that violates the law. Article 60 Prohibitions for officials, employees or public sector organizations It is prohibited for officials, employees or public sector organizations responsible for the certification of electronic signatures to have the following	

		actions: 1. Access the electronic signature authentication system and disclose information about electronic signature authentication without permission; 2. Modify, destroy or disseminate official secret information without permission; 3. Disregarding or neglecting their responsibilities; 4. Have other behavior that violates the law.	
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012	Article 39 Prohibitions for Individuals, Legal Entities and other Organizations Individuals, legal entities and other organizations are prohibited to behave as follows: 1. Forge electronic documents, electronic signatures or electronic certificates or use forged digital signatures; 2. Provide false information and forged electronic signatures; 3. Access, copy, restructure or take over another person's electronic signature system without [valid] authorization; 4. Use the identity of another person without authorization; 5. Claim falsely that they are representatives to claim for the suspension, cancellation or approval of digital signature; 6. Publish a forged, false, revoked or suspended digital certificate or knowingly place such certificate at the disposal of another person; 7. Provide data messages and electronic records that give rise to damage to national stability, security and social order; 8. Other acts that violate the laws and regulations.	
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		

8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014	Article 15: Restrictions for Internet Service Providers Internet Service Providers are prohibited from: 1. Disseminating information of Internet users without their permission; 2. Creating environments or facilitating individuals, legal entities, or organizations, whose activities include attacking or destroying government-party policy, that impacts national defense and peaceful activities; 3. Behave in ways that violate the regulations and laws.	
10	Decree on E-commerce No. 296/GOV	Article 34 Data protection Data protection in electronic commerce channels is the use of methods and measures to prevent access, use, disclosure, modification, transmission, transfer or destruction of personal information stored without the permission of the owner of the information or relevant management agencies. In the conduct of electronic business, the owner of the electronic channel can store the customer's information or give the right to another person who must comply with the law on the protection of electronic information, other related laws and regulations. Article 42 Prohibitions for electronic commerce operators a. Traders through their electronic channels are prohibited from the following	Article 35 Rights of merchants through their electronic channels Merchants through their electronic channels have the following rights: 1. Conduct trade through its electronic channel; 2. Receive information necessary to conduct electronic commerce; 3. Propose the establishment of an electronic word association; 4. Use other rights according to laws and regulations.

		behavior: a. 1. Conduct business without electronic notification as stipulated in this decree and related regulations; 2. Conducting business that is not in accordance with the scope announced; 3. To carry out business and trade in prohibited goods or services as defined in the law and regulations; 4. Raise funds through electronic trading channels without permission; 5. Provide incorrect or incomplete information in the business notification process; 6. Provide information about goods or services inconsistent with the actual goods or services; 7. Collect, use or disseminate customer information without permission; 8. Send messages that advertise their products or services beyond the prescribed limits; 9. There are other behaviors that violate laws and regulations. b. Buyers in the electronic market must not engage in the following behaviors: a. 1. Conduct business without notifying electronic commerce as stipulated in this decree and related regulations; 2. Conduct business that is not in accordance with the scope specified in the business license; 3. Conduct business of selling prohibited goods or services as stipulated in the law and regulations, 4. Provide incorrect or incomplete information in the process of applying for a business license; 5. Provide information about goods or services inconsistent with the goods or services listed below: 6. There are other behaviors that violate laws and regulations. c. Electronic market service providers must not engage in the following behaviors:	

		a. 1. Conduct business without permission according to regulations, 2. Conduct business that is not in accordance with the scope specified in the business license; 3. Permit or discourage the sale of prohibited goods or services as defined in the law and regulations; 4. To raise funds through electronic trading channels without permission; 5. Provide incorrect or incomplete information in the process of applying for a business license; 6. Collect, use or disseminate customer information without permission; 7. Send messages that advertise their products or services beyond the prescribed limits; 8. There are other behaviors that violate laws and regulations.	
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020	Article 13 Maintenance of user information User information is personal information, financial information, passwords such as ATM card code, e-view code, mobile bank code. The service provider must keep the user's information and not disclose it to other unauthorized persons or Organizations that do not have relevant authority. User information can be stored in paper and electronic form. service provider It is necessary to notify and advise users how to store passwords. In the event that users' password information is leaked or disclosed without permission, the service provider must record and notify the affected users immediately. In the event that the leak or disclosure creates a serious or widespread impact, the service provider must record and report to the management and inspection organization to protect financial service users urgently. The service provider	

		will be able to disclose the user's information to a third party after receiving written consent from the user. In the case of disclosure of information to the competent authority must act according to the relevant law. 5 Article 22 Prohibitions for service providers Providers are prohibited from engaging in the following behaviors: 1. Provide services without compliance with laws and regulations; 2. Collecting fees for receiving, researching and correcting users' proposals: 3. Unauthorized disclosure of user information; 4. Disclose information or advertise financial services inconsistently with reality; 5. Create products that damage good customs or cause harm to society; 6. Limit the right of users to receive information, offer, sue, protect personal information or raise cancel the contract; 7. Other behavior that violates laws and regulations.	
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012	Article 4. Exchange of Information Before consider giving credit to customer, the members of the CIC shall obtain a written consent from their customer to allow the CIC of the Bank of Lao PDR and its members to apply the general information, credit information, financial status and other information available in the reporting form set out by the Bank of the Lao PDR to disclose and exchange with members or to be used in any objectives in accordance with the regulation of the CIC. The disclosure and exchange of information shall guarantee the accuracy and reality. Article 12. Access to Credit Information	

		1. CIC members can seek the information of credit requesting customer based on the products provided by the Bank of the Lao PDR; 2. CIC members can seek the information of credit requesting customer through the user code issued by CIC; 3. Individual or legal entity who is the customer of CIC member and needs to know about his own credit information can request for the information from CIC of The Bank of the Lao PDR; 4. Individual or legal entity who is not the customer of CIC member and needs to know about the credit information of any individual or legal entity shall receive a written consent from such individual or legal entity before being able to inquire such information with CIC; 5. The access to the customer's credit information shall be printed out in order to incorporate in the customer's credit application document. Article 13. Letter of Consent The customer's credit documentation shall comprise of the letter of consent from the customer using a standard form provided by CIC, which authorizes member of CIC, Bank of the Lao PDR, to disclose and use personal information, credit information and other information of customer. Article 15. Prohibition CIC members are prohibited from performing any action as follows: 1. Disclose the customer's credit information without the CIC authorization; 2. Use the customer's credit information out of the limit provided in this Decision;	

		3. Carry out the exchange of credit information without getting through CIC. CIC is prohibited from any of the following actions; Disclose the customer's information to individuals and legal entities who are not the member of CIC, unless receiving a letter from organization having authority or the Board of Governor of the Bank of Lao PDR.	
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020	Article 54 Prohibition for service management staff It is prohibited for management staff or public sector organizations responsible for service management to issue electronic signature certificates with the following behavior: 1. Access the electronic signature certification system and disclose information about electronic signature certification without permission; 2. Modify, destroy or disclose official secret information without permission; 3. Disregarding or neglecting their responsibilities; 4. Other behavior that violates laws and regulations.	
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016	Article 45 Prohibitions for officials, employees or public sector organizations. Officials, state employees and state organizations in charge of the Internet Information Center are prohibited from engaging in the following behaviors: 1. Access personal information databases or databases that store official secret information without permission; 2. Modify, destroy or disseminate personal information or official secret information without	

		permission; 3. Using the system of providing services and providing information of the public sector through the Internet that is against the guidelines of the party-state; 4. Perform duties and responsibilities assigned by the organization; 5. Bring the public sector database and information to be stored at the Internet Information Center located abroad without permission; 6. There are other behaviors that violate laws and regulations.	
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No 224/GOV dated July 19, 2019		
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016	Article 9 Use of electronic data The use of electronic data is as follows: 1. Individuals, legal entities or organizations can use electronic data to enter the point send anything that is valid and in accordance with the law; 2. Providing, exchanging, receiving, sending, collecting and using electronic data must comply with this law and other related laws; 3. The use of information via the Internet must be guaranteed to be accurate, safe and authorized by the owner of the information. 4. Individuals, legal entities or organizations can use or refer to the content of electronic information authorized by the relevant individuals, legal entities or organizations and	

		must state the source of the obtained information correctly Article 46 Prohibitions for information communication technology workers It is forbidden for information communication technology employees to behave as follows: 1. Access, destroy, modify, falsify, supply, use or disseminate information of the state, individual, legal entity or organization without permission; 2. Abusing power, duties, and positions to threaten others, conspire to gain benefits or cause damage to individuals, legal entities, or state organizations, groups, or society: 3. Disclose information or secret documents of the state or official secret documents; 4. Demanding, demanding, receiving bribes or other benefits, delaying consideration Miscellaneous documents; 5. Press and pull products of information communication technology that have been approved or certified; 6. There are other behaviors that violate laws and regulations Article 47 Prohibitions for information communication technology service providers Information and communication technology service providers are prohibited from engaging in the following behaviors: 1. Conducting business related to information communication technology without obtaining a license allow; 2. Sell, transfer, rent or lend a business license related to information communication technology; 3. Access to information communication technology equipment or related electronic	

		equipment without permission; 4. Electronic waste or information communication technology equipment Non-standard news; 5. Access, collect, use, disclose or disseminate information of individuals, legal entities or organizations without permission; 6. Provide, use, modify, destroy or disclose the personal information provided without permission; 7. Receive information that is obscene, distorted, promotes terrorism or against the government of the Lao People's Democratic Republic that he knows; 8. Produce, assemble, sell, import, export or provide repair services for non- standard communication technology equipment, information or related electronic equipment; 9. There are other behaviors that violate laws and regulations. Article 48 Prohibitions for service users Service users are prohibited from the following behavior: 1. Access, collect, provide, use, modify, destroy, disclose or disseminate information of individuals, legal entities or organizations without permission; 2. Use of information communication technology to advertise against the laws and regulations: 3. Create and disseminate information that is obscene, distorted, promotes terrorism or opposes the government of the Lao People's Democratic Republic; 4. Destruction of information communication technology equipment such as	

		infrastructure, information communication technology network: 5. There are other behaviors that violate laws and regulations.	
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA dated May 17, 2017	Article 164 Disclosure of Protection Measures against Illegal Access to a Computer System Any person who discloses special protection measures against illegal access to a computer system without permission and causes damage to the State, individuals, legal persons, organizations or society shall be sentenced to imprisonment for a term ranging from three months to one year and a fine shall be imposed ranging from 1,000,000 kip to 4,000,000 kip.	

#	Regulation		
		necessary for compliance with a legal obligation	necessary in order to protect the vital interests
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	Article 16 Using and Disclosing of Electronic Data Data administration authority can use or disclose personal data that they collected, maintained or administrated when have been approved by data owner, except the law specified in others. Data administration authority cannot provide personal data that they collected, maintained or administrated to a third person if unapproved by data owner or have been proposed from the relevant authorized government organization as specify in the law.	

		Article 18 Accessing of Electronic Data Individual, legal entities or organizations are objective to access the electronic data that not general data, and must propose to the relevant data administration authority as specify in the Article 16 of this law for legal consideration.	
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015	Article 41 Prohibitions for Officials and relevant Staffs Officials and relevant staffs are prohibited from the following behaviors: 1. Disclose privacy of the state, official, individuals, legal entities or organizations through the computerized system; 2. Disclose computer access code and specific safeguarding measures of its sectors; 3. Hand over to other persons any computer data, data circulated through the computerized system or data of service users, except handing-over that benefits case proceedings such as to implement court sentences or in case that authorization is made from case proceeding authority; 4. Delay, hinder and falsify document regarding the cybercrime information; 5. Make use of position for personal interest, interest of family and clan; 6. Abandon responsibilities assigned by organizations; 7. Have other behaviors that violate the laws and regulations.	
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018	Chapter 2 9. Article 16 Using or disclosing electronic information is bringing information out for use or disclosure to a third party to meet the requirements of the work which must be approved by the owner of the information unless it is proposed by the relevant government	

		organization. For example: He also committed the crime of defrauding citizens by making false calls to other people to pay him, which caused other people to suffer. In such a case, if there is a request for phone call information from the government organization with relevant authority to request Mr. Khe's information, the data manager must provide the information as proposed without the need to notify Mr. Khe.	
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018	Chapter 2 19. Article 41 Prohibitions for officials and related employees are regulations to prohibit behavior that violates laws and regulations. Prohibitions for officials and related employees are defined as follows: 19.1. Reveal the secrets of the state, government, of individuals, legal entities or organizations through the system Computers such as confidential organizational information, national security information, commercial information, etc Financial transactions and others; 19.2. Disclose computer system access codes and specific protection measures of their sector such as: methods, terms and specific regulations in maintaining the security of computer systems. 19.3. Handing over computer data, traffic data through computer system or data of service users to -- other persons, except handing over for the purpose of conducting litigation, such as executing an order or obtaining permission from the prosecution organization; 19.4. Hacking, hacking and falsifying information about computer crimes. In the event that there is information that is a crime committed by the computer	

		system when there is a need to use such information, officials and related employees must facilitate cooperation, provide complete and accurate information according to the truth. Chapter 2 20. Article 44 Informing, reporting or complaining about computer system crimes. Individuals, legal entities or organizations can notify or submit to the police investigation agency or public prosecutor's office such as computer system crimes or computer system crimes specified in Article 8 of the Law on Combating and Suppressing Computer Crimes. The investigative agency of the police officer or public prosecutor's office must consider the notification, report or petition within five business days from the date of receipt of the notification, report or petition. For example: He has edited her photo and posted it on Facebook without permission, which will cause damage to her. If she wants to claim justice, she must bring information and evidence to inform the investigation agency of the police officer to consider according to the principle of computer investigation. Chapter 2 13. Article 22 Notification of emergencies Individuals, legal entities and organizations both domestic and foreign who live, operate and use computer systems and/or computer data in the Lao PDR must notify the post, telecommunications and communications sector of emergencies related to crimes	

		that occur on their computer systems as stipulated in Articles 50 and 51 of the Law on Combating and Suppressing Computer Crime. For general reasons such as websites, web pages, blogs, and online social media comments related to any sector, contact, coordinate and notify that sector as a researcher, consider providing information and clarification. For example: The company's computer system has been infected with the WannaCry Ransomware Wanna Decryptor 2.0 virus which has caused damage to the company. The company should report an emergency to the computer emergency prevention and resolution center, the Ministry of Posts, Telecommunications and Communications to ask for advice, how to fix and prevent the virus from happening to the computer system again. Emergency notifications can be made in the following ways: 1. Application according to the formula; 2. Telephone, fax, hotline; 3. Electronic mail; 4. Another method.	
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018	Article 61 Prohibition for electronic signature certificate issuers Prohibits electronic signature certificate issuers from the following behaviors: 1. Providing services for issuing electronic signature certificates without permission or incorrectly according to the license; 2. Bring the license to others to use, rent or transfer; 3. Disclose service user information unless otherwise specified by law or specific regulations; 4. Collect service fees not in accordance with the regulations or as agreed;	

		5. Have other behavior that violates the law.	
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017	Article 7 Fail to provide computer data within the time limit Individuals, or legal entities, or organizations, that receive information regarding to the misconduct in cyber, but fail to inform the investigation authority within time limit. Police officers shall make a recommendation to individuals, legal entities, or other relevant organizations to provide evidence for prosecution.	
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017	III. Network management 1. Computer user listing Computer management authorities should determine rights, scope, and users' history that will help enable verification and monitoring the use of computer network as follows: 1.1. Accession to computer network; 1.2. Accession to importation information in document management system; 1.3. The use of specific programs such as accounting, human resource management, computer database, and others; 1.4. Should immediately stop or remove irrelevant computer network users' accounts in organizations; 1.5. The irrelevant users are not allowed to make copies, destroy or change organizations' information.	
9	Decree on Internet Information Management No. 327/GOV, dated		

	16 September 2014		
10	Decree on E-commerce No. 296/GOV	Article 9 Electronic market services Providing electronic market services is when a business operator creates an electronic trading channel to provide services to other customers by charging a service fee or other consideration. Individuals or legal entities that operate electronic market services must obtain permission from the Ministry of Industry and Trade before conducting activities and must inform the Ministry of Industry and Trade of their electronic market trader information to collect information and monitor activities. A foreign individual or legal entity can operate an electronic market service business in the Lao PDR, but can hold a maximum of 90 percent of shares and must have a registered capital of 100 billion kip or more.	
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020	Article 13 Maintenance of user information User information is personal information, financial information, passwords such as ATM card code, e-view code, mobile bank code. The service provider must keep the user's information and not disclose it to other unauthorized persons or Organizations that do not have relevant authority. User information can be stored in paper and electronic form. service provider It is necessary to notify and advise users how to store passwords. In the event that users' password information is leaked or disclosed without permission, the service provider must record and notify the affected users immediately. In the event that the leak or	

		disclosure creates a serious or widespread impact, the service provider must record and report to the management and inspection organization to protect financial service users urgently. The service provider will be able to disclose the user's information to a third party after receiving written consent from the user. In the case of disclosure of information to the competent authority must act according to the relevant law. 5 Article 17 Provision of credit Before providing credit, the service provider must collect a summary of income and expenses and the financial position of the user with all the details of assets, liabilities and collateral. In case it is seen that the user may not be able to repay the loan or the debt obligation is higher than the income, the service provider must explain and recommend suitable options to the user to prevent excessive indebtedness. In case it is found that the user does not have the ability to pay, the service provider must refuse to provide credit In providing credit, the service provider must make a written loan agreement with content Mainly as follows: 1. 5x credit which is defined in numbers and letters precisely and clearly; 2. Conditions for exercising or using the credit limit; 3. Terms of payment of principal, normal interest, interest and other fees (if any); 4. On the calculation or method of interest calculation, in case of using the method of calculating the fixed interest rate or offer, the service provider must provide information about the amount of interest and the actual annual interest rate, 5.	

		Consequences of defaulting on payment of land, capital and loan interest, 6. Conditions for early payment of debt; 7. Conditions for withdrawal of collateral. The process of monitoring and collecting loans leads users to not use force, threats or violence that is not allowed by law. In the event that the user comes to pay the debt, the service provider must pay the principal and the outstanding interest first so that they can deduct the payment of fees or other words.	
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012	Article 9. Recording Credit Information 1. CIC members must have the database system to serve the credit information tasks. All credit information must be recorded in a full and precise manner based on the credit information reporting standard set out by the Bank of the Lao PDR; 2. All the changes made to the customer's credit information shall be recorded in a full and timely manner. Article 10. Sending of Credit Information The CIC members must send the credit information based on the reporting standard to the CIC, the Bank of Lao PDR, in the form of reporting table in according to the standard form provided by the CIC, at least once a month and no later than the fifth day of the next month. After CIC verify the information obtained from its members and if mistake is found in the information, CIC shall notify such mistake to the members and the members must completely correct the mistake and send to CIC within 2 banking business days after the acknowledgement of such errors.	

		Article 16. Member Inspection CIC under the Bank of the Lao PDR can undertake the inspection on credit information of its member on a regular and emergency basis: 1. Regular inspection is the annual inspection; 2. Emergency inspection can be done at any time if deemed necessary in case of having suspicious information: Member's violation of regulation on the supply and use of credit information that might cause problem to CIC system or financial risks which create the loss to its members. CIC member who is undergone the inspection shall cooperate and give convenience to CIC inspector by providing the information to the inspector in a full and timely basis, appointing staff in charge of credit information to work with the inspector. Before conducting the inspection, the CIC inspector shall inform the members to prepare document, information to be available for the inspection. After the completion of each inspection, the inspector of CIC must prepare a report on the findings of the inspection jointly endorsed with the inspected member.	
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		

15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016	Article 16 Dissemination of information through the Internet of government organizations Ministries, government agencies equivalent to ministries and local government agencies at the provincial level can have websites, programs or other channels to provide services or provide information to government organizations, business units and society as appropriate. Websites and e-mails of government organizations must use the national Internet name code of the Lao PDR and store it in their center. If you don't have your own center, keep it in the information center through the national internet. Ministries, government agencies equivalent to ministries and local government agencies at the provincial level that disseminate information via the Internet must comply with relevant laws and regulations and must be responsible for the content of the information they disseminate. Article 21 Converting information into electronic form of government organizations Various information of government organizations must be created and stored in electronic form in accordance with the regulations on standards and techniques to ensure easy and safe access or search. Government organizations must copy and store information in electronic format in the database in accordance with Article 15 of this decree, and must also comply with the regulations on copying and storing official documents. Government organizations must promote the bringing of information that is	

		not yet in electronic form in electronic form according to the order of importance. The format of electronic documents that are created and stored must comply with relevant regulations that are promulgated from time to time. Electronic documents in the Lao language that are created must use the computer Lao script that is announced to be used from time to time. Article 22 Database and information of the private sector Databases and information of the private sector created to provide services in the Lao PDR must be stored in an information center via the Internet within the country, ensuring security and confidentiality. Article 42 Rights and Obligations of Internet Information Center Service Providers Legal entities or organizations that provide Internet Information Center services have the following rights and obligations: 1. Proposing to continue, change, suspend or cancel the operation of its business; 2. Suspend service to service users who violate the contract or have behavior that may cause damage to the center, peace or social order; 3. Comply with the regulations of the Ministry of Posts, Telecommunications and Communications domestic and international network connections; 4. Respect the rights and store personal information of service users with regulations and technical systems to create and 5. Record usage information and report technical information to the postal sector, telecommunications and	

		communications; 6. Do not disclose personal information of users of the service except with the proposal of the relevant government organization; 7. Provide services as promised or notified to service users; 8. There are measures to solve problems and technical problems for users clearly through its website and clearly defined in the service contract for users; 9. Use live and perform other obligations as defined in laws and regulations.	
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020	Article 16 Rights and obligations of service providers The service provider has the following rights and obligations: 1. Provide information on the use of telephone numbers, data packages, telephone and Internet service charges, telephone and Internet service charges and other related documents to the postal, telecommunications and communication sectors when proposed; 2. Responsible for registering phone numbers in all systems for service users to have complete and accurate information, 3. Monitor all parties who allow themselves to use the service to call or/and send messages as defined in Article 8 of this Agreement; 4. Receive and consider solutions to problems proposed by service users; 5. Compensation for damages due to products and services that are not of good quality and not standard base for service users; 6. Use rights and perform other obligations as defined in laws and regulations.	

17	Decree on Credit Information No 224/GOV dated July 19, 2019	Article 10 Data collection Credit Information Company of Lao PDR collects credit information from members and stakeholders according to the prescribed format. After collecting information or receiving credit information The Credit Information Company of Lao PDR must check the information using technology and technical techniques to filter, edit the information to be accurate and complete, and record it in the database. Members and stakeholders are responsible for providing information to the Credit Information Company of the Lao PDR from time to time or as requested by the Credit Information Company of the Lao PDR. Article 31 Rights and obligations of members Members of the Credit Information Company of the Lao PDR have the following rights and obligations: 1. Collect, provide information and be responsible for the accuracy, completeness, clarity and timeliness according to the report form of the Credit Information Company of the Lao PDR; 2. Develop and improve the technology system to support the credit information system of the Bank of the Lao PDR; 3. Create regulations, manuals for the use and reporting of credit information; 4. Inspect, update and correct erroneous information on time; 5. Use credit information products in accordance with the regulations of the Lao PDR Trust Information Company; 6. Lose the service charge for using credit information	

		according to the regulations of the information company Credit Court of Lao PDR; 7. Appoint staff or units responsible for implementing credit information work; 8. Report credit information work according to regulations; 9. Use rights and perform other obligations as defined in laws and regulations. Article 36 Responsibilities of data owners Credit information owners have the following responsibilities: 1. Use credit information correctly according to the regulations of the credit information company of the Lao PDR; 2. To propose the credit information company of the Lao PDR to correct in case its information is incorrect or wrong; 3. Provide complete, accurate and precise credit information to members; 4. Authorize in writing for the Credit Information Company of Lao PDR to collect and disclose its credit information; 5. Have other responsibilities as defined in laws and regulations. Article 37 Responsibilities of state organizations, legal entities and organizations State organizations, legal entities and organizations have the following responsibilities: 1. Provide accurate, complete and timely credit information, 2. Use credit information correctly according to the regulations of the credit information company of the Lao PDR; 3. Cooperate in coordination and be responsible for providing credit information related;	

		4. Have other responsibilities as defined in laws and regulations.	
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA dated May 17, 2017		

#	Regulation		
		necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	necessary for the purposes of the legitimate interests pursued by the controller or by a third party
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017		
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015		
3	Guideline on the implementation of the Law on		

	Electronic Data Protection no. 2126/MPT, dated 8 August 2018		
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018		
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014		
10	Decree on E-commerce No. 296/GOV		Article 39 Rights of electronic market service providers Electronic market service providers have the following rights: 1. Provide electronic market services according to the authorized scope; 2. To receive the necessary information in conducting electronic market service business; 3. Propose the establishment of an electronic

			trade association; 4. Use other rights according to laws and regulations.
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020		
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012		Article 12. Access to Credit Information 1. CIC members can seek the information of credit requesting customer based on the products provided by the Bank of the Lao PDR; 2. CIC members can seek the information of credit requesting customer through the user code issued by CIC; 3. Individual or legal entity who is the customer of CIC member and needs to know about his own credit information can request for the information from CIC of The Bank of the Lao PDR; 4. Individual or legal entity who is not the customer of CIC member and needs to know about the credit information of any individual or legal entity shall receive a written consent from such individual or legal entity before being able to inquire such information with CIC; 5. The access to the customer's credit information shall be printed out in order to incorporate in the customer's credit application document.
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		Article 5 Approaches of Credit Information Access a member, information owner, and non-information owner are able to access to the credit information by the following methods: 1. A member, who requires credit information, is able to access it by himself by putting his name and password to log in

			to the database, those name and password are provided by the credit information center. After, the member access to the database, the member can search for the required information. 2. An information owner or non-information owner who requires credit information shall submit a written request to the credit information center. For the non-information owners must have the authorization from the information owner along with the request. After the credit information center has received the written request, if the request is correct or complete, the credit information center will provide the required information to the requester within three working days. In case there is no such information, the authority will inform the requester within the above-mentioned period.
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016		
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No		

	224/GOV dated July 19, 2019		
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA datd May 17, 2017		

#	Regulation	opt-out	others
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017		
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015		
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018		
4	Guideline on the Implementation of the Law On		

	Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018		
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014		
10	Decree on E-commerce No. 296/GOV		
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020		
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012		

13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016		
16	Decision on consumer protection for telecommunicati on and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No 224/GOV dated July 19, 2019		
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunicati ons (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA dated May 17, 2017		

Rights of the data subject

#	Regulation	Right to be informed	Right of access
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017		Article 27 Rights of the Data Owner Data owners have the following rights: 1. Create, access, use, disclose, provide, update, terminate, delete, input the electronic data security code; 2. Propose to the data administration authority and other relevant sectors to access, use, disclose, provide, update, terminate, delete his or her data; 3. Inform data administration authority and other relevant sectors to secure his or her electronic data when the data have been damaged or in risk; 4. Complaint to the relevant organizations when receiving non-benefit from electronic data protection; 5. Use other rights as specified in the law.
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015		
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018		
4	Guideline on the Implementation of the Law On Counter and Prevention of		

	Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018		
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014		
10	Decree on E-commerce No. 296/GOV		
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020		
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012		
13	Decision on the Access of Credit Information No.		

	03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016		
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No 224/GOV dated July 19, 2019		
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA datd May 17, 2017		

#	Regulation	Right to rectification	Right to erasure
1	The Law on Electronic Data Protection No.	Article 19 Updating or Editing of Electronic Data Data owner can request to data	Article 19 Updating or Editing of Electronic Data Data owner can request to data

	25/NA, dated May 12, 2017	administration authority for updating or editing the electronic data, or request to stop sending and transferring the data to a third person. After receiving the request from the data owner, the data administration authority must: 1. Proceed in updating or editing data as requested by data owner, or provide methods to data owner in order to be able to update, editing or deleting the data by themselves; 2. Inform the data owner in case of unable to activate the request regarding to the technical problem or other factors.	administration authority for updating or editing the electronic data, or request to stop sending and transferring the data to a third person. After receiving the request from the data owner, the data administration authority must: 1. Proceed in updating or editing data as requested by data owner, or provide methods to data owner in order to be able to update, editing or deleting the data by themselves; 2. Inform the data owner in case of unable to activate the request regarding to the technical problem or other factors.
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015		
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018	Chapter 2 12. Article 19 Updating or correcting electronic data is modifying or changing from the original data to make the data correct and consistent according to the data owner's proposal. For example: You want to update or correct your information such as address, phone number, size of information, etc. He must propose to the data manager to consider correcting or provide methods for him to be able to update and correct the information himself,	Chapter 2 13. Article 20 Deletion of electronic data is the destruction of data from electronic devices or database systems, for example: if you want to delete information that you do not want to use, you must propose to the data manager to delete or delete it. Its information is out of the database system. In the event that the data has expired, the data manager has the right to delete or Destroy the information from the database system but must notify the owner of the information. In the event that your information affects national security, peace, harmony The order of society, culture and the good customs of the nation or

			information that defames others. The data manager must delete or destroy the information according to the proposal of the authorities or related persons.
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018		
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014		
10	Decree on E-commerce No. 296/GOV		
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020		

12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012		
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016		
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No 224/GOV dated July 19, 2019	Article 14 Correction of wrong information Members must be responsible for correcting the credit information sent incorrectly according to the credit information report form and report to the credit information company of the Lao PDR within five business days. In case the Credit Information Company of Lao PDR finds credit information of poor quality, it must notify the member to correct the information and report to the Credit Information Company of Lao PDR within five	

		business days. In case any member finds the credit information of his/her customer with another member or related person to be incorrect, he/she must notify the Credit Information Company of Lao PDR in writing to coordinate with the other member or related person to correct it. If the relevant person finds that the reported credit information is incorrect or wrong, he must report it to the Credit Information Company of Lao PDR or a member of the company with whom he has a contractual relationship to correct the information within five business days.	
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA dated May 17, 2017		

#	Regulation	Right to restrict processing	Right to data portability
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	Article 19 Updating or Editing of Electronic Data Data owner can request to data administration authority for updating or editing the electronic data, or request to stop sending and transferring the data to a third person. After receiving the request from the data owner, the data administration authority must: 1. Proceed in updating or editing data as requested by data owner,	Article 27 Rights of the Data Owner Data owners have the following rights: 1. Create, access, use, disclose, provide, update, terminate, delete, input the electronic data security code; 2. Propose to the data administration authority and other relevant sectors to access, use, disclose, provide, update, terminate, delete his or her data;

		or provide methods to data owner in order to be able to update, editing or deleting the data by themselves; 2. Inform the data owner in case of unable to activate the request regarding to the technical problem or other factors.	3. Inform data administration authority and other relevant sectors to secure his or her electronic data when the data have been damaged or in risk; 4. Complaint to the relevant organizations when receiving non-benefit from electronic data protection; 5. Use other rights as specified in the law.
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015		
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018		
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018		
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in		

	Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014		
10	Decree on E-commerce No. 296/GOV		
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020		
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012		
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		
15	Decree on Internet Information Center / Decree on data center pass though		

	internet No 412 November 2016		
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No 224/GOV dated July 19, 2019		
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA dated May 17, 2017		

#	Regulation	Right to object	Right not to be subject to a decision based solely on automated processing
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	Article 27 Rights of the Data Owner Data owners have the following rights: 1. Create, access, use, disclose, provide, update, terminate, delete, input the electronic data security code; 2. Propose to the data administration authority and other relevant sectors to access, use, disclose, provide, update, terminate, delete his or her data; 3. Inform data administration authority and other relevant sectors to secure his or her	

		electronic data when the data have been damaged or in risk; 4. Complaint to the relevant organizations when receiving non-benefit from electronic data protection; 5. Use other rights as specified in the law.	
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015		
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018		
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018		
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		

8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014		
10	Decree on E-commerce No. 296/GOV		
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020		
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012		
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016		
16	Decision on consumer		

	protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No 224/GOV dated July 19, 2019		
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA datd May 17, 2017		

#	Regulation		
		Right to withdraw consent	others
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017		Article 27 Rights of the Data Owner Data owners have the following rights: 1. Create, access, use, disclose, provide, update, terminate, delete, input the electronic data security code; 2. Propose to the data administration authority and other relevant sectors to access, use, disclose, provide, update, terminate, delete his or her data; 3. Inform data administration authority and other relevant sectors to secure his or her electronic data when the data have been damaged or in risk; 4. Complaint to the relevant organizations when receiving non-benefit from electronic data protection;

			5. Use other rights as specified in the law.
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015		
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018		
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018		
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		

9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014		
10	Decree on E-commerce No. 296/GOV		
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020		
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012		
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016		
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020		

17	Decree on Credit Information No 224/GOV dated July 19, 2019		
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA dated May 17, 2017		

Extraterritorial application

#	Regulation		
		applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction	applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017		
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015	(Article 6 Scope of Law Application This law is applied for individuals, legal entities and organizations (both domestic and foreign) who live, perform activity, and study on the use of computerized system and computer data in the Lao PDR.)	
3	Guideline on the implementation of the Law on Electronic Data		

	Protection no. 2126/MPT, dated 8 August 2018		
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018	Article 6 Scope of application of the law This law applies to individuals, legal entities or organizations both domestic and foreign that create, develop, service and use electronic signatures.	
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012	Article 6 Scope of Application This Law applies to individuals, legal entities, State organizations [and agencies], international organizations and civil society that use electronic transactions in Lao PDR. This Law does not apply to: 1) The creation of a will; 2) Certificates related to births, marriage, divorce, and death; 3) Documents of title; 4) The creation, enforcement or certification of the possession of other's property or power of attorney; 5) Contracts for the sale, transfer, or other disposition of ownership or any interest in land or immovable property; 6) Petitions under the Law on Petitions; 7) Bills of exchange, bills of lading, warehouse receipts or any document that entitles the bearer or beneficiary to claim the delivery of goods, unless laws and regulations define otherwise.	
7	Decision on Penalties in Cyber Crime No.		Article 4 Scope of Application This decision is applied for individuals, legal entities and organizations which monitor

	3624, dated 11 December 2017		information data and electronic devices in the Lao PDR.
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014	Article 5: Scope of this Decree This decree applies to individuals, legal entities, governmental organizations, and the private sector, both Lao nationals and expats, which provide and use Internet service in the Lao PDR.	
10	Decree on E-commerce No. 296/GOV	Article 5 scope of use This decree applies to individuals, legal entities or organizations both domestically and internationally. Movement on electronic commerce in Lao PDR.	
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020	Article 6 Scope of use of the decree This decree applies to service providers, users and organizations managing the protection of users of financial services in the Lao PDR.	
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012		
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018	Article 4 Scope of Application This decision shall apply to the departments of the Bank of Lao PDR, the members, the information owners, and non-information owners whose functions involving credit information assess.	
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020	Article 4 scope of use This agreement applies to individuals, legal entities or organizations that provide electronic signature certification services within the Lao PDR,	

15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016	Article 6 Scope of use This decree applies to individuals, legal entities and organizations both domestic and foreign who create, develop, provide services and use information centers through the Internet in the Lao PDR.	
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020	Article 4 scope of use This agreement applies to service providers and users of telecommunications and Internet services in Lao PDR	
17	Decree on Credit Information No 224/GOV dated July 19, 2019	Article 6 Scope of use of the decree This decree applies to individuals, legal entities and organizations related to credit information work.	
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016	Article 6 Scope of application of the law This law applies to individuals, legal entities or organizations both domestic and foreign active, using and conducting business related to information communication technology in Lao PDR.	
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA dated May 17, 2017	Article 8 Application of the Penal Law within the Territory of the Lao PDR The Penal law is applied to all offences committed on the territory of the Lao PDR. A person or legal person who commits an offence within the territory of the Lao PDR shall be punished in accordance with the Penal Code of the Lao PDR. In the event that diplomatic representatives or individuals enjoying diplomatic immunity, conferred by International	

		Conventions to which the Lao PDR is a party, commit offences on the territory of the Lao PDR, these cases shall be settled based on the International Conventions to which the Lao PDR is a party or through diplomatic channels. Article 9 Extraterritorial Application of the Penal Law Lao citizens who commit offences outside the territory of the Lao PDR shall be charged with and punished for such offences if they are defined as offences under this Penal Code and other related Laws of the Lao PDR that define criminal offences and punishment. Aliens and stateless individuals residing in the Lao PDR who commit offences outside the territory of the Lao PDR shall also be punished. Foreign individuals who commit offences outside the territory of the Lao PDR, which infringe on the national interests of the Lao PDR or legitimate rights and interests of Lao citizens, shall also be punished.	

#	Regulation		
		no express territorial scope, but would require some nexus to the jurisdiction	other
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017		Article 6 Scope of Application This law is applicable to domestic and international individuals, legal entities or organizations that located or activated within the territory of the Lao PDR.
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime),		

	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015		
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018		
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018		
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014		

10	Decree on E-commerce No. 296/GOV		
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020		
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012		
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016		
17	Decision on consumer protection for telecommunicati on and Internet service No. 1061/MPT, dated 25 May 2020		
18	Decree on Credit Information No 224/GOV dated July 19, 2019		
19	Law on Information and Communication		

	Technology (No. 02/NA, dated November 7, 2016		
20	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
21	The Penal Code No.26/NA dated May 17, 2017		

#	Regulation	
		Representatives of controllers or processors not established in the country
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015	
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018	
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018	

5	Law on Electronic Signature no. 59/NA, dated 12 December 2018	
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012	
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017	
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017	
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014	
10	Decree on E-commerce No. 296/GOV	
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020	
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012	
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018	
14	Decision on Business	

	Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020	
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016	
17	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020	
18	Decree on Credit Information No 224/GOV dated July 19, 2019	
19	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016	
20	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021	
21	The Penal Code No.26/NA dated May 17, 2017	

Notification obligation

#	Regulation		
		Data breach notification to authorities	Data breach notification to affected individuals
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017		

2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015	Article 22 Emergency Alert Individuals, legal entities and organizations (both local and foreign) who live, perform activities and use computerized system and/or computer data in the Lao PDR shall give crime related emergency alert which occurred to their computer system to Division of Post and Telecommunication as specified in Article 50 and 51 of this Law. For common event, emergency alert shall be given to other relevant sectors. Emergency Alert can be operated through the following methods: 1. Standard application form; 2. Telephone, fax, hot line; 3. Electronic mail; 4. Other methods.	
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018	Chapter 2 18. Article 26 Response to data intrusion is to check and collect information, evidence about the intrusion as well as coordinate with relevant parties to stop and solve the incident in a timely manner. In the case of receiving a notification from an individual, legal entity or organization, the data manager must quickly check, analyze, manage, correct, notify and define various protection methods to prevent data intrusion again. Data managers must report emergencies to the Computer Emergency Prevention and Resolution Center of the Ministry of Posts, Telecommunications and Communications in order to collect information, coordinate and take corrective actions in a timely manner.	
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no.	Chapter 2 11. Article 20 Notification is the Ministry of Posts, Telecommunications and Communications as the notification. Dangers that occur	

	2543/MPT, dated 24 September 2018	in computer systems and the Internet, such as notifications of fake websites, programs malicious intent, computer system vulnerability reporting, electronic mail fraud, etc. In the event that a virus is found that is spreading in the company and abroad, the Ministry of Posts, Telecommunications and Communications must issue a warning as well as advise how to prevent the virus so that the managers Channels and users of domestic computer systems take note. The computer system service provider must notify and set conditions for accessing the computer system to limit or not allow certain types of service users to access the computer system. For example: The Company, which is the manager of the computer system, received a notification about the spread of the Wanna Cry virus. It must issue a notification as well as advise how to prevent the virus for the users of the computer system to be informed. 12. Article 21 Counseling is the post, telecommunications and communication sector as a consultant, recommending prevention methods and technical solutions such as: finding the source of computer system attacks, proving electronic evidence, correcting computer system vulnerabilities, correcting the phenomenon through online social media, including counseling on work to combat and prevent computer crime to individuals, legal entities and organizations in order to reduce data loss, data disturbance, not to Stopping the functioning of the computer system, preventing the spread of computer viruses and the destruction of information in the	

		computer system. For example: The company's server system was attacked by hackers, causing the server system to be unable to operate normally and causing damage to the company. The company should request advice and guidance from the Computer Emergency Prevention and Resolution Center, Ministry of Posts, Telecommunications and Communications to check, find the source of the attack and improve the system to be able to return to normal use.	
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018		
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014		
10	Decree on E-commerce No. 296/GOV		
11	Decree on consumer protection in financial services No. 225/GO,		

	dated 06 April 2020		
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012		
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016		
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No 224/GOV dated July 19, 2019		
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunications (Revised Version) No. 05,		

	dated November 16, 2021		
20	The Penal Code No.26/NA dated May 17, 2017		

Obligations of Data Fiduciaries

#	Regulation	external	external
		Notification of data processing	registration of database
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	Article 20 Deleting of Electronic Data Data administration authority must delete electronic data that they collected as proposed by the data owner or when using purpose is terminated, the collection is expired or as specify in the Article 29 section 3 of this law. Deleting of electronic data must inform the data owner, except the law is specified in others	
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015	Article 20 Warning Notice The Ministry of Post and Telecommunication is in charge of informing about any dangers occurred in the computer system and the internet such as a warning notice about fake website, malicious code, notifying about possible vulnerability in computer system, deceiving through e-mail and others. Computer system service provider shall give a warning notice and determine the condition in the access to the computerized system in order to limit or not to authorize some types of service users to access to the computerized system. Article 23 Solution Procedures After receiving an emergency alert through the computerized system, the Ministry of Post and Telecommunication shall make consideration and send a notifying reply and give solution procedure within the period of	

		five business days. In case of necessity and urgency, the Ministry of Post and Telecommunication shall promptly carry on technical solution procedures in according to the emergency alert made by the person concerned. In case of being notified about any events relating to some behaviors as specified in Article 11 and 13 of this law which affect the national security or the dignity of any individuals, relevant sectors (both in central and local level) shall consider replying on a case-by-case basis.	
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018		
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018	Chapter 2 11. Article 20 Notification is the Ministry of Posts, Telecommunications and Communications as the notification. Dangers that occur in computer systems and the Internet, such as notifications of fake websites, programs malicious intent, computer system vulnerability reporting, electronic mail fraud, etc. In the event that a virus is found that is spreading in the company and abroad, the Ministry of Posts, Telecommunications and Communications must issue a warning as well as advise how to prevent the virus so that the managers Channels and users of domestic computer systems take note. The computer system service provider must notify and set conditions for accessing the computer system to limit or not allow certain types of service users to access the computer system. For example: The	

		Company, which is the manager of the computer system, received a notification about the spread of the Wanna Cry virus. It must issue a notification as well as advise how to prevent the virus for the users of the computer system to be informed. 12. Article 21 Counseling is the post, telecommunications and communication sector as a consultant, recommending prevention methods and technical solutions such as: finding the source of computer system attacks, proving electronic evidence, correcting computer system vulnerabilities, correcting the phenomenon through online social media, including counseling on work to combat and prevent computer crime to individuals, legal entities and organizations in order to reduce data loss, data disturbance, not to Stopping the functioning of the computer system, preventing the spread of computer viruses and the destruction of information in the computer system. For example: The company's server system was attacked by hackers, causing the server system to be unable to operate normally and causing damage to the company. The company should request advice and guidance from the Computer Emergency Prevention and Resolution Center, Ministry of Posts, Telecommunications and Communications to check, find the source of the attack and improve the system to be able to return to normal use.	
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018	Article 55 Rights and Obligations of Electronic Signature Certificate Holders Electronic Signature Certificate Holders have the following rights and obligations: 1. Provide accurate and clear	

		information when requesting an electronic signature certificate; 2. Provide private key information or other necessary information to authorized organizations to provide for national defense-security work as required by law; 3. Store and use your private key securely and confidentially during the period of validity of your electronic signature certificate; 4. Notify the electronic signature certificate issuer immediately if its private key information is disclosed or stolen. 5. Submit your electronic signature certificate before the expiration date of thirty days; 6. Be responsible before the law regarding the information provided and the use of electronic signature certificates that violate laws and regulations; 7. Use the rights and perform other obligations as defined in the law, Article 35 Intermediary Liability Even if an intermediary does not have liability as defined in Article 34 of this Law, an intermediary still has the following liabilities: 1. Must follow regulations and procedures developed by the Ministry of Posts and Telecommunications; 2. Be subject to civil or criminal liability depending on each case if it knows the facts or circumstances where a data message would result in damage to individuals, legal entities or other organizations; 3. Must comply with any valid contractual or additional legal obligation that it may have in respect of a data message or electronic record; If an intermediary has actual knowledge that information in a	

		data message or electronic record gives rise to civil or criminal liability, the intermediary shall: (a) Remove the data message or electronic record from any information processing system that the intermediary controls and cease to provide services in respect of that information but shall notify the originator if it is unaware[of such fact]; (b) Notify the Post, Telecommunications, and Communications Sector or the appropriate law enforcement agency of the relevant facts and, where it is known to the intermediary, the identity of the person for whom the intermediary was supplying services in respect of the data message or electronic record. 4. Be subject to other liabilities as defined in relevant laws and regulations.	
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014	Article 25: Warning Website managers shall warn, and set the conditions for disseminating information through their own web pages.	
10	Decree on E-commerce No. 296/GOV		

11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020		
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012	Article 10. Sending of Credit Information The CIC members must send the credit information based on the reporting standard to the CIC, the Bank of Lao PDR, in the form of reporting table in according to the standard form provided by the CIC, at least once a month and no later than the fifth day of the next month. After CIC verify the information obtained from its members and if mistake is found in the information, CIC shall notify such mistake to the members and the members must completely correct the mistake and send to CIC within 2 banking business days after the acknowledgement of such errors.	
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016		
16	Decision on consumer protection for telecommunicati		

	on and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No 224/GOV dated July 19, 2019		
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA dated May 17, 2017		

#	Regulation	external	external
		Data protection impact assessment	Others
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017		
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015		
3	Guideline on the implementation of the Law on Electronic Data Protection no.		

	2126/MPT, dated 8 August 2018		
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018		
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014		
10	Decree on E-commerce No. 296/GOV		
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020		
12	Decision on the Activities Regarding Credit		

	Information No. 928/BoL, dated 20 September 2012		
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016		
16	Decision on consumer protection for telecommunicati on and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No 224/GOV dated July 19, 2019		
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunicati ons (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA dated May 17, 2017		

#	Regulation	internal	internal
		technical and organisational measures	Purpose Limitation
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	Article 21 The Measures on Securing of Electronic Data Securing of electronic data, the data administration authority must comply with the following measures: 1. Ranking of the official data security; 2. Maintenance of electronic data; 3. Data accession security; 4. Codification of data security; 5. Responding to data attacks. Article 22 Ranking of the Official Data Security Ranking of the official data security are as following: 1. First Level when the data have been destroyed or disclosed that damages rights and benefits of state, individual, legal entities or organizations; 2. Second Level when the data have been destroyed or disclosed which causing serious damage the rights and benefits of state, individual, legal entities or organizations, or effect the benefit of the community; 3. Third Level when the data have been destroyed or disclosed that damages the production, peace, social security and nation-public security. Article 23 Maintenance of Electronic Data The data administration authority shall maintain electronic data as follow: 1. Contain specific units or staffs that responsible for the administration of data security; 2. Create the collection system, data usage system, the administration of data security system and other relevant	

		systems; 3. Use technical system to secure the data that suitable with the system size; 4. Recheck deleting and destroying of data; 5. Record data with paper, light, magnetic or other methods, and use the suitable processes for the maintenance; 6. Inspect and evaluate the risk of data system at least once a year and must fix the detected problem including update the data system to be secured; 7. Inspect the accessing of data storage system and secure from attacking, virus or other similar risks and others; 8. Immediately solve the incident that cause or may cause serious impact when receiving permission or investigation report from the administration of data security unit or other relevant units; 9. Secure the data that in his or her responsibility in order to avoid unpermitted person to access, use, disclose, copy, change or eradicate data. Article 24 Security of Data Accession Data administration authority must specify measures on data accession security for the accessible of data owner safely. Data administration authority must facilitate the data owner for inspection, monitoring, using and searching of information must be quick, safe and up-to-date. Data owner must be responsible for maintenance, changing and protection of his or her password for unusable of other persons. Article 25 Codification of Data Security Sending or transferring of	

		important electronic data which mainly are financial, banking, investment, and accounting data via computer system. The data administration authority must use the data security code, and the electronic certificate that certified by the Ministry of Posts and Telecommunication in order to secure from unpermitted person in accessing, reading, destroying, using, disclosing, sending, transferring, editing, deleting, changing, and other acts that causing damage. Article 29 Rights of the Data Administration Authority Data Administration Authority has the following rights: 1. Intercept the creating, accessing, sending, receiving, using or disclosing electronic data that effect on the stability of the nation, peace and orderliness of the society; 2. Suspend the service of data owner who violates the agreement or has behavior that causing the damage to data administration authority, peace or orderliness of the society; 3. Delete the electronic data that relating to the stability of the nation, peace and orderliness of the society or the information that slander other persons as proposed by the officer or relevant person; 4. Create the inspection, monitoring and observation units for the security of data system; 5. Eradicate sources of dangerous program, virus, and others; 6. Comply with other rights as specified in the law. Article 30 Obligations of data administration authority Data administration authority has the following obligations:	

		1. Secure specific data of the owner, for the official data shall have the maintenance and administration system in accordance with the level of data security as specified in the Article 22 of this law; 2. Accessing, using, disclosing, providing, updating, terminating, editing, deleting the electronic from the request of data owner; 3. Responsible for the data that have been damaged; 4. Provide information to relevant officers for finding the offender; 5. Administrate the maintenance system and equipment of electronic data; 6. Ensure the accessing, using, disclosing, sending and transferring electronic data without effecting the stability of the nation and the orderliness of the society; 7. Create and update database system, database backup system, secured system, automatic data searching system, data restoring system and others to be ready; 8. Coordinate with Posts and Telecommunication Sectors regarding to secure form attacking data; 9. Ensure the measures regarding to the resolution of technical problems; 10. Research and use information technology to approach the social demand; 11. Comply with other obligations as specified in the law. Article 45 Organization of Electronic Data Protection Inspection Organization of electronic data protection inspection comprises of: 1. Internal inspection	

		organization; 2. External inspection organization. Internal inspection organization is an administration organization of the Electronic Data Protection as specify in Article 40 of this law. External inspection organization comprises of the National Assembly, the Provincial People's Assembly, State Audition Organization, State Inspection Organization, Lao National Front for Development, and Mass Organization. Article 15 Maintenance of Electronic Data Data administration authority can maintain electronic data when necessary from the collection purpose and other purposes. Following by the personal data may be deleted or blocked from accessing, except the law specified in others. Data administration authority must create a list of electronic data maintenance which can be easily check and the maintenance measures and methods must be safe. Data administration authority is able to handover electronic data to other authorities and shall be agreed from the data owner. Article 30 Obligations of data administration authority Data administration authority has the following obligations: 1. Secure specific data of the owner, for the official data shall have the maintenance and administration system in accordance with the level of data security as specified in the Article 22 of this law; 2. Accessing, using, disclosing, providing, updating, terminating, editing, deleting the electronic	

		from the request of data owner; 3. Responsible for the data that have been damaged; 4. Provide information to relevant officers for finding the offender; 5. Administrate the maintenance system and equipment of electronic data; 6. Ensure the accessing, using, disclosing, sending and transferring electronic data without effecting the stability of the nation and the orderliness of the society; 7. Create and update database system, database backup system, secured system, automatic data searching system, data restoring system and others to be ready; 8. Coordinate with Posts and Telecommunication Sectors regarding to secure form attacking data; 9. Ensure the measures regarding to the resolution of technical problems; 10. Research and use information technology to approach the social demand; 11. Comply with other obligations as specified in the law. Article 45 Organization of Electronic Data Protection Inspection Organization of electronic data protection inspection comprises of: 1. Internal inspection organization; 2. External inspection organization. Internal inspection organization is an administration organization of the Electronic Data Protection as specify in Article 40 of this law. External inspection organization comprises of the National	

		Assembly, the Provincial People's Assembly, State Audition Organization, State Inspection Organization, Lao National Front for Development, and Mass Organization.	
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015	Article 21 Consultancy The Division of Post and Telecommunication shall provide consultancy and give advice on safeguarding method and technical solution to individuals, legal entities and organizations in order to reduce data loss, data disturbance, avoiding stopping the operation of computerized system, deterring the spread of computer virus and the attack to data in the computerized system. Article 28 Developing Data Protection Activities To guarantee the safety in the computerized system and the protection of computer data, the post and telecommunication sector, the security sector, service providers and data maintenance persons shall develop activities for sharing knowledge in terms of safety, computer system application to learn about the technique and data protection method within the state organization, private sector and education premises. Article 29 Emergencies Safeguarding The Post and Telecommunication sector shall be the body to safeguard emergencies through the monitoring, inspection, giving advice, warning notice, protection and response to the dangers occurred in the computer system. Article 44 Announcement, Reporting or Petition Announcement, reporting or petition regarding cybercrime	

		offense shall be made or submitted to the police investigation-interrogation authority or to the Public Prosecution Authority. The police investigation-interrogation authority or the Public Prosecution Authority shall consider making announcement, reporting or petition no later than fifty business days from the date of receiving announcement, report or petition onward. In case of complexity, such consideration shall not exceed ten business days. Article 45 Opening of Investigation-Interrogation In case of having strong information regarding cybercrime, the head of the police investigation-interrogation authority or the head of the public prosecution authority shall issue an order to open the investigation-interrogation within the scope of its rights and responsibilities as specified in the Law on criminal procedures. In case of necessity, urgency and availability of data proving of any cybercrime plan or action, the head of police investigation-interrogation authority or the head of the Public Prosecution shall issue an instruction/order to keep and protect computer data or data circulated through the computerized system. The service provider or data management sector shall have an obligation to keep and protect such data in good form until the end of the case proceedings in order to guarantee that there are no changes or loss to the data. Article 46 Investigation-Interrogation Proceedings The policy investigation-	

		interrogation authority or the Public Prosecution Authority shall collaborate with the Post and Telecommunication Sector and other relevant sectors to conduct a search for data, evidence and the background of cybercrime to be used as reference for the investigation-interrogation process. The investigation-interrogation proceedings for computer related cases shall apply the investigation-interrogation method, restraining measures and time limit for the investigation-interrogation as specified in the Law on Criminal Procedures. Article 47 Summarizing of Investigation-Interrogation and Completion of Case File After ending the investigation-interrogation by police officer, if there is no strong evidence proving that such infringement is offense on computerized system, the investigation-interrogation authority shall summarize and complete case file in order to submit to the Public Prosecution Authority for consideration and lodge a lawsuit to the court. In case that the Public Prosecution Authority is the body conducting investigation-interrogation, such authority shall summarize, complete case file, issue an indictment order and statement to the court for consideration making case sentence in accordance with the law. Article 48 Management Authority The Government is in charge of managing the cybercrime resistance and prevention activities in a centralized and uniformed manner throughout the country by assigning the	

		Ministry of Post and Telecommunication to directly responsible for and to take initiative in collaborating with the Ministry of National Defense, Ministry of Public Security, Ministry of Information, Culture and Tourism, Ministry of Sciences and Technology, other ministries and local administration concerned. The Authority in charge of the management of cybercrime resistance and prevention activities comprises of: 1. Ministry of Post and Telecommunication; 2. Division of Post and Telecommunication of provincial, city level; 3. Office of Post and Telecommunication at district, municipality level. Article 53 Inspection Authority The Cybercrime Resistance and Prevention Activities Inspection Authority comprises of: 1. The Internal Inspection Authority which is the same authority as the Authority in charge of the management of cybercrime resistance and prevention activities as specified in Article 48 of this law; 2. The External Inspection Authority which includes the National Assembly, the State Audit Authority, the Government Inspection Anti-Corruption Authority, the Lao Front for National Construction and the mass organization.	
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018	Chapter 2 8. Article 15 Electronic data storage is the management and maintenance of data to ensure that the data is safe, not lost, damaged as well as to facilitate quick access and Use. Data managers must define measures and methods of safe storage,	

		such as creating an archive Maintain electronic information that can be easily checked, information security level, authorization Data access, data retention period, data backup, etc. For example: any information service center must keep your information, such as phone history or sending information via electronic mail, for at least 90 days, after the deadline, your information may be deleted, block access or comply with the agreement of both parties. Chapter 2 17. Article 25 Security encryption is to maintain the confidentiality of information by encoding information to prevent information from being accessed, read, destroyed, used, disclosed, sent, transferred, updated, deleted, changed and other actions that cause damage. For example: Data managers must use the electronic certificate (Certificate Authority) on the system to provide information services, encryption in PGP (Pretty Good Privacy) format when sending or transferring important electronic data through electronic mail (email), encryption of electronic data in normal format and other formats to be correct according to security standards. For data security encryption, details are provided in the Computer Security Guidelines, Chapter 2 11. Article 18 Access to electronic information is access to general information or specific information to use and disclose according to work requirements. In the case of individuals, legal entities or organizations with the	

		purpose of accessing specific information, they must submit to the relevant data manager for research, consideration according to laws and regulations Chapter 2 18. Article 26 Response to data intrusion is to check and collect information, evidence about the intrusion as well as coordinate with relevant parties to stop and solve the incident in a timely manner. In the case of receiving a notification from an individual, legal entity or organization, the data manager must quickly check, analyze, manage, correct, notify and define various protection methods to prevent data intrusion again. Data managers must report emergencies to the Computer Emergency Prevention and Resolution Center of the Ministry of Posts, Telecommunications and Communications in order to collect information, coordinate and take corrective actions in a timely manner.	
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018	Chapter 2 11. Article 20 Notification is the Ministry of Posts, Telecommunications and Communications as the notification. Dangers that occur in computer systems and the Internet, such as notifications of fake websites, programs malicious intent, computer system vulnerability reporting, electronic mail fraud, etc. In the event that a virus is found that is spreading in the company and abroad, the Ministry of Posts, Telecommunications and Communications must issue a warning as well as advise how to prevent the virus so that the managers Channels and users of domestic computer systems take	

		note. The computer system service provider must notify and set conditions for accessing the computer system to limit or not allow certain types of service users to access the computer system. For example: The Company, which is the manager of the computer system, received a notification about the spread of the Wanna Cry virus. It must issue a notification as well as advise how to prevent the virus for the users of the computer system to be informed. 12. Article 21 Counseling is the post, telecommunications and communication sector as a consultant, recommending prevention methods and technical solutions such as: finding the source of computer system attacks, proving electronic evidence, correcting computer system vulnerabilities, correcting the phenomenon through online social media, including counseling on work to combat and prevent computer crime to individuals, legal entities and organizations in order to reduce data loss, data disturbance, not to Stopping the functioning of the computer system, preventing the spread of computer viruses and the destruction of information in the computer system. For example: The company's server system was attacked by hackers, causing the server system to be unable to operate normally and causing damage to the company. The company should request advice and guidance from the Computer Emergency Prevention and Resolution Center, Ministry of Posts, Telecommunications and Communications to check, find the source of the attack and improve the system to be able to return to normal use.	

		Chapter 2 15. Article 28 Creation of data protection activities to ensure computer system security and computer data protection The postal, telecommunication and communication sectors, the peace protection sector, service providers and data custodians must create activities to provide knowledge on security, the use of computer systems to know the techniques and methods of data protection according to public, private and educational institutions. For example: The Computer Emergency Prevention and Resolution Center has created activities related to cyber security by distributing Chapter 2 20. Article 44 Informing, reporting or complaining about computer system crimes. Individuals, legal entities or organizations can notify or submit to the police investigation agency or public prosecutor's office such as computer system crimes or computer system crimes specified in Article 8 of the Law on Combating and Suppressing Computer Crimes. The investigative agency of the police officer or public prosecutor's office must consider the notification, report or petition within five business days from the date of receipt of the notification, report or petition. For example: He has edited her photo and posted it on Facebook without permission, which will cause damage to her. If she wants to claim justice, she must bring information and evidence to inform the investigation agency of the police officer to consider according to	

		the principle of computer investigation.	
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018	Article 21 Sending and receiving electronic information Sending and receiving electronic information must be done as follows: 1. The initiator of the communication may be the owner of the information himself or a representative who must identify himself when sending electronic information, for the representative must have a power of attorney; 2. The owner of the information can create an information system to send information through an automatic system, In the case of a representative sending information through an automatic system, the identity must be identified and verified Data owner at any time: 3. The recipient of the communication must check the accuracy of the electronic data according to the method determined by the originator of the communication or according to the agreement of the originator and the recipient of the communication; 4. In the event of any error which the originator of the communication has informed the recipient of the communication within the agreed upon time to consider the electronic data sent as invalid; 5. In case of receiving the same or similar electronic data from multiple transmissions, take the first electronic data as the main one if not notified by the originator of the communication: 6. The time of transmission shall be taken according to the actual time that the electronic data was sent from the electronic system of the initiator of the communication;	

		7. The time of receipt shall be taken according to the actual time that the electronic data entered the electronic system of the recipient of the communication; 8. The location of sending or receiving electronic data shall be based on the location referred to by the originator of the communication or the recipient of the communication, in case the originator of the communication or the recipient of the communication does not have a reference location shall be the location where the electronic data is actually sent or received or as agreed by the originator and the recipient of the communication. Article 36 Technical standards for issuing electronic signature certificates General electronic signature certificate issuers must have the following service technical standards: 1. Store the information of the holder of the electronic signature certificate completely, correctly and up-to-date until the expiration date of the electronic signature certificate; 2. Store the list of electronic signature certificates that are still valid and have expired in the data collection system in a complete, accurate and up-to-date manner as well as guarantee access to the said system around the clock; 3. Have a system that can detect, warn and block attacks and unauthorized connections through computer systems; 4. There is a backup system to ensure that the system works properly and safely In case of system failure; 5. All technical systems used in providing	

		services must be in Lao PDR; 6. Buildings equipped with technical systems must have a fire or natural disaster protection system; 7. Other technical standards set by the Ministry of Posts, Telecommunications and Communications. Article 53 Rights and obligations of the issuer of the general electronic signature certificate The issuer of the general electronic signature certificate has the following rights and obligations: 1. Provide electronic signature certification services as authorized; which is related to electronic signature certification services only, unless the law stipulates otherwise: 2. Store user information securely, confidentially and for work-specific use 3. Extend, suspend or cancel the electronic signature certificate of the holder of the signature certificate General electronics; 4. Advise holders of general electronic signature certificates on how to use electronic signature certificates; 5. Use as a substitute for damages caused by defects in technical systems or from providing services its own; 6. Complain to related parties in case their rights are violated; 7. Comply with the regulations regarding reasonable prices and services; 8. Report activities to the Electronic Signature Certification Management Agency regularly; 9. Use rights and fulfill other obligations as defined in the law. Article 54 Rights and obligations of public and private electronic signature certificate issuers	

		Public and private electronic signature certificate issuers have the following rights and obligations: 1. Choose a technique or store information about issuing an electronic signature certificate; 2. Create regulations on the use of electronic signature certificates based on policy Rules and regulations set by the national electronic signature certificate issuer; 3. Store the certificate holder's information such as electronics securely and confidentially; 4. Extend, suspend or cancel the service user's electronic signature certificate; 5. Advise service users on how to use electronic signature certificates; 6. Be responsible for damages caused by defects in the technical system or from the provision of its services; 7. Regularly report on the activities of issuing electronic signature certificates to the Ministry of Posts, Telecommunications and Communications; 8. Use rights and fulfill other obligations as stipulated in the law.	
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017	V. Coordination and Cooperation Solving emergency problems happened to computer in data center shall be acted as follows: 1. Data center shall establish a computer safety unit to coordinate for the defense and	

		emergency solving work (Lao CERT center); 2. Apply the process, technical standards when solving emergency problems happened to computers; 3. Create and notify address, phone number and email to relevant organizations or computer emergency defense units; 4. Coordinate to organize technical trainings, practicing to solve and respond to computer emergencies.	
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014		
10	Decree on E-commerce No. 296/GOV	Article 34 Data protection Data protection in electronic commerce channels is the use of methods and measures to prevent access, use, disclosure, modification, transmission, transfer or destruction of personal information stored without the permission of the owner of the information or relevant management agencies. In the conduct of electronic business, the owner of the electronic channel can store the customer's information or give the right to another person who must comply with the law on the protection of electronic information, other related laws and regulations. Article 36 Obligations of buyers through their electronic channels Traders through their electronic channels have the following obligations: 1. Notification of electronic commerce to the industrial and commercial sector; 2. Provide complete and accurate information about	

		products and services; 3. Comply with data protection regulations; 4. Be legally responsible for the products or services brought to sell, exchange or provide services in their electronic commerce channels; 5. Create a mechanism for customers to give feedback on products or services and disclose such feedback in their electronic commerce channel as well as a mechanism for customers to check, modify or delete their comments at any time; 6. Provide information and store information about its business operations according to laws and regulations; 7. Cooperate with the Electronic Commerce Management Organization regarding electronic commerce; 8. Use payment tools or payment methods of payment service providers authorized by the Bank of Lao PDR to pay for goods or services; 9. Perform other obligations according to laws and regulations. Article 40 Obligations of electronic market service providers Electronic market service providers have the following obligations: 1. Display information on enterprise registration and business license on the main page of the electronic commerce channel; 2. Determine and display the terms of electronic market services; 3. Store the customer's information in the electronic market; 4. Create a mechanism for buyers to be able to present information about goods or services as well as a mechanism for checking and monitoring; 5. Create a mechanism for customers to provide feedback on products or services and disclose such	

		feedback on their electronic channels as well as a mechanism for customers to review, modify or delete their comments; 6. Create a mechanism for merchants and customers to create commercial contracts electronically; 7. Comply with the requirements regarding the protection of electronic commercial information; 8. Determine appropriate and timely remedial measures in the event of a conflict or violation of the law in its electronic market; 9. Provide information and store information about its business operations according to the law and regulations; 10. Cooperate with the Electronic Commerce Management Organization regarding electronic commerce; 11. Use payment tools or payment methods of payment service providers authorized by the Bank of the Lao PDR to pay for goods or services; 12. Use delivery services from service providers authorized by law; 13. Perform other obligations according to laws and regulations.	
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020	Article 13 Maintenance of user information User information is personal information, financial information, passwords such as ATM card code, e-view code, mobile bank code. The service provider must keep the user's information and not disclose it to other unauthorized persons or Organizations that do not have relevant authority. User information can be stored in paper and electronic form. service provider It is necessary to notify and advise users how to store passwords. In the event that users' password information is leaked or disclosed without	

		permission, the service provider must record and notify the affected users immediately. In the event that the leak or disclosure creates a serious or widespread impact, the service provider must record and report to the management and inspection organization to protect financial service users urgently. The service provider will be able to disclose the user's information to a third party after receiving written consent from the user. In the case of disclosure of information to the competent authority must act according to the relevant law. 5 Article 18 Card services In the card service, the service provider must act as follows: 1. Make a card service contract with the main content namely Features, methods of use and restrictions on the use of cards; Fees for cash withdrawals, card usage at home and abroad; Responsibilities and obligations of service providers and users in case of card loss, suspension, theft or stolen card information; Determine the debt ratio or the amount of money that must be paid each month for the credit card. 2. Keep the card code safe and confidential; 3. Be responsible for the damage that occurs during the delivery of the card and card code to the person Use: 4. Open the opportunity for users to suspend or cancel the use of the card at any time free of charge. Article 20 Rights and obligations of service providers Provide services with the following terms and conditions: Person 1. Provide financial services according to the authorized scope; 2. Determine	

		appropriate policies and procedures to manage the risk of damage loss to users from providing their services; 3. Assess the appropriateness of financial services for target users; 4. Advertise or disclose information about financial services completely, accurately and Clear for users to recognize and understand before deciding to use the service; 5. Service to users accurately, transparently and fairly; 6. Create an internal mechanism to receive and correct suggestions from users as well as to cooperate in the work such; 7. Keep information about users confidential; 8. Report on user protection work to the Bank of Lao PDR on a regular basis. In case there is a problem that may affect users in a wide range, it must be reported to the Bank of the Lao PDR urgently; 9. Exercising rights and fulfilling other obligations according to laws and regulations. Article 24 Prohibitions for the employees of the management and inspection organization to protect the users of financial services Prohibit employees of management and inspection agencies from protecting users of health services Finance behaves as follows: 1. Acting in a biased or illegal manner; 2. Receiving bribes or demanding benefits related to the work of managing and inspecting protection users of financial services; 3. Falsifying documents or using fake documents, revealing secrets, suppressing or destroying documents related to the protection of financial service users; 4. Behavior that violates laws and regulations.	

12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012	Article 8. Right and Functions of CIC Member The members of CIC shall have the main rights as follows: 1. 1. Implement provision, regulations and other legislative related to the credit information task issued by the Bank of the Lao PDR; 2. Develop the credit information program, such as the database system, to be fully in accordance with the credit information reporting standard issued by the Bank of the Lao PDR; 3. Collect, provide credit information in an accurate, complete, precise and timely manner as specified in this Decision. All changes made to the customer's credit information shall be recorded by the CIC members; 4. Maintain confidentiality and apply the credit information as specified in the regulation; 5. Train and recruit staff working in the credit information sufficiently and effectively; 6. Pay service charge for the search and use of credit information in accordance with the regulation issued by the Bank of the Lao PDR; 7. Exercise other rights and perform other duties assigned by the CIC. Article 6. Rights and Functions of the CIC The CIC shall have the right and functions as follow: 1. Study the policy and regulation for the management of credit information tasks in order to submit to the Governor of the Bank of Lao PDR for consideration and approval; 2. Collect general information, information on credit, financial status and other information from its members, as well as	

		safely maintain such information in the database system; 3. Summarize, use the credit information, create product in order to supply to its member and individuals who have connection with in accordance with the regulations of CIC; 4. Develop the credit information system to become up-to-date, create diverse products to serve its members and society; 5. Set up the standard form for credit information reporting to be used by its members; 6. Guarantee the efficiency and safety in the administration of credit information; 7. Provide the credit information to relevant sectors of the Bank of the Lao PDR in order to apply in the task for the management of commercial banks and in other tasks; 8. Provide training on the credit information tasks to CIC staff and members in order to raise their skill in the credit information tasks; 9. Coordinate with other relevant sectors to successfully perform the CIC role and responsibility; 10. Guarantee the exercise of right and duties of its members based on the regulations in a strict manner, redress the problem in providing inaccurate information as proposed by the customers of the member; 11. Inspect credit information of the members as specified in this Decision; 12. Impose measures to members who violates the regulation on the management of credit information. 13. Exercise other rights and perform duties as assigned by the Director General of Department. Article 9. Recording Credit	

		Information 1. CIC members must have the database system to serve the credit information tasks. All credit information must be recorded in a full and precise manner based on the credit information reporting standard set out by the Bank of the Lao PDR; 2. All the changes made to the customer's credit information shall be recorded in a full and timely manner.	
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020	Section 8 Location and safety standards Article 41 Standards for service providers issuing electronic signature certificates The electronic signature certification service must include the following 1. Location - The service facility must have a closed-circuit camera system to monitor the recording of the incident in the location - Service providers must allocate space and install appropriate systems to ensure protection 2. Entering the equipment control room - Entry-exit control equipment installed in the electronic signature certificate service must only be the personnel assigned by the service provider who has access-exit rights to the area which controls entry-exit with smart card access control device, fingerprint verification device (Finger Scan) with the use of a password, and a sound system when the door is opened (Door Hold Open Sounder). 3. Electrical system and air	

		conditioning system -The service provider must have a main generator and a backup generator to protect the system in the event of a power failure; There is an air conditioning system to control the heat and humidity of the room to be constant, separate from the air conditioning system in the building. 4. Fire prevention -The area where the electronic signature certificate is installed must be equipped with a fire protection system that has special features that do not damage electrical and electronic equipment and has been certified to ensure fire safety. Article 42 System security standards The security standards for issuing electronic signature certificates are as follows: 1. must ensure the security of all information of service users from being destroyed, changed or stolen; 2. There must be a backup system to ensure that it can be used regularly; 3. Must ensure the security of the system so as not to be a vulnerability used by unscrupulous people to attack, damage (or cause damage to) others; 4. There is a notification system to prevent attacks and unauthorized connections through the computer system 5. The equipment used to record or store information, if it is damaged or not used, must be destroyed in an appropriate way to ensure that the information cannot be reused or searched again; 6. Important backups must be stored off-site to prevent data	

		loss in the event of an emergency; 7. All technical systems used in providing services must be located in Lao PDR; 8. Other technical standards set by the Ministry of Posts, Telecommunications and Communications. Chapter 9 Specific technical standards Article 43 Key Pair Generation and Installation Providers of electronic signature certificates must generate and install key pairs for electronic signature certificates as follows: 1. Key Pair Generation must comply with Federal Information Processing standard (FIPS) 140-2 Level 3; 2. Delivery of private key (Private Key Delivery to Subscriber) must determine the procedure Safe delivery of private keys to service users; 3. Public key delivery (Public Key Delivery to Certificate Issuer) must be specified transmission of public keys and identification information of users of the Service; 4. Public Key Delivery to Relying Parties (CA Public Key Delivery to Relying Parties) must determine the access channel to the public key of the relevant partner; 5. The size of the key pair (Key Sizes) must use the RSA method with the length of the key pair being 2,048 bits. Article 44 Private Key Protection and Cryptographic Module Engineering Controls Providers of certificates such as electronic certificates must protect private keys and manage devices for encryption as follows:	

		1. Cryptographic Module Standards and Controls and Cryptographic Module Rating must Compliance with Federal Information Processing standard (FIPS) 140-2 Level 3; 2. Private Key Multi-person Control (Private Key Multi-person Control) must have at least 02 reliable personnel in charge of access management; 3. Private Key Backup must comply with Federal Information Processing standard (FIPS) 140-2 Level 3; 4. Private Key Archival records must be stored in a secure facility and in an appropriate period of time; 5. Private Key Transfer into or from a Cryptographic Module (Private Key Transfer into or from a Cryptographic Module) must have at least 02 reliable personnel responsible for this function; 6. Private Key Storage on Cryptographic Module (Private Key Storage on Cryptographic Module) must be stored in the key management device and private key backup in the key storage device: 7. Activating the private key (Method of Activating Private Key) must be done by at least 02 designated personnel and must have the correct password; 8. Canceling the use of private key (Method of Deactivating Private Key) must leave the system (Log Out) immediately at the end of use; 9. The method of destroying the private key (Method of Destroying Private Key) must arrange for the destruction of the private key when the use is canceled by an appropriate process and ensure security, Article 46 Information used to	

		install the electronic signature certificate (Activation Data) The electronic signature certificate service provider must perform the following steps when using the information to install the electronic signature certificate: 1. Creation and configuration of data for activating the private key (Activation Data Generation and Installation) must be carried out in the process of installing the key management device by the person who has the right to operation and must have a valid password; 2. Protection of the data used to activate the private key (Activation Data Protection) must be determined to verify the identity of the person before activating the private key every time, 3. The security management of the computer system (Computer Security Controls) must have appropriate technical requirements and details about the security of the computer system (Specific Computer Security Technical Requirements) and the security level of the computer system (Computer Security Rating) must be in accordance with the standards set by the national electronic signature certificate issuer. Article 47 Technical management of the service system (Life Cycle Technical Controls) Service providers issuing electronic signature certificates must manage the technical aspects of the service system by following the following methods: 1. System Development Controls must have a verification process before installing the software	

		used in the system; 2. Security Management Controls must Control the management of security in accessing the service system and using the system appropriately and ensure security; 3. Network Security Controls must define a specific channel to access the network; 4. Time-stamping must be installed in accordance with the standard time setting device (NTP Server) by the device related to the electronic signature certificate service system that refers to the time from the same device. 1. The format of the electronic signature certificate (Certificate Profile) must conform to the ITU-T X.509 version 3 standard and the RFC 5280 Internet X.509 Public Key Infrastructure Certificate and CRL standard as a minimum. 1.1. The additional part of the electronic certificate (Certificate Extensions) must conform to the ITU- T X.509 standard and the RFC 5280 standard as a minimum and must include the following information: - The purpose of key usage (Key Usage) must be specified in the electronic signature certificate with at least a digital signature, key Cert Sign and CRL Sign. - Certificate revocation information (CRL Distribution Points) must determine the channel that can access the electronic signature certificate revocation list. - Authority Key Identifier (Authority Key Identifier) (must specify the identity of the issuer of the electronic signature certificate in the electronic signature certificate. - Key usage information (Subject	

		Key Identifier) must be specified in the electronic signature certificate. 1.2. Name Forms must specify the information of the issuer (Issuer) and use (Subject) in detail, such as the country name (Country (C)), organization name (Organization (O)), and common name (CN). 2. The electronic signature certificate cancellation list (Certification Revocation List (CRL) Profile) must specify information about the cancellation list format, such as the key certification information (Authority Key Identifier) and the number of the cancellation list (Base CRL Number) in accordance with the ITU-T X.509 version 2 standard and the RFC 5280 standard at least. 3. The protocol format (Online Certificate Status Protocol (OCSP) Profile) must allow to check the status of the electronic certificate. Article 49 Rights and obligations of service providers The electronic signature service provider has the following rights and obligations: 1. Proposing to continue, change, suspend or cancel its operations; 2. Suspend service to service users who violate laws and regulations; 3. To cooperate with postal, telecommunication and communication officials and organizations management-inspection involved in management and inspection; 4. Keep the service user's information confidential and secure, unless instructed by the organization Organizations with relevant authority: 5. Under the management and	

		supervision of the Ministry of Posts, Telecommunications and Communications; 6. Assign obligations according to laws and regulations; 7. Perform other rights and obligations as defined in laws and regulations, Article 54 Prohibition for service management staff It is prohibited for management staff or public sector organizations responsible for service management to issue electronic signature certificates with the following behavior: 1. Access the electronic signature certification system and disclose information about electronic signature certification without permission; 2. Modify, destroy or disclose official secret information without permission; 3. Disregarding or neglecting their responsibilities; 4. Other behavior that violates laws and regulations.	
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016	Article 15 Database of government organizations The database of government organizations is a database that stores information in electronic form of ministries, government agencies equivalent to ministries and local government agencies, including other state organizations, parties, so that government organizations, business units and society can use such information through programs, websites or other online formats. Government organizations that have their own Internet Information Center must store databases and information in their own centers and must have a backup system for such databases and information in the National Internet Information	

		Center. For government organizations that do not have their own Internet Information Center, they must store their databases and information only in the National Internet Information Center. Article 16 Dissemination of information through the Internet of government organizations Ministries, government agencies equivalent to ministries and local government agencies at the provincial level can have websites, programs or other channels to provide services or provide information to government organizations, business units and society as appropriate. Websites and e-mails of government organizations must use the national Internet name code of the Lao PDR and store it in their center. If you don't have your own center, keep it in the information center through the national internet. Ministries, government agencies equivalent to ministries and local government agencies at the provincial level that disseminate information via the Internet must comply with relevant laws and regulations and must be responsible for the content of the information they disseminate. Article 17 Conditions for disseminating information through the Internet of government organizations Dissemination of information through the Internet of government organizations must comply with the following conditions: 1. Ensure convenient, accurate and safe access to information; 2. Update information regularly and promptly;	

		3. There is an information search tool that is easy to use and practical; 4. Guarantee the service at any time, in case of not being able to provide the service must be notified through the website or its office at least seven business days except for unforeseen circumstances. Article 26 Security measures Legal entities or Organizations that have an information center through internet must organize all activities To ensure safety as follows: 1. There are staff responsible for safety management, planning and problem solving; 2. There is a technical system that has been improved, upgraded gradually to keep up with the changes 3. There are specific regulations to unify and increase the number of incoming internal and external controls Article 27 Information security guarantee The management of service user information and personal information that is stored in the Internet Information Center must ensure that it is not stolen, changed, destroyed or deleted by complying with the laws and regulations on the management of personal information, fraud and computer crimes and other related laws. Electronic information that is a government secret must be classified, stored and protected as specified in the relevant laws and regulations. Electronic information must be backed up with the same level of security as the main electronic information Access to the database and	

		information must use a password that is sufficiently complex and 3 changed regularly to ensure security, Part V Recruitment and development of personnel Article 29 Personnel composition The information center, both public and private, must include personnel with knowledge of information technology both at the center and local level according to the appropriateness of the work related to the information center through the Internet, database and other information technology work within the scope of responsibility of the sector. Article 42 Rights and Obligations of Internet Information Center Service Providers Legal entities or organizations that provide Internet Information Center services have the following rights and obligations: 1. Proposing to continue, change, suspend or cancel the operation of its business; 2. Suspend service to service users who violate the contract or have behavior that may cause damage to the center, peace or social order; 3. Comply with the regulations of the Ministry of Posts, Telecommunications and Communications domestic and international network connections; 4. Respect the rights and store personal information of service users with regulations and technical systems to create and 5. Record usage information and report technical information to the postal sector, telecommunications and	

		communications; 6. Do not disclose personal information of users of the service except with the proposal of the relevant government organization; 7. Provide services as promised or notified to service users; 8. There are measures to solve problems and technical problems for users clearly through its website and clearly defined in the service contract for users; 9. Use live and perform other obligations as defined in laws and regulations.	
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No 224/GOV dated July 19, 2019	Article 11 Maintenance of credit information Credit information must be stored in a standardized database as determined by the Bank of the Lao PDR and backed up to ensure the security and continuity of providing such information. Credit information must be kept for at least ten years from the date the information was stored or updated for the last time.	
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		

20	The Penal Code No.26/NA datd May 17, 2017		

#	Regulation	internal	internal
		Accuracy	Retention Limitation
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	Article 13 Inspection of Electronic Data Data owner and data administration authority must inspect and ensure the correction and completion of data in order to ensure that the content of data is not contradict with the laws and regulations, and shall not impact on the Socio-Economic Development, the stability of the nation, peace and orderliness of the society. Article 26 Responding to Data Attacks Responding to data attacks shall comply as following: 1. Data administration authority uses interception and fixed methods when have been informed by individual, legal entities or organizations that relating to sending of data that cause or may cause unpeaceful of the society; 2. Data administration authority coordinates with relevant sectors to collect attacked information and evidence such as date, time, location, form, and amount of attacks; the effect and source of attack for fixing. In case of unable to fix, shall inform the Computer Emergency Interception and Resolution Center, the Ministry of Posts and Telecommunication; 3. Computer Emergency Interception and Resolution Center coordinates with the Data Security Administration Unit of data administration authority and other relevant sectors both domestic and international in	Article 20 Deleting of Electronic Data Data administration authority must delete electronic data that they collected as proposed by the data owner or when using purpose is terminated, the collection is expired or as specify in the Article 29 section 3 of this law. Deleting of electronic data must inform the data owner, except the law is specified in others

		order to restrain and fix the incident on time.	
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015		
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018		Chapter 2 8. Article 15 Electronic data storage is the management and maintenance of data to ensure that the data is safe, not lost, damaged as well as to facilitate quick access and Use. Data managers must define measures and methods of safe storage, such as creating an archive Maintain electronic information that can be easily checked, information security level, authorization Data access, data retention period, data backup, etc. For example: any information service center must keep your information, such as phone history or sending information via electronic mail, for at least 90 days, after the deadline, your information may be deleted, block access or comply with the agreement of both parties.
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no.	Article 39 Agents provide services The issuer of the general	

	59/NA, dated 12 December 2018	electronic signature certificate can allow any person or legal entity to act as its representative in the registration service, check the accuracy and completeness of the application and information of the applicant for the electronic signature certificate before sending it to the issuer of the general electronic signature certificate to consider issuing the electronic signature certificate. The general electronic signature certificate issuer must notify the national electronic signature certificate issuer about its representative within thirty days from the date of the representation contract. The conditions and procedures for representation are defined in separate regulations. Article 36 Technical standards for issuing electronic signature certificates General electronic signature certificate issuers must have the following service technical standards: 1. Store the information of the holder of the electronic signature certificate completely, correctly and up-to-date until the expiration date of the electronic signature certificate; 2. Store the list of electronic signature certificates that are still valid and have expired in the data collection system in a complete, accurate and up-to-date manner as well as guarantee access to the said system around the clock; 3. Have a system that can detect, warn and block attacks and unauthorized connections through computer systems; 4. There is a backup system to ensure that the system works properly and safely In case of system failure; 5. All technical	

		systems used in providing services must be in Lao PDR; 6. Buildings equipped with technical systems must have a fire or natural disaster protection system; 7. Other technical standards set by the Ministry of Posts, Telecommunications and Communications.	
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014		
10	Decree on E-commerce No. 296/GOV		
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020		
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012	Article 4. Exchange of Information Before consider giving credit to customer, the members of the CIC shall obtain a written consent from their customer to allow the CIC of the Bank of Lao PDR and its members to apply the general information, credit	Article 11. Keeping of Credit Information CIC members shall keep the credit information as follows: 1. Regular debt of customer, problematical debt in which payment cannot be made under the term provided in the agreement, shall be kept in a

		information, financial status and other information available in the reporting form set out by the Bank of the Lao PDR to disclose and exchange with members or to be used in any objectives in accordance with the regulation of the CIC. The disclosure and exchange of information shall guarantee the accuracy and reality. Article 6. Rights and Functions of the CIC The CIC shall have the right and functions as follow: 1. Study the policy and regulation for the management of credit information tasks in order to submit to the Governor of the Bank of Lao PDR for consideration and approval; 2. Collect general information, information on credit, financial status and other information from its members, as well as safely maintain such information in the database system; 3. Summarize, use the credit information, create product in order to supply to its member and individuals who have connection with in accordance with the regulations of CIC; 4. Develop the credit information system to become up-to-date, create diverse products to serve its members and society; 5. Set up the standard form for credit information reporting to be used by its members; 6. Guarantee the efficiency and safety in the administration of credit information; 7. Provide the credit information to relevant sectors of the Bank of the Lao PDR in order to apply in the task for the management of commercial banks and in other tasks; 8. Provide training on the credit information tasks to CIC staff and	safe database system; 2. Debt which has been fully paid or has been washed out from the balance sheet of asset shall be kept in the database system for a minimum of 5 years.

		members in order to raise their skill in the credit information tasks; 9. Coordinate with other relevant sectors to successfully perform the CIC role and responsibility; 10. Guarantee the exercise of right and duties of its members based on the regulations in a strict manner, redress the problem in providing inaccurate information as proposed by the customers of the member; 11. Inspect credit information of the members as specified in this Decision; 12. Impose measures to members who violates the regulation on the management of credit information. 13. Exercise other rights and perform duties as assigned by the Director General of Department. Article 9. Recording Credit Information 1. CIC members must have the database system to serve the credit information tasks. All credit information must be recorded in a full and precise manner based on the credit information reporting standard set out by the Bank of the Lao PDR; 2. All the changes made to the customer's credit information shall be recorded in a full and timely manner. Article 20. Conflict Resolution Customers of CIC member who find mistake in their credit information can submit an application to CIC to solve such mistaken information. The content of the application must show the inaccurate information and the need to modify. After receiving an application from its customer, CIC must	

		inspect such information in order to redress the customer's application within 30 banking business days. CIC must inform the result of modifying the customer's application in written either directly or by post or electronic mail.	
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		Article 45 Other Aspects of Key Pair Management Electronic signature certificate service providers must manage key pairs according to the following principles: 1. Public Key Archival records must be stored in a secure device and in an appropriate period of time; 2. Certificate Operational Periods and Key Pair Usage Periods are determined by the issuer of the electronic signature certificate of nation.
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016		
16	Decision on consumer protection for telecommunicati on and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No 224/GOV dated July 19, 2019	Article 10 Data collection Credit Information Company of Lao PDR collects credit information from members and stakeholders according to the prescribed format. After collecting information or receiving credit information	Article 11 Maintenance of credit information Credit information must be stored in a standardized database as determined by the Bank of the Lao PDR and backed up to ensure the security and continuity of providing such

		The Credit Information Company of Lao PDR must check the information using technology and technical techniques to filter, edit the information to be accurate and complete, and record it in the database. Members and stakeholders are responsible for providing information to the Credit Information Company of the Lao PDR from time to time or as requested by the Credit Information Company of the Lao PDR. Article 14 Correction of wrong information Members must be responsible for correcting the credit information sent incorrectly according to the credit information report form and report to the credit information company of the Lao PDR within five business days. In case the Credit Information Company of Lao PDR finds credit information of poor quality, it must notify the member to correct the information and report to the Credit Information Company of Lao PDR within five business days. In case any member finds the credit information of his/her customer with another member or related person to be incorrect, he/she must notify the Credit Information Company of Lao PDR in writing to coordinate with the other member or related person to correct it. If the relevant person finds that the reported credit information is incorrect or wrong, he must report it to the Credit Information Company of Lao PDR or a member of the company with whom he has a contractual relationship to correct the information within five business days.	information. Credit information must be kept for at least ten years from the date the information was stored or updated for the last time.

18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA datd May 17, 2017		

#	Regulation	internal	internal
		drawing up of codes of conduct	record of processing activities
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017		
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015		
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018		
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated		

	24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018		
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014		
10	Decree on E-commerce No. 296/GOV		
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020		
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012		
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		

14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016		
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No 224/GOV dated July 19, 2019	Article 31 Rights and obligations of members Members of the Credit Information Company of the Lao PDR have the following rights and obligations: 1. Collect, provide information and be responsible for the accuracy, completeness, clarity and timeliness according to the report form of the Credit Information Company of the Lao PDR; 2. Develop and improve the technology system to support the credit information system of the Bank of the Lao PDR; 3. Create regulations, manuals for the use and reporting of credit information; 4. Inspect, update and correct erroneous information on time; 5. Use credit information products in accordance with the regulations of the Lao PDR Trust Information Company; 6. Lose the service charge for using credit information according to the regulations of	

		the information company Credit Court of Lao PDR; 7. Appoint staff or units responsible for implementing credit information work; 8. Report credit information work according to regulations; 9. Use rights and perform other obligations as defined in laws and regulations.	
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA datd May 17, 2017		

#	Regulation	internal	internal
		Designation of the data protection officer	Others
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017		
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015		
3	Guideline on the implementation of the Law on Electronic Data		

	Protection no. 2126/MPT, dated 8 August 2018		
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018		
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012		
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014		
10	Decree on E-commerce No. 296/GOV		
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020		
12	Decision on the Activities		

	Regarding Credit Information No. 928/BoL, dated 20 September 2012		
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016		
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No 224/GOV dated July 19, 2019		
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016		
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		

20	The Penal Code No.26/NA datd May 17, 2017		

Data Cross Boarder Dist

#	Regulation	Cross-border data transfer & Exceptions	Data localization
		Provisions for Transborder Data Transfer. What are the exceptions? (e.g., sufficient authorization, transfers based on contracts equivalent to Standard Contract Clauses (SCC) or Binding Corporate Rules (BCR), transfers based on corporate certification, etc.), Transborder transfer assessment (TIA)	Presence or absence of provisions, stipulations regarding the types of data that must be stored in the country
		Provisions for cross boarder data transfer	Provisions on requirement of localization; and Type of data required for localization
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	Article 17 Sending or Transferring of Electronic Data Sending or transferring of electronic data shall comply as following: 1. Have permission from the data owner and ensure the receiver is able to secure those data; 2. Input data security for the important data which mainly are financial, banking, investment and accounting data; 3. Do not falsify data sources that have been sent and transferred; 4. Consistent with the agreement between sender and receiver; 5. Stop sending or transferring data when the receiver denies. Individual, legal entities or organizations cannot send or transfer personal data and official data outside the Lao PDR without permission from the data owner or if contradicts with the law.	Article 17 Sending or Transferring of Electronic Data Sending or transferring of electronic data shall comply as following: 1. Have permission from the data owner and ensure the receiver is able to secure those data; 2. Input data security for the important data which mainly are financial, banking, investment and accounting data; 3. Do not falsify data sources that have been sent and transferred; 4. Consistent with the agreement between sender and receiver; 5. Stop sending or transferring data when the receiver denies. Individual, legal entities or organizations cannot send or transfer personal data and official data outside the Lao PDR without permission from the data owner or if contradicts with the law.
2	Law On Resistance and Prevention of Cybercrime No.		

	61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015		
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018		
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018		
6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012	Article 45 International Settlement When an international dispute involving electronic transactions occurs, it shall be resolved according to the international treaties and agreements to which Lao PDR is a party.	
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017		
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information		

	Management No. 327/GOV, dated 16 September 2014		
10	Decree on E-commerce No. 296/GOV		
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020		
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012		
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020		
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016		Article 22 Database and information of the private sector Databases and information of the private sector created to provide services in the Lao PDR must be stored in an information center via the Internet within the country, ensuring security and confidentiality.
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020		
17	Decree on Credit Information No		

	224/GOV dated July 19, 2019		
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016	Article 11 The contents of the use of information communication technology by government organizations The contents of the use of information communication technology by government organizations are as follows: 1. Exchange of information between state organizations to consolidate and improve information effectively; 2. Keeping the database safe and being able to disseminate useful information to the society in general; 3. Exchange services, provide information and collect proposals from individuals, legal entities or organizations in the network system; 4. Providing public services to develop knowledge and improve the quality of life to be: 5. Education, training within state organizations and people in remote areas; 6. Information exchange to connect with foreign countries, regional and international.	
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA dated May 17, 2017		

#	Regulation	Government Access
		National Security Law, Cybersecurity Law Provisions
		Provision allowed govt to access regulated data/to not comply to data regulation
1	The Law on Electronic Data Protection No. 25/NA, dated May 12, 2017	

2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015	
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018	Chapter 2 9. Article 16 Using or disclosing electronic information is bringing information out for use or disclosure to a third party to meet the requirements of the work which must be approved by the owner of the information unless it is proposed by the relevant government organization. For example: He also committed the crime of defrauding citizens by making false calls to other people to pay him, which caused other people to suffer. In such a case, if there is a request for phone call information from the government organization with relevant authority to request Mr. Khe's information, the data manager must provide the information as proposed without the need to notify Mr. Khe.
		Chapter 2 13. Article 20 Deletion of electronic data is the destruction of data from electronic devices or database systems, for example: if you want to delete information that you do not want to use, you must propose to the data manager to delete or delete it. Its information is out of the database system. In the event that the data has expired, the data manager has the right to delete or Destroy the information from the database system but must notify the owner of the information. In the event that your information affects national security, peace, harmony The order of society, culture and the good customs of the nation or information that defames others. The data manager must delete or destroy the information according to the proposal of the authorities or related persons.
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018	
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018	

6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012	
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017	
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017	
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014	
10	Decree on E-commerce No. 296/GOV	
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020	
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012	
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018	
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020	

15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016	
16	Decision on consumer protection for telecommunication and Internet service No. 1061/MPT, dated 25 May 2020	
17	Decree on Credit Information No 224/GOV dated July 19, 2019	
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016	
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021	
20	The Penal Code No.26/NA dated May 17, 2017	

Penalties

#	Regulation	Corporate Punishments	Individual Punishments
		Forms of penalties (e.g., recommendations for corrective action, public penalties, fines, confiscation of assets and income, data deletion, data processing, business suspension, etc.)	Penalties (penalties, fines, demotion, etc.)
		Forms of penalties on corporate	Forms of penalties on individual
1	The Law on Electronic Data Protection No.	Article 49 Measures against Violator Individual, legal entities or organizations that violate this	Article 49 Measures against Violator Individual, legal entities or organizations that violate this

	25/NA, dated May 12, 2017	law or other relevant laws will be educated, warned, disciplined, fined or penalized depending on the degree of violation.	law or other relevant laws will be educated, warned, disciplined, fined or penalized depending on the degree of violation.
		Article 50 Re-educational Measures Individual, legal entities or organizations that violate this law mainly are the prohibitions that specify in this law in minor manner will be re-educated or warned.	Article 50 Re-educational Measures Individual, legal entities or organizations that violate this law mainly are the prohibitions that specify in this law in minor manner will be re-educated or warned.
		Article 52 Fining Measures Individual, legal entities or organizations that violate this law mainly are the prohibitions that specify in Article 31, 32, and 33 which are not considered as criminal offence will be fined 15.000.000 Kip.	Article 52 Fining Measures Individual, legal entities or organizations that violate this law mainly are the prohibitions that specify in Article 31, 32, and 33 which are not considered as criminal offence will be fined 15.000.000 Kip.
		Article 53 Civil Measures Individual, legal entities or organizations violate this law that causing the damage to other persons shall pay the compensation of the damage that has been occurred.	Article 53 Civil Measures Individual, legal entities or organizations violate this law that causing the damage to other persons shall pay the compensation of the damage that has been occurred.
			Article 54 Penal Measures Individual who violates this law which is considered as criminal offence will be penalized as specified in Criminal Law and other laws that specified criminal penalties depending on the degree of violation
2	Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015 (Law on Cybercrime), Law On Resistance and Prevention of Cybercrime No. 61/NA, dated 15 July 2015	Article 57 Measures against Violators Individuals, legal entities or organizations who violate this law, especially the infringement of any prohibitions, shall be subject to re-education, warning, disciplinary measures, fine, compensating for civil loss or criminal punishment based on the seriousness of the case as specified in the laws and regulations.	Article 57 Measures against Violators Individuals, legal entities or organizations who violate this law, especially the infringement of any prohibitions, shall be subject to re-education, warning, disciplinary measures, fine, compensating for civil loss or criminal punishment based on the seriousness of the case as specified in the laws and regulations.
		Article 58 Re-educational Measures Individuals, legal entities or organizations who violate this	Article 58 Re-educational Measures Individuals, legal entities or organizations who violate this

		law which is the first violation and that causes minor damages shall be subject to re-education and warning.	law which is the first violation and that causes minor damages shall be subject to re-education and warning.
		Article 60 Fine Measures Individuals, legal entities or organizations who violate this law shall be fined according to the following cases: 1. Provide incorrect information to concerned staff and officials that cause no damages to anyone; 2. Fail to provide information within the time limit given by concerned staff of officials; 3. Delete data in computerized system or computer data of other persons without any authorization; 4. Other cases as specified in the laws and regulations related to administrative violation. Rates of fine for each case are specified in a separate regulation.	Article 60 Fine Measures Individuals, legal entities or organizations who violate this law shall be fined according to the following cases: 1. Provide incorrect information to concerned staff and officials that cause no damages to anyone; 2. Fail to provide information within the time limit given by concerned staff of officials; 3. Delete data in computerized system or computer data of other persons without any authorization; 4. Other cases as specified in the laws and regulations related to administrative violation. Rates of fine for each case are specified in a separate regulation.
			Article 61 Civil Measures Individuals, legal entities or organizations who violate this law which cause damages to other persons shall compensate for any damages incurred.
			Article 62 Penal Measures Individuals who committed a crime in the following cases shall be subject to punishments as follows: 1. Revelation of computer access protection measures shall be subject to a deprivation of liberty punishment from one month to one year and shall be imposed with a fine from 1,000,000 kips to 4,000,000 kips. 2. Unauthorized access to computerized system shall be subject to a deprivation of liberty punishment from 3 months to one year and shall be imposed with a fine from 2,000,000 kips to 5,000,000 kips; 3. Censor of content, photo,

			moving picture, sound and video without authorization shall be subject to a deprivation of liberty punishment from three months to two years and shall be imposed with a fine from 3,000,000 kips to 10,000,000 kips; 4. Stealing data in the computerized system without authorization shall be subject to a deprivation of liberty punishment from three months to three years and shall be imposed with a fine from 4,000,000 kips to 20,000,000 kips; 5. Incurring damages through online social network shall be subject to a deprivation of liberty punishment from five months to three years and shall be imposed with a fine from 4,000,000 kips to 20,000,000 kips; 6. Publication of pornography through computerized system shall be subject to a deprivation of liberty punishment from one year to five years and shall be imposed with a fine from 5,000,000 kips to 30,000,000 kips; 7. Interference of computerized system shall be subject to a deprivation of liberty punishment from one to five years and shall be imposed with a fine from 5,000,000 kips to 30,000,000 kips; 8. Falsification of computer data shall be subject to a deprivation of liberty punishment from one to five years and shall be imposed with a fine from 5,000,000 kips to 30,000,000 kips; 9. Destruction of computer data shall be subject to a deprivation of liberty punishment from three to five years and shall be imposed with a fine from 10,000,000 kips to 50,000,000

			kips; 10. Operation of business related to cybercrime apparatus shall be subject to a deprivation of liberty punishment from three years to five years and shall be imposed with a fine from 10,000,000 kips to 50,000,000 kips.
3	Guideline on the implementation of the Law on Electronic Data Protection no. 2126/MPT, dated 8 August 2018	Chapter 2 21. Article 54 Criminal measures are persons who violate the Law on the Protection of Electronic Information, which is a criminal offense, will be punished according to the Criminal Law, the Law on Combating and Suppressing Computer Crime, which is specified in Article 62 or other related laws, depending on whether the case is light or serious.	Chapter 2 21. Article 54 Criminal measures are persons who violate the Law on the Protection of Electronic Information, which is a criminal offense, will be punished according to the Criminal Law, the Law on Combating and Suppressing Computer Crime, which is specified in Article 62 or other related laws, depending on whether the case is light or serious.
4	Guideline on the Implementation of the Law On Counter and Prevention of Cybercrime no. 2543/MPT, dated 24 September 2018		
5	Law on Electronic Signature no. 59/NA, dated 12 December 2018	Article 75 Measures against violators Individuals, legal entities or organizations that have violated this law will be educated, warned, disciplined, rehabilitated, compensated or punished criminally.	Article 75 Measures against violators Individuals, legal entities or organizations that have violated this law will be educated, warned, disciplined, rehabilitated, compensated or punished criminally.
		Article 76 Measures to educate individuals, legal entities or organizations that violate this law, such as the prohibitions specified in this law, in light places will be warned and educated.	Article 76 Measures to educate individuals, legal entities or organizations that violate this law, such as the prohibitions specified in this law, in light places will be warned and educated.
		Article 77 Disciplinary measures Officials and employees who violate this law, such as the prohibitions set forth in this law, which are not criminal offenses, will be disciplined according to the law on civil servants.	Article 77 Disciplinary measures Officials and employees who violate this law, such as the prohibitions set forth in this law, which are not criminal offenses, will be disciplined according to the law on civil servants.

		Article 78 Fine measures Individuals, legal entities or organizations that violate this law will be fined by the Department of Posts, Telecommunications and Communications in the following cases: 1. Operating the business of issuing electronic signature certificates without permission; 2. Destroy, block or disrupt the operation of the certificate issuing service system such as electronics which do not cause significant damage; 3. Get a license for others to use, assign or transfer; 4. The service is incorrect as indicated in the license; 5. Provide information or publish information about invalid electronic signature authentication; 6. Disclosure of service user information; 7. Provide incorrect services according to the contract or notification; 8. Provide information or disseminate information about the endorsement of items such as electronic checks Scheduled: 9. Not recording usage data and not reporting data according to laws and regulations; 10. Claiming to be a service agent; 11. Unauthorized use of electronic signature certificates of others. The rate of renewal in each case is determined in a separate regulation.	Article 78 Fine measures Individuals, legal entities or organizations that violate this law will be fined by the Department of Posts, Telecommunications and Communications in the following cases: 1. Operating the business of issuing electronic signature certificates without permission; 2. Destroy, block or disrupt the operation of the certificate issuing service system such as electronics which do not cause significant damage; 3. Get a license for others to use, assign or transfer; 4. The service is incorrect as indicated in the license; 5. Provide information or publish information about invalid electronic signature authentication; 6. Disclosure of service user information; 7. Provide incorrect services according to the contract or notification; 8. Provide information or disseminate information about the endorsement of items such as electronic checks Scheduled: 9. Not recording usage data and not reporting data according to laws and regulations; 10. Claiming to be a service agent; 11. Unauthorized use of electronic signature certificates of others. The rate of renewal in each case is determined in a separate regulation.
		Article 79 Financial measures Individuals, legal entities or organizations that violate this law and cause damage to others must pay for the damages they have incurred.	Article 79 Financial measures Individuals, legal entities or organizations that violate this law and cause damage to others must pay for the damages they have incurred.
		Article 80 Criminal measures Individuals and legal entities who violate this law, which is a criminal offense, will be punished according to the law, regardless of whether the case is light or serious.	Article 80 Criminal measures Individuals and legal entities who violate this law, which is a criminal offense, will be punished according to the law, regardless of whether the case is light or serious.

6	Decree and Law on Electronic Transaction No. 20/NA, dated 7 December 2012	Article 56 Measures against Violators Individuals, legal entities or organizations violating this Law shall be warned, educated, face disciplinary actions, be fined, shall pay for civil damages or face criminal actions depending on the seriousness of cases in accordance with the laws and regulations.	Article 56 Measures against Violators Individuals, legal entities or organizations violating this Law shall be warned, educated, face disciplinary actions, be fined, shall pay for civil damages or face criminal actions depending on the seriousness of cases in accordance with the laws and regulations.
7	Decision on Penalties in Cyber Crime No. 3624, dated 11 December 2017	Article 2 Penalties in Cyber Crime Penalties in Cyber Crime is the imposition of administrative penalties on individuals, legal entities, or organizations in violation of article 60, under the Law on Resistance and Prevention of Cybercrime.	Article 2 Penalties in Cyber Crime Penalties in Cyber Crime is the imposition of administrative penalties on individuals, legal entities, or organizations in violation of article 60, under the Law on Resistance and Prevention of Cybercrime.
		Article 9 Fine Rate Individuals, legal entities or organizations that violate to this Decision shall be imposed with a fine as follows: 1. Provide incorrect computer data shall be imposed with a fine from 1,500,000 kips to 2,000,000 kips; 2. Fail to provide computer data within the time limit shall be imposed with a fine from 2,500,000 kips to 3,000,000 kips; 3. Delete data in computerized system or computer data of other persons without any authorization shall be imposed with a fine from 4,000,000 kips to 5,000,000 kips.	Article 9 Fine Rate Individuals, legal entities or organizations that violate to this Decision shall be imposed with a fine as follows: 1. Provide incorrect computer data shall be imposed with a fine from 1,500,000 kips to 2,000,000 kips; 2. Fail to provide computer data within the time limit shall be imposed with a fine from 2,500,000 kips to 3,000,000 kips; 3. Delete data in computerized system or computer data of other persons without any authorization shall be imposed with a fine from 4,000,000 kips to 5,000,000 kips.
8	Guidelines on Computer Systems Security No. 3623, dated 11 December 2017		
9	Decree on Internet Information Management No. 327/GOV, dated 16 September 2014	Article 26: Measures against Violators Individuals, legal entity or organizations that violate this decree may be warned, educated, penalized, fined, and	Article 26: Measures against Violators Individuals, legal entity or organizations that violate this decree may be warned, educated, penalized, fined, and

		subjected to civil or criminal charges depending on the severity of the case.	subjected to civil or criminal charges depending on the severity of the case.
10	Decree on E-commerce No. 296/GOV	Article 59 Measures against violators Individuals, legal entities or organizations that violate this decree will be punished, trained, disciplined, rehabilitated, compensated for civil damages or criminally punished according to light or heavy cases	Article 59 Measures against violators Individuals, legal entities or organizations that violate this decree will be punished, trained, disciplined, rehabilitated, compensated for civil damages or criminally punished according to light or heavy cases
11	Decree on consumer protection in financial services No. 225/GO, dated 06 April 2020	Article 35 Measures against violators Those who violate this decree or regulations related to the protection of financial service users will be warned, educated, disciplined, charged, held civilly liable or prosecuted according to law.	Article 35 Measures against violators Those who violate this decree or regulations related to the protection of financial service users will be warned, educated, disciplined, charged, held civilly liable or prosecuted according to law.
12	Decision on the Activities Regarding Credit Information No. 928/BoL, dated 20 September 2012		
13	Decision on the Access of Credit Information No. 03/BOL, dated 02 January 2018		
14	Decision on Business Operation of Electronic Signatures No. 1101/MPT, dated 29 May 2020	Article 59 Measures against violators Individuals, legal entities or organizations that violate this agreement will be educated, warned, penalized and fined, paid in lieu of civil damages or criminally punished in severe or light cases.	Article 59 Measures against violators Individuals, legal entities or organizations that violate this agreement will be educated, warned, penalized and fined, paid in lieu of civil damages or criminally punished in severe or light cases.
		Article 62 Fine measures Individuals and legal entities who violate this agreement will be fined in the following cases: 1. Operating the business of issuing electronic signature certificates without permission will be fined 40,000,000 kip; 2. Destroying, obstructing or obstructing the operation of the	Article 60 Education measures Civil servants or service providers issuing electronic signature certificates will be trained in the following cases: 1. Non-cooperation, procrastination, delay, impolite or inappropriate speech; 2. Unreasonable delay in service

		electronic signature certificate issuing service system which does not cause significant damage will be fined 5,000,000 kip; 3. Taking the license for others to use, rent or transfer will be fined 15,000,000 kip; 4. Incorrect services as specified in the license will be fined 15,000,000 kip; 5. Providing information or disseminating information about validating electronic signatures will be corrected New 10,000,000 kip; 6. Unauthorized disclosure of service user information will be fined 10,000,000 kip; 7. Providing incorrect services according to the contract or notice will be fined 15,000,000 kip; 8. Providing information or disseminating information about the electronic signature certificate, delaying the deadline will be fined 10,000,000 kip; 9. Failure to record usage data and failure to report data according to laws and regulations will be fined 10,000,000 kip; 10. Claiming to be an agent Service providers issuing certificates such as electronics will be fined 15,000,000 kip; 11. Using someone else's electronic signature certificate without permission will be fined 10,000,000 kip; 12. In the case of changing, suspending or canceling the service before the due date, a fine of 10,000,000 kip will be imposed; 13. Failure to notify or late notification of its representative to the national electronic signature certificate issuer before the deadline will be fined 5,000,000 kip;	provision or violation of other prohibitions.

		14. Late renewal of business license will be fined 5,000,000 kip.	
			Article 61 Disciplinary measures Civil servants or management officials who violate the prohibitions of this agreement will be disciplined according to relevant laws.
			Article 62 Fine measures Individuals and legal entities who violate this agreement will be fined in the following cases: 1. Operating the business of issuing electronic signature certificates without permission will be fined 40,000,000 kip; 2. Destroying, obstructing or obstructing the operation of the electronic signature certificate issuing service system which does not cause significant damage will be fined 5,000,000 kip; 3. Taking the license for others to use, rent or transfer will be fined 15,000,000 kip; 4. Incorrect services as specified in the license will be fined 15,000,000 kip; 5. Providing information or disseminating information about validating electronic signatures will be corrected New 10,000,000 kip; 6. Unauthorized disclosure of service user information will be fined 10,000,000 kip; 7. Providing incorrect services according to the contract or notice will be fined 15,000,000 kip; 8. Providing information or disseminating information about the electronic signature certificate, delaying the deadline will be fined 10,000,000 kip; 9. Failure to record usage data and failure to report data according to laws and regulations will be fined 10,000,000 kip;

			10. Claiming to be an agent Service providers issuing certificates such as electronics will be fined 15,000,000 kip; 11. Using someone else's electronic signature certificate without permission will be fined 10,000,000 kip; 12. In the case of changing, suspending or canceling the service before the due date, a fine of 10,000,000 kip will be imposed; 13. Failure to notify or late notification of its representative to the national electronic signature certificate issuer before the deadline will be fined 5,000,000 kip; 14. Late renewal of business license will be fined 5,000,000 kip.
15	Decree on Internet Information Center / Decree on data center pass though internet No 412 November 2016	Article 60 measures against violators Individuals, juristic persons or organizations that have violated this law will be educated, warned, disciplined, fined or criminally punished in light or serious cases, including compensation for damages.	Article 60 measures against violators Individuals, juristic persons or organizations that have violated this law will be educated, warned, disciplined, fined or criminally punished in light or serious cases, including compensation for damages.
		Article 61 Education measures Individuals, legal entities or organizations that violate this law, such as the prohibitions set forth in this decree, will be warned and educated. Article 62 Disciplinary measures Employees and officials who violate this decree, such as the prohibitions specified in this decree, which do not constitute a criminal offense, will be disciplined according to relevant laws.	Article 61 Education measures Individuals, legal entities or organizations that violate this law, such as the prohibitions set forth in this decree, will be warned and educated. Article 62 Disciplinary measures Employees and officials who violate this decree, such as the prohibitions specified in this decree, which do not constitute a criminal offense, will be disciplined according to relevant laws.
		Article 63 Fine measures Individuals, legal entities or organizations that violate this decree will be fined in each case as follows: 1. Conduct information center activities through the Internet	Article 63 Fine measures Individuals, legal entities or organizations that violate this decree will be fined in each case as follows: 1. Conduct information center activities through the Internet

		without permission from the sector Post, telecommunication and communication will be fined 50,000,000 kip; 2. Take the license for others to use, transfer or transfer will be fined 20,000,000 kip; 3. Improper service as indicated in the license will be fined 10,000,000 kip; 4. Improving and expanding the information center through the Internet or connecting to the network without permission will be fined 20,000,000 kip 5. Failure to provide complete and correct information about network connection to the postal, telecommunication and communication sector will be fined 10,000,000 kip; 6. Failure to record usage information and failure to report information in accordance with laws, regulations and regulations of the postal, telecommunications and communications sector will be fined 10,000,000 kip; 7. Failure to carry out activities within one year after obtaining permission will be fined 20,000,000 kip; 8. Disclosing personal information of service users without permission from the owner will be fined 20,000,000 kip; 9. Providing wrong services as promised or notified to users through various media will be fined 20,000,000 kip.	without permission from the sector Post, telecommunication and communication will be fined 50,000,000 kip; 2. Take the license for others to use, transfer or transfer will be fined 20,000,000 kip; 3. Improper service as indicated in the license will be fined 10,000,000 kip; 4. Improving and expanding the information center through the Internet or connecting to the network without permission will be fined 20,000,000 kip 5. Failure to provide complete and correct information about network connection to the postal, telecommunication and communication sector will be fined 10,000,000 kip; 6. Failure to record usage information and failure to report information in accordance with laws, regulations and regulations of the postal, telecommunications and communications sector will be fined 10,000,000 kip; 7. Failure to carry out activities within one year after obtaining permission will be fined 20,000,000 kip; 8. Disclosing personal information of service users without permission from the owner will be fined 20,000,000 kip; 9. Providing wrong services as promised or notified to users through various media will be fined 20,000,000 kip.
			Article 64 Criminal measures A person who violates this decree, which is a criminal offense, will be punished according to the criminal law according to light or serious cases.
16	Decision on consumer protection for	Article 21 measures against violators Individuals, legal entities or	Article 21 measures against violators Individuals, legal entities or

	telecommunication and Internet service No. 1061/MPT, dated 25 May 2020	organizations that have violated this agreement will be warned or educated as well as reimburse the damages they incurred.	organizations that have violated this agreement will be warned or educated as well as reimburse the damages they incurred.
17	Decree on Credit Information No 224/GOV dated July 19, 2019	Article 48 Measures against violators Individuals, legal entities and organizations that have violated this decree will be educated, warned, disciplined, rehabilitated, used in lieu of civil damages and will be criminally punished according to specific or severe cases.	Article 48 Measures against violators Individuals, legal entities and organizations that have violated this decree will be educated, warned, disciplined, rehabilitated, used in lieu of civil damages and will be criminally punished according to specific or severe cases.
18	Law on Information and Communication Technology (No. 02/NA, dated November 7, 2016	Article 64 Measures against violators Individuals, legal entities or organizations that have violated this law will be educated, warned, disciplined, fined or criminally punished in light or heavy cases, including compensation for the damages they have incurred.	Article 64 Measures against violators Individuals, legal entities or organizations that have violated this law will be educated, warned, disciplined, fined or criminally punished in light or heavy cases, including compensation for the damages they have incurred.
		Article 65 Education measures Individuals, legal entities or organizations that violate this law, such as the prohibitions specified in this law, will be warned and educated.	Article 65 Education measures Individuals, legal entities or organizations that violate this law, such as the prohibitions specified in this law, will be warned and educated.
		Article 66 Disciplinary measures Employees who violate this law, such as the prohibitions stipulated in this law, which are not criminal offenses, will be disciplined according to the relevant law.	Article 66 Disciplinary measures Employees who violate this law, such as the prohibitions stipulated in this law, which are not criminal offenses, will be disciplined according to the relevant law.
		Article 67 Fine measures Individuals, legal entities or organizations that violate this law will be fined in the following cases: 1. Conducting business related to information communication technology without obtaining a license catch 2. Take the license that he received for others to use. rent or transfer to others; 3. Unauthorized access to information and communication technology equipment; 4.	Article 67 Fine measures Individuals, legal entities or organizations that violate this law will be fined in the following cases: 1. Conducting business related to information communication technology without obtaining a license catch 2. Take the license that he received for others to use. rent or transfer to others; 3. Unauthorized access to information and communication technology equipment; 4.

		Produce, assemble, sell, supply, export or repair technical equipment Non-standard communication technology, information or related electronic equipment; 5. Access, collect, use information of individuals, legal entities or organizations without receiving it disease; 6. Provide, use the personal information provided without permission; 7. The use of information communication technology to promote propaganda that is against the law Marks and Regulations; The rate of fine in each case is determined in separate regulations.	Produce, assemble, sell, supply, export or repair technical equipment Non-standard communication technology, information or related electronic equipment; 5. Access, collect, use information of individuals, legal entities or organizations without receiving it disease; 6. Provide, use the personal information provided without permission; 7. The use of information communication technology to promote propaganda that is against the law Marks and Regulations; The rate of fine in each case is determined in separate regulations.
		Article 68 Civil measures Individuals, juristic persons or organizations that have violated this law and caused damage to others must pay for the damages they incurred	Article 68 Civil measures Individuals, juristic persons or organizations that have violated this law and caused damage to others must pay for the damages they incurred
			Article 69 Criminal measures A person who violates this law, which is a criminal offense, will be punished according to the criminal law, other laws that determine criminal punishment, and each case is light or heavy.
19	Law on Telecommunications (Revised Version) No. 05, dated November 16, 2021		
20	The Penal Code No.26/NA dated May 17, 2017		Article 164 Disclosure of Protection Measures against Illegal Access to a Computer System Any person who discloses special protection measures against illegal access to a computer system without permission and causes damage to the State, individuals, legal persons, organizations or society shall be sentenced to imprisonment for a term ranging from three months to one year

			and a fine shall be imposed ranging from 1,000,000 kip to 4,000,000 kip.
			Article 165 Illegal Access to a Computer System Any person using electronic instruments in a computer system with special protection system with the intent of illegally obtaining data pertaining to commerce, finance or individuals' privately held information, legal persons, organizations, and other data, shall be sentenced to imprisonment for a term ranging from three months to one year and a fine shall be imposed ranging from 2,000,000 kip to 5,000,000 kip.
			Article 166 Remaking Photographs, Films, Music or Videos without Authorization Any person remaking photographs, films, music or videos through new construction, complement, modification by electronic or other means for dissemination through computer systems, causing loss to natural, legal persons or concerned organizations, shall be sentenced to imprisonment for a term ranging from three months to two years and a fine shall be imposed ranging from 3,000,000 kip to 10,000,000 kip.
			Article 167 Illegal Interception of Computer Data Any person intercepting, without permission, non-public transmissions of computer data by electronic means to, from or within a computer system shall be sentenced to imprisonment for a term ranging from three months to three years and a fine shall be imposed ranging from 4,000,000 kip to 20,000,000 kip.
			Article 168 Damage through Online Media Any person causing damage

			through online media shall be sentenced to imprisonment for a term ranging from three months to three years and a fine shall be imposed ranging from 4,000,000 kip to 20,000,000 kip.
			Article 170 Interference of Computer Systems Any person using computer programs, viruses or other instruments to obstruct or destroy computer operation systems, transmitting computer data or electronic messages by hiding the address or source of data transmitter to interfere with the operating system, shall be sentenced to imprisonment for a term ranging from one year to five years and a fine shall be imposed ranging from 5,000,000 kip to 30,000,000 kip.
			Article 171 Falsifying Computer Data Any person using a computer, computer systems or electronic instruments to alter data by inputting, altering, falsifying electronic addresses or deleting data in a computer system resulting in data being modified from its original state, intentionally or by means of hacking, falsifying without authorization financial, commercial or confidential data or other data of individuals, legal persons or organizations or creating false websites to fraudulently incite internet users to input credit account information, credit card codes or internet passwords in order to cause damage to other individuals, legal persons or organizations shall be sentenced to imprisonment for a term ranging from one year to five years and a fine shall be imposed ranging from 5,000,000 kip to 30,000,000 kip.

			Article 172 Destruction of Computer Data Any person who deletes, modifies or alters computer data resulting in damage to the original computer data shall be sentenced to imprisonment for a term ranging from three years to five years and a fine shall be imposed ranging from 10,000,000 kip to 50,000,000 kip.
			Article 173 Activities related to Cyber Crime Any person creating new instruments or producing, importing, possessing, trading, distributing, advertising, disseminating or instructing electronic instruments namely software, or designing computer data in order to commit cybercrimes shall be punished by three years to five years of imprisonment and shall be fined from 10,000,000 Kip to 50,000,000 kip

E) Malaysia

Legal system overview

#	Regulation	Translation	Purpose of the Legal System
			What purpose does the legal system serve? (e.g. cybersecurity)
		Google translation or Translation by certain organization	
1	Personal Data Protection Act 2010	Original	An Act to regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto.
2	Personal Data Protection Regulations 2013	Google translation	ON exercising the powers conferred by section 143 of the Data Protection Act Personal 2010 [Act 709], the Minister made the following regulations:
3	Personal Data Protection (Registration of	Google translation	ON exercising the powers conferred by section 143 of the Data Protection Act In these Regulations, unless the context otherwise requires "data

	Data User) Regulations 2013		user" means a data user who is in the group Personal 2010 [Act 709], the Minister made the following regulations:
4	Personal Data Protection (Fees) Regulations 2013	Google translation	
5	Personal Date Protection Standard 2015	Google translation	
6	Personal Data Protection (Compounding Of Offences) Regulations 2016	Google translation	
7	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016	Translation by certain organization	
8	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner	Google translation	
9	General Code on the Practice of Personal Data Protection (2022)	Original	aims to enforce compliance to Section 23 of the Personal Data Protection Act [Act 709], regulations and standard and establish a guideline to the Class of Data Users who have not prepared a Code of Practice and there is no data user forum to develop the relevant Code of Practice for the Class of Data Users. Should you require further information, kindly consult
10	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)	Original	Data user forums were formed for specific industries, in particular the communications, banking and finance, insurance, hospitality, transport, direct sales, professional services, and utility sectors. Each data user forum was directed by the Commissioner to develop its own codes of practice for adherence by data users in the respective sectors.

11	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017	Original	same as above
12	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)	Original	same as above
13	Personal Data Protection Code of Practice for the Communications Class Data Users 2017	Original	same as above
14	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022	Original	same as above
15	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022	Original	same as above
16	Cybersecurity Bill 2024	Original	The Bill aims to provide a regulatory framework for the safeguarding of Malaysia's cyber security landscape by requiring national critical information infrastructure entities to comply with certain measures, standards and processes in the management of the cyber security threats and cyber security incidents.

#	Regulation	Form of legal system	Target Business
		Is it introduced in accordance with government ordinances and guidelines? (Is it introduced in a format that ensures lead time?)	Does the law target specific industry or in general? Is it clearly stated in the regulations?
		Regulation level	Industry

1	Personal Data Protection Act 2010	Law	General
2	Personal Data Protection Regulations 2013	Subordinate Laws and Guidelines	General
3	Personal Data Protection (Registration of Data User) Regulations 2013	Subordinate Laws and Guidelines	General
4	Personal Data Protection (Fees) Regulations 2013	Subordinate Laws and Guidelines	General
5	Personal Date Protection Standard 2015	Subordinate Laws and Guidelines	Cybersecurity
6	Personal Data Protection (Compounding Of Offences) Regulations 2016	Subordinate Laws and Guidelines	General
7	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016	Subordinate Laws and Guidelines	General
8	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner	Subordinate Laws and Guidelines	General
9	General Code on the Practice of Personal Data Protection (2022)	Subordinate Laws and Guidelines	General
10	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)	Subordinate Laws and Guidelines	Banking and Financial Sector
11	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017	Subordinate Laws and Guidelines	Utilities Sector (Electricity)

12	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)	Subordinate Laws and Guidelines	Insurance and Takaful Insurance Industries
13	Personal Data Protection Code of Practice for the Communications Class Data Users 2017	Subordinate Laws and Guidelines	Communications
14	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022	Subordinate Laws and Guidelines	Healthcare Industry
15	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022	Subordinate Laws and Guidelines	Utilities Sector (Water)
16	Cybersecurity Bill 2024	Law	General

#	Regulation	Regulatory authority	Jurisdiction
		Which regulatory authority has jurisdiction over regulation?	Cyber security, data security, personal information protection, etc.
		Name of ministry/organization	Similar to purpose?
1	Personal Data Protection Act 2010	Personal Data Protection Commissioner	personal information protection
2	Personal Data Protection Regulations 2013	Personal Data Protection Commissioner	personal information protection
3	Personal Data Protection (Registration of Data User) Regulations 2013	Personal Data Protection Commissioner	personal information protection
4	Personal Data Protection (Fees) Regulations 2013	Personal Data Protection Commissioner	personal information protection

5	Personal Date Protection Standard 2015	Personal Data Protection Commissioner	personal information protection
6	Personal Data Protection (Compounding Of Offences) Regulations 2016	Personal Data Protection Commissioner	personal information protection
7	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016	Personal Data Protection Commissioner	personal information protection
8	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner	Personal Data Protection Commissioner	personal information protection
9	General Code on the Practice of Personal Data Protection (2022)	Personal Data Protection Commissioner	personal information protection
10	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)	Personal Data Protection Commissioner	personal information protection
11	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017	Personal Data Protection Commissioner	personal information protection
12	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)	Personal Data Protection Commissioner	personal information protection
13	Personal Data Protection Code of Practice for the Communications Class Data Users 2017	Personal Data Protection Commissioner	personal information protection
14	Personal Data Protection Code	Personal Data Protection Commissioner	personal information protection

	of Practice for Private Hospitals in the Healthcare Industry 2022		
15	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022	Personal Data Protection Commissioner	personal information protection
16	Cybersecurity Bill 2024	National Cyber Security Agency ('NACSA'); Cyber Security Malaysia ('CSM'); the MCMC; the Department of Personal Data Protection ('PDP'); and the Special Cyber Court ('the Cyber Court').	Cyber security

#	Regulation	Status	Citation
		Legislation / Public Comment / Passage / Enforcement / Amendment, etc.	
		Status of the regulation: Draft = drafting (new regulation) published = published in the gazzette but not yet enacted Enact = published in the gazzette and already enacted Amendment = enacted regulation being on amending process	URL
1	Personal Data Protection Act 2010	Enact	https://www.pdp.gov.my/jpdpv2/laws-of-malaysia-pdpa/personal-data-protection-act-2010/?lang=en
2	Personal Data Protection Regulations 2013	Enact	—
3	Personal Data Protection (Registration of Data User) Regulations 2013	Enact	https://www.pdp.gov.my/ppdpv1/
4	Personal Data Protection (Fees) Regulations 2013	Enact	
5	Personal Date Protection Standard 2015	Enact	

6	Personal Data Protection (Compounding Of Offences) Regulations 2016	Enact	
7	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016	Enact	
8	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner	Enact	
9	General Code on the Practice of Personal Data Protection (2022)	Enact	https://www.dataguidance.com/sites/default/files/28.12.2022-final-printing-cop-bi.pdf
10	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)	Enact	https://www.pdp.gov.my/ppdpv1/
11	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017	Enact	https://www.pdp.gov.my/ppdpv1/
12	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)	Enact	https://www.pdp.gov.my/ppdpv1/
13	Personal Data Protection Code of Practice for the Communications Class Data Users 2017	Enact	https://www.pdp.gov.my/ppdpv1/
14	Personal Data Protection Code of Practice for Private Hospitals	Enact	https://www.pdp.gov.my/ppdpv1/

	in the Healthcare Industry 2022		
15	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022	Enact	https://www.pdp.gov.my/ppdpv1/
16	Cybersecurity Bill 2024	Enact	https://www.article19.org/wp-content/uploads/2024/04/2024.04.04-Malaysia-Cybercrime-Analysis-2024.pdf

Definitions for basic items

#	Regulation	Type and Scope of Data	Data processing and handling
		Personal data, personal information/sensitive and important data/children and minors' data, etc. Is the scope of data clearly written in the regulations? What are the unclear points?	Processing, handling / disclosure, sharing, provision, transmission, outsourcing / use for advertising, etc.
		Specific type of data required to complied with the regulation	Provision for data processing
1	Personal Data Protection Act 2010	Section 4. Interpretation "personal data" means any information in respect of commercial transactions, which- (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is	Section 4. Interpretation "processing", in relation to personal data, means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including- (a) the organization, adaptation or alteration of personal data; (b) the retrieval, consultation or use of personal data; (c) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or (d) the alignment, combination, correction, erasure or destruction of personal data; "disclose", in relation to personal data, means an act by which such personal data is made available by a data user;

		processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010; "sensitive personal data" means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the Gazette. "relevant person", in relation to a data subject, howsoever described, means- (a) in the case of a data subject who is below the age of eighteen years, the parent, guardian or person who has parental responsibility for the data subject; (b) in the case of a data subject who is incapable of managing his own affairs, a person who is appointed by a court to manage those affairs, or a person authorized in writing by the data subject to act on behalf of the data subject; or (c) in any other case, a person authorized in writing by the data subject to make a data access request, data correction request, or both such requests, on behalf of the data subject;	
2	Personal Data Protection Regulations 2013		
3	Personal Data Protection (Registration of Data User) Regulations 2013		

4	Personal Data Protection (Fees) Regulations 2013		
5	Personal Date Protection Standard 2015		
6	Personal Data Protection (Compounding Of Offences) Regulations 2016		
7	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
8	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
9	General Code on the Practice of Personal Data Protection (2022)	3.1 Scope of the Code Upon registration of this Code by the Commissioner, the Code shall apply to all Data Users. This shall include all: (i) (ii) (iii) (iv) Network Facilities Providers; Network Services Providers; Applications Service Providers; and Content Applications Service Providers, Personal data means any information in respect of commercial transactions, which – (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly	PART2 1.0 Definitions Disclose in relation to personal data, means an act by which such personal data is made available by a Data User; Processing / process in relation to personal data, means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including – (a) the organization, adaptation or alteration of personal data; (b) the retrieval, consultation or use of personal data; (c) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or (d) the alignment, combination, correction, erasure or destruction of personal data;

		to a Data Subject, who is identified or identifiable from that information or from that and other information in the possession of a Data User, including any sensitive personal data and expression of opinion about the Data Subject, but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010; sensitive personal data means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other belief or a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the Gazette	
10	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
11	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
12	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)	Non-Sensitive Personal Data: (a) (b) (c) (d) (e) (f) (g) (h) (i) (j) (k) (l) (m) name and age; home/mailing address; NRIC/passport number; contact information, telephone number, email address; biodata/personal profile; photograph or video image of an individual; employment information;	

		financial information; investment and risk preferences in respect of investment type products; vehicle registration numbers; personal data of family members/next-of-kin; personal data of the beneficiaries or nominees relevant to the processing of insurance/takaful claims, the provision of the insurance/takaful and related products and services; and/or such other personal data required with Data Subject's consent. Sensitive Personal Data: (a) (b) (c) (d) (e) (f) thumbprint or DNA profile; physical and/or mental health condition; religious belief; commission or alleged commission of any offence or contravention of any laws at any point of time; expression of opinion; and/or such other sensitive personal data required with Data Subject's consent.	
13	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
14	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
15	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		

16	Cybersecurity Bill 2024		

#	Regulation	Data handlers
		Classification/ distinction by responsibility (data processor, data controller)/ size of data, (national security) critical services, etc.
		Provision on type of data handler
1	Personal Data Protection Act 2010	Section 4. Interpretation "data processor, in relation to personal data, means any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes; "data user" means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor;
2	Personal Data Protection Regulations 2013	2. Interpretauion "data user" means a data user who is in the group Personal 2010 [Act 709], the Minister made the following regulations: othersdata user specified in an order made under subsection 14(1)
3	Personal Data Protection (Registration of Data User) Regulations 2013	
4	Personal Data Protection (Fees) Regulations 2013	
5	Personal Date Protection Standard 2015	
6	Personal Data Protection (Compounding Of Offences) Regulations 2016	
7	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016	
8	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner	

9	General Code on the Practice of Personal Data Protection (2022)	Data processor means any person, other than an employee of the Data User, who processes the personal data solely on behalf of the Data User, and does not process the personal data for any of his own purposes; Data Subject means an individual who is the subject of personal data and for the purposes of this Code includes (without limitation) the individuals identified in 3.2 of Part 1; Data User means a licensee, whether class or individual, under the Communications and Multimedia Act 1998 who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data (but does not include a data processor), and for the purpose of this Code shall also refer to the persons that are subject to the Code;
10	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)	
11	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017	
12	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)	"Data Processor" refers to any person, other than an employee of the Data User, who processes the personal data solely on behalf of the Data User, and does not process the personal data for any of its own purposes. "Data User" refers to a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a Data Processor. "Insurer/Operator" refers to an insurance company/takaful operator licensed under the FSA/IFSA, and duly registered as a Data User with the Personal Data Protection Commissioner ("Commissioner") under the Act, and collectively to be referred to as "Insurers/Operators". Unless expressly stated otherwise, Insurers/Operators shall include Insurance/Takaful Intermediaries (as defined below). "Data Subject" refers to an individual to whom the personal data relates to, including but not limited to a proposer, a policyholder/certificate holder, an insured person/covered person, a beneficiary, a nominee, a trustee, a claimant, their authorized representative and any other individual whose personal

		data is being assessed, processed or negotiated pursuant to the insurance/takaful business, and collectively to be referred to as "Data Subjects".
13	Personal Data Protection Code of Practice for the Communications Class Data Users 2017	
14	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022	
15	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022	
16	Cybersecurity Bill 2024	

legal basis

#	Regulation		
		consent	necessary for the performance of a contract
1	Personal Data Protection Act 2010	Section6. general principle (a)in the case of personal data other than sensitive personal data, process personal data about a data subject unless the data subject has given his consent to the processing of the personal data; or (b)in the case of sensitive personal data, process sensitive personal data about a data subject except in accordance with the provisions of section 40.	(a)for the performance of a contact to which the data subject is a party; (b)for the taking of steps at the request of the data subject with a view to entering into a contract;
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		

3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)	(ii) the fulfilment of a pre-contractual request of the Data Subject; or Example 1: Where a Data Subject requests that the Data User mail/e-mail one or more financial services product brochures to the Data Subject. Example 2: Where the Data Subject makes an application for a facility with the Data User, and the Data User conducts the necessary precontractual credit, anti-money laundering and risk management checks. Example 3: Where an automobile	3.1 GENERAL PRINCIPLE 3.1.1 Data Users are permitted to "process" (e.g. to collect, use, modify, store and/or dispose of) personal data, either with or without consent, as detailed in 3.1.2 and 3.1.3 below. 3.1.2 Data Users are permitted to process personal data without obtaining the consent of Data Subjects where the processing is necessary for the following purposes: (i) the performance of a contract with a Data Subject; or

		dealer, acting as the agent for the Data Subject, submits a Data Subject's personal data to a Data User in order to obtain the Data User's best rate and terms. Example 4: Where a real estate agent or developer, acting as the agent for the Data Subject, submits a Data Subject's personal data to a Data User, requesting the Data User to contact the Data Subject on available financing packages.	Example: Where a Data Subject enters into an agreement with a Data User in order to secure a loan/financing or a credit card, open a savings or current account, open a fixed deposit facility and/or to transmit monies using a money transfer service.
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)	all Insurers/Operators must comply with all seven Personal Data Protection Principles below: (a) (b) (c) (d) (e) (f) (g) General Principle; Notice and Choice Principle; Disclosure Principle; Security Principle; Retention Principle; Data Integrity Principle; and Access Principle, 7. General Principle 7.1. Insurers/Operators collect personal data through various modes of communication including proposal forms, claim forms and other documentation completed or provided by the Data Subjects, as well as verbally e.g. via face-to-face, phone calls or electronically, e.g. by point of sale systems or over the Internet. 7.2. The collection and processing of personal data by Insurers/Operators usually happens at various main stages, such as: (a) (b) (c) pre-contractual stage, including advising, marketing, application or proposal stage; contractual stage, during the term of the	

		insurance policy/takaful certificate; and claim stage. 7.3. As a general rule, Insurers/Operators will be allowed to process the Data Subjects' personal data in accordance with the provisions of the Act and, if required, where consent has been obtained from the relevant Data Subjects.	
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

#	Regulation		
		necessary for compliance with a legal obligation	necessary in order to protect the vital interests
1	Personal Data Protection Act 2010	(c)for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract; (a)the personal data is processed for a lawful purpose directly related to an activity of the data user;	(d)in order to protect the vital interests of the data subject;
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		

3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner	Currently, the PDPA requires the following classes of data users to register under the PDPA: Communications A licensee under the Communications and Multimedia Act 1998 A licensee under the Postal Services Act 2012 Banking and financial institutions A licensed bank and licensed investment bank under the Financial Services Act 2013 A licensed Islamic bank and licensed international Islamic bank under the Islamic Financial Services Act 2013 A development financial institution under the Development Financial Institution Act 2002 Insurance A licensed insurer under the Financial Services Act 2013 A licensed takaful operator	

		under the Islamic Financial Services Act 2013 A licensed international takaful operator under the Islamic Financial Services Act 2013 Health A licensee under the Private Healthcare Facilities and Services Act 1998 A holder of the certificate of registration of a private medical clinic or a private dental clinic under the Private Healthcare Facilities and Services Act 1998 A body corporate registered under the Registration of Pharmacists Act 1951 Tourism and hospitalities A licensed person who carries on or operates a tourism training institution, licensed tour operator, licensed travel agent or licensed tourist guide under the Tourism Industry Act 1992 A person who carries on or operates a registered tourist accommodation premises under the Tourism Industry Act 1992 Transportation Certain named transportations services providers Education A private higher educational institution registered under the Private Higher Educational Institutions Act 1996 A private school or private educational institution registered under the Education Act 1996 Direct selling A licensee under the Direct Sales and Anti-Pyramid Scheme Act 1993 Services A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961 carrying on business as follows: legal audit accountancy	

		engineering architecture A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961, who conducts retail dealing and wholesale dealing as defined under the Control Supplies Act 1961 A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961, who carries on the business of a private employment agency under the Private Employment Agencies Act 1981 Real estate A licensed housing developer under the Housing Development (Control and Licensing) Act 1966 A licensed housing developer under the Housing Development (Control and Licensing) Enactment 1978, Sabah A licensed housing developer under the Housing Developers (Control and Licensing) Ordinance 1993, Sarawak Utilities Certain named utilities services providers Pawnbroker A licensee under the Pawnbrokers Act 1972 Moneylender A licensee under the Moneylenders Act 1951	
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)	(iii) in order to comply with any non-contractual legal obligation that the Data User is subject to; or Example 1: Where the Data User is required to provide personal data of Data Subjects to Bank Negara Malaysia, Inland Revenue Board or other law enforcement	

		authorities in order to comply with the regulatory reporting requirements of the Anti-Money Laundering and Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001. Example 2: Where the Data User is required to provide the personal data of Data Subjects to Bank Negara Malaysia in fulfilment of its obligations under the Financial Services Act 2013 or for the purpose of complying with the regulations or guidelines of Bank Negara Malaysia.	
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)		
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

#	Regulation		
		necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	necessary for the purposes of the legitimate interests pursued by the controller or by a third party
1	Personal Data Protection Act 2010	(e)for the administration of justice; or (f)for the exercise of any functions conferred on any person by or under any law.	(b)the processing of the personal data is necessary for or directly related to that purpose; and (c)the personal data is adequate but not excessive in relation to that purpose.
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of		

	Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)		
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

#	Regulation		
		opt-out	others
1	Personal Data Protection Act 2010		
2	Personal Data Protection (Class		

	Of Data Users) (Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		

13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)		
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

Rights of the data subject

#	Regulation	Right to be informed	Right of access
1	Personal Data Protection Act 2010		Section 12. access principle A data subject shall be given access to his personal data held by a data user and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is

			refused under this act. Section 30. right to access to personal data (1)an individual is entitled to be informed by a data user whether personal data of which that individual is the data subject is being processed by or on behalf of the data user. (2)a requestor may, upon payment of a prescribed fee, make a data access request in writing to the data user- (a)for information of the data subject's personal data that is being processed by or on behalf of the data user; and (b)to have communicated to him a copy of the personal data in an intelligible form. (3)a data access request for any information under subsection(2) shall be treated as a single request, and a data access request for information under paragraph(2)(a) shall, in the absence of any indication to the contrary, be treated as extending also to such request under paragraph(2)(b). (4)in the case of a data user ...(continue)
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		

6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		1. As a data subject under the Personal Data Protection Act 2010 (the "PDPA"), you are entitled to have your personal data processed1 by the Bank strictly in compliance with the Personal Data Protection principles2. The principles (each of which will be explained briefly below) are: (i) (ii) (iii) (iv) (v) (vi) (vii) General Principle; Notice and Choice Principle; Disclosure Principle; Security Principle; Retention Principle; Data Integrity Principle; and Access Principle. 5.1 RIGHT OF ACCESS TO PERSONAL DATA 5.1.1 Under the Access Principle, a Data Subject has the right to lodge a data access request ("DAR") with the Data User and to receive a reply from the Data User within the time period set in the Act. 5.1.2 A DAR may also be made on behalf of the Data Subject by the following persons:

			(i) (ii) (iii) in the case of a Data Subject who is below the age of eighteen years, the parent, guardian or person who has parental responsibility for the Data Subject; or in the case of a Data Subject who is incapable of managing his own affairs, a person who is appointed by a court to manage those affairs, or a person authorized in writing by the Data Subject to act on behalf of the Data Subject; or in any other case, a person authorized in writing by the Data Subject to make a data access request, data correction request, or both such requests, on behalf of the Data Subject, (collectively referred to as the "Relevant Persons" and for the purpose of this Part 5, the Data Subject or the Relevant Person making the DAR or DCR (defined in 5.2.1 below) shall be referred to as the "Requestor"). Ambit Of A DAR 5.1.3 A DAR may be made in respect of personal data that is currently within the various electronic and physical systems of the Data User as provided by the Data Subject to the Data User. 5.1.4 Data Users are required to ensure that a copy of the personal data is provided to the Requestor in an intelligible form. "Intelligible form" has not been defined in the Act, and as such should be interpreted to mean that the information provided by the Data User should be capable of being understood by a Requestor. For example, where a Data User holds personal data in specific abbreviations, codes or other undefined terms, the same must be explained to the Requestor in a manner a layperson is able to understand. 5.1.5 For the avoidance of doubt,

			personal data being retained for backup and electronic archival purposes are not subject to the Access Principle.
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)		6. Data Subject's Rights Subject to the exemptions and exceptions stated in any laws, rules, regulations, this Code and the Act, a Data Subject has the following rights, namely: 6.1. Right of access to personal data - a Data Subject is entitled to be informed by an Insurer/Operator whether his personal data is being processed by or on behalf of the Insurer/Operator.
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

#	Regulation	Right to rectification	Right to erasure
1	Personal Data Protection Act 2010	Section 12. access principle A data subject shall be given access to his personal data held by a data user and be able to	

		correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is refused under this act. Section 34. right to correct personal data (1)where- (a)a copy of the personal data has been supplied by the data user in compliance with the data access request under section 30 and the requestor consider that the personal data is inaccurate, incomplete, misleading or not up-to-date; or (b)the data subject knows that his personal data being held by the data user is inaccurate, incomplete, misleading or not up-to-date. ...(continue)	
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		

8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)	6.2. Right to correct personal data - a Data Subject is entitled to correct his personal data if it is inaccurate, incomplete, misleading or not up-to-date.	
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities		

	Sector (Water) 2022		
17	Cybersecurity Bill 2024		

#	Regulation	Right to restrict processing	Right to data portability
1	Personal Data Protection Act 2010	section 42. right to prevent processing likely to cause damage or distress (1)subject to subsection(2), a data subject may, at any time by notice in writing to a data user, referred to as the "data subject notice", require the data user at the end of such period as is reasonable in the circumstances, to- (a)cease the processing of or processing for a specified purpose or in a specified manner; or (b)not begin the processing of or processing for a specified purpose or in a specified manner, Any personal data in respect of which he is the data subject if, based on reasons to be stated by him- ...(continue) Section 43. right to prevent processing for purpose of direct marketing (1)a data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his personal data for purposes of direct marketing. (2)where the data subject is dissatisfied with the failure of the data user to comply with the notice, whether in whole or in part, under subsection (1), the data subject may submit an application to the commissioner to require the data user to	

		comply with the notice. ...(continue)	
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code of Practice for		

	the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)	6.4. Right to prevent processing likely to cause damage or distress - a Data Subject is entitled to request the Insurer/Operator to cease or not begin the processing of his personal data based on the reasons that the processing of that personal data is causing or likely to cause substantial damage or substantial distress to him or to another; and the damage or distress is or would be unwarranted. 6.5. Right to prevent processing for purposes of direct marketing - a Data Subject is entitled to request the Insurer/Operator to cease or not begin processing his personal data for purposes of direct marketing.	
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

#	Regulation		
		Right to object	Right not to be subject to a decision based solely on automated processing

1	Personal Data Protection Act 2010		
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code		

	of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)		
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

#	Regulation	Right to withdraw consent	others
1	Personal Data Protection Act 2010	Section 38. withdrawal of consent to process personal data (1) a data subject may by notice in writing withdraw his consent to the processing of personal data in respect of which he is the data subject. (2) the data user shall, upon receiving the notice under subsection (1), cease the processing of the personal data. ...(continue)	
2	Personal Data Protection (Class Of Data Users)		

	(Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data	6.3. Right to withdraw consent - a Data Subject is entitled to	

	Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)	withdraw his consent to the processing of personal data.	
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

Extraterritorial application

#	Regulation		
		applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction	applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction
1	Personal Data Protection Act 2010	Section 2. application (1)this act applies to- (a)any person who processes; and (b)any person who has control over or authorizes the processing of, any personal data in respect of commercial transactions. (2)subject to subsection (1), this act applies to a person in respect of personal data if- (a)the person is established in Malaysia and the personal data is processed, whether or not in	

		the context of that establishment, by that person or any other person employed or engaged by that establishment; or (b)the person is not established in Malaysia, but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia. (3)a person falling within paragraph (2)(b) shall nominate for the purposes of this act a representative established in Malaysia. (4)for the purposes of subsections (2) and (3), each of the following is to be treated as established in Malaysia; (a)an individual whose physical presence in Malaysia shall not be less than one hundred and eighty days in one calendar year (b)a body incorporated under the companies act 1965(act 125); (c)a partnership or other unincorporated association formed under any written laws in Malaysia; and (d)any person who does not fall within paragraph (a), (b) or (c) but maintains in Malaysia- (i)an office, branch or agency through which he carries on any activity; or (ii)a regular practice. Section 3. Non-application (1) this act shall not apply to the federal government and state governments (2) this act shall not apply to any personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia.	
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		

3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and	8.6. For Insurers/Operators, in addition to Paragraph 8.5 above, the purposes of processing of personal data shall also include	

	Takaful Insurance Industries in Malaysia (2017)	the following: (f)compliance with the requirements of any law, any regulations or guidelines, any present or future contractual or other commitment with any legal, regulatory, judicial, administrative, public or law enforcement body, whether in or outside Malaysia, that are issued by regulatory or other authorities with which the Insurer/Operator or any other group members of the Insurer/Operator need or are expected to comply, including but not limited to making any enquiries, any investigation, disclosure or reporting requirements and/or meeting obligations pursuant to such law, regulations guidelines and/or the relevant authorities; 9.4. Where such organizations or third parties as set out in Paragraph 9.2 above are not located in Malaysia, the relevant Insurer/Operator may transfer the relevant personal data to places outside of Malaysia in accordance with Section 129 of the Act.	
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

#	Regulation	no express territorial scope, but would require some nexus to the jurisdiction	other
1	Personal Data Protection Act 2010		Section 2. application (1)this act applies to- (a)any person who processes; and (b)any person who has control over or authorizes the processing of, any personal data in respect of commercial transactions. (2)subject to subsection (1), this act applies to a person in respect of personal data if- (a)the person is established in Malaysia and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or (b)the person is not established in Malaysia, but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia. (3)a person falling within paragraph (2)(b) shall nominate for the purposes of this act a representative established in Malaysia. (4)for the purposes of subsections (2) and (3), each of the following is to be treated as established in Malaysia; (a)an individual whose physical presence in Malaysia shall not be less than one hundred and eighty days in one calendar year (b)a body incorporated under the companies act 1965(act 125); (c)a partnership or other unincorporated association formed under any written laws in Malaysia; and (d)any person who does not fall

			within paragraph (a), (b) or (c) but maintains in Malaysia- (i)an office, branch or agency through which he carries on any activity; or (ii)a regular practice. Section 3. Non-application (1) this act shall not apply to the federal government and state governments (2) this act shall not apply to any personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia.
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data		

	Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)		
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
17	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
18	Cybersecurity Bill 2024		

#	Regulation	
		Representatives of controllers or processors not established in the country

1	Personal Data Protection Act 2010	Section 2. application (1)this act applies to- (a)any person who processes; and (b)any person who has control over or authorizes the processing of, any personal data in respect of commercial transactions. (2)subject to subsection (1), this act applies to a person in respect of personal data if- (a)the person is established in Malaysia and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or (b)the person is not established in Malaysia, but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia. (3)a person falling within paragraph (2)(b) shall nominate for the purposes of this act a representative established in Malaysia. (4)for the purposes of subsections (2) and (3), each of the following is to be treated as established in Malaysia; (a)an individual whose physical presence in Malaysia shall not be less than one hundred and eighty days in one calendar year (b)a body incorporated under the companies act 1965(act 125); (c)a partnership or other unincorporated association formed under any written laws in Malaysia; and (d)any person who does not fall within paragraph (a), (b) or (c) but maintains in Malaysia- (i)an office, branch or agency through which he carries on any activity; or (ii)a regular practice. Section 3. Non-application (1) this act shall not apply to the federal government and state governments (2) this act shall not apply to any personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia.
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016	
3	Personal Data Protection Regulations 2013	
4	Personal Data Protection (Registration of Data User) Regulations 2013	
5	Personal Data Protection	

	(Fees) Regulations 2013	
6	Personal Date Protection Standard 2015	
7	Personal Data Protection (Compounding Of Offences) Regulations 2016	
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016	
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner	
10	General Code on the Practice of Personal Data Protection (2022)	
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)	
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017	
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)	
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017	

15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022	
17	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022	
18	Cybersecurity Bill 2024	

Notification obligation

#	Regulation	Data breach notification to authorities	Data breach notification to affected individuals
1	Personal Data Protection Act 2010		
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		

8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)		
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities		

	Sector (Water) 2022		
17	Cybersecurity Bill 2024		

Obligations of Data Fiduciaries

#	Regulation	external	external
		Notification of data processing	registration of database
1	Personal Data Protection Act 2010	Section 7. Notice and choice principle (1) a data user shall by written notice inform a data subject- (a) that personal data of the data subject is being processed by or on behalf of the data user, and shall provide a description of the personal data to that data subject; (b) the purposes for which the personal data is being or is to be collected and further processed; (c) of any information available to the data user as to the source of that personal data; (d) of the data subject's right to request access to and to request correction of the personal data and how to contact the data user with any inquiries or complains in respect of the personal data; (e) of the class of third parties to whom the data user discloses or may disclose the personal data; (f) of the choices and means the data user offers the data subject for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data; (g) whether it is obligatory or voluntary for the data subject to supply the personal data; and (h) where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he fails to supply the personal data. ..(continue)	Section 14. registration of data users (1)the minister may, upon the recommendation of the commissioner, by order published in the gazette, specify a class of data users who shall be required to be registered as data users under this act. (2)the commissioner shall, before making his recommendation under subsection (1), consult with- (a)such bodies representative of data users belonging to that class; or (b)such other interested persons. ...(continue)

2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code of Practice for the Utilities		

	Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)		
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

#	Regulation	external	external
		Data protection impact assessment	Others
1	Personal Data Protection Act 2010		
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		

5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)		
14	Personal Data Protection Code of Practice for the Communications		

	Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

#	Regulation	internal	internal
		technical and organisational measures	Purpose Limitation
1	Personal Data Protection Act 2010	Section 8. disclosure principle Subject to section 39, no personal data shall, without the consent of the data subject, be disclosed- (a)for any purpose other than- (i)the purpose for which the personal data was to be disclosed at the time of collection of the personal data; or (ii)a purpose directly related to the purpose referred to in subparagraph(i); or (b)to any party other than a third party of the class of third parties as specified in paragraph 7(1)(e). Section 9. security principle (1) a data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard- (a)to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure,	

		alternation or destrunction; (b)to the place or location where the personal data is stored; (c)to any security measures incorporated into any equipment in which the personal data is stored; (d)to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and (e)to the measures taken for ensuring the secure transfer of the personal data. (2)where processing of personal data is carried out by a data processor on behalf of the data user, the data user shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction, ensure that the data processor- (a)provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and (b)takes reasonable steps to ensure compliance with those measures.	
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		

6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)	10. Security Principle 10.1. As the contents in Paragraph 10.2 below are meant to be used as a guide for Insurers/Operators, each Insurer/Operator shall be at liberty to determine its own security measures, so long as the Insurer/Operator develops and implements a security policy that complies with the Security Principle requirements under the Act and with any regulations and guidelines as issued by BNM and the PDP Commission from time to time in relation to the security standards.	

		10.2. To comply with the Security Principle, Insurers/Operators will need to ensure that they take practicable security measures to prevent unauthorised access to, or alteration, disclosure or destruction of the personal data and prevent their accidental loss, destruction, access or other similar risks. In particular, Insurers/Operators will need to establish internal policies, processes and procedures by taking into consideration and being guided by the following standards and best practices. All of the following are not meant to be prescriptive or exhaustive, and shall be referred to by the Insurers/Operators as a guiding principle in determining the level and type of security that is necessary to protect personal data:	
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

#	Regulation	internal	internal
		Accuracy	Retention Limitation
1	Personal Data Protection Act 2010	Section 11. data integrity principle A data user shall take reasonable steps to ensure that	Section 10. retention principle (1)the personal data processed for any purpose shall not be kept longer than is necessary for the

		the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed. section 12. access principle a data subject shall be given access to his personal data held by a data user and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is refused under this act.	fulfilment of that purpose. (2)it shall be the duty of a data user to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of		

	Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)		
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

#	Regulation	internal	internal
		drawing up of codes of conduct	record of processing activities

1	Personal Data Protection Act 2010	section 23. code of practice (1) a data user forum may prepare a code of practice- (a) on its own initiative; or (b) upon request by the commissioner. (2) the data user forum shall, in preparing a code of practice under subsection (1), consider matters including- (a) the purpose for the processing of personal data by the data user or class of data users; (b) the views of the data subjects or groups representing data subjects; (c) the views of the relevant regulatory authority, if any, to which the data user is subject to; and (d) that the code of practice, upon having regard to all of the matters in paragraphs (a), (b) and (c) and any other matters, offers an adequate level of protection for the personal data of the data subjects concerned. (3)the commissioner may register the code of practice prepared pursuant to subsection (1), if the commissioner is satisfied that- (a) the code of practice is consistent with the provisions of this act; and (b) the matters as set out in subsection (2)have been given due consideration. ...(continue)	section 44. record to be kept by data user (1) a data user shall keep and maintain a record of any application, notice, request or any other information relating to personal data that has been or is being processed by him. (2) the commissioner may determine the manner and form in which the record is to be maintained.
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of		

	Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)	10. Security Principle 10.1. As the contents in Paragraph 10.2 below are meant to be used as a guide for Insurers/Operators, each Insurer/Operator shall be at liberty to determine its own security measures, so long as the Insurer/Operator develops and implements a security policy	

		that complies with the Security Principle requirements under the Act and with any regulations and guidelines as issued by BNM and the PDP Commission from time to time in relation to the security standards. 10.2. To comply with the Security Principle, Insurers/Operators will need to ensure that they take practicable security measures to prevent unauthorised access to, or alteration, disclosure or destruction of the personal data and prevent their accidental loss, destruction, access or other similar risks. In particular, Insurers/Operators will need to establish internal policies, processes and procedures by taking into consideration and being guided by the following standards and best practices. All of the following are not meant to be prescriptive or exhaustive, and shall be referred to by the Insurers/Operators as a guiding principle in determining the level and type of security that is necessary to protect personal data:	
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

#	Regulation	internal	internal
		Designation of the data protection officer	Others
1	Personal Data Protection Act 2010		
2	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
3	Personal Data Protection Regulations 2013		
4	Personal Data Protection (Registration of Data User) Regulations 2013		
5	Personal Data Protection (Fees) Regulations 2013		
6	Personal Date Protection Standard 2015		
7	Personal Data Protection (Compounding Of Offences) Regulations 2016		
8	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
9	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
10	General Code on the Practice of Personal Data Protection (2022)		
11	Personal Data Protection Code		

	of Practice for the Banking and Financial Sector (2017)		
12	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
13	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)		
14	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
15	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
16	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
17	Cybersecurity Bill 2024		

Data Cross Boarder Dist

#	Regulation	Cross-border data transfer & Exceptions	Data localization
		Provisions for Transborder Data Transfer. What are the exceptions? (e.g., sufficient authorization, transfers based on contracts equivalent to Standard Contract Clauses (SCC) or Binding Corporate Rules (BCR), transfers	Presence or absence of provisions, stipulations regarding the types of data that must be stored in the country

		based on corporate certification, etc.), Transborder transfer assessment (TIA)	
		Provisions for cross boarder data transfer	Provisions on requirement of localization; and Type of data required for localization
1	Personal Data Protection Act 2010	Section 129. Transfer of personal data to places outside Malaysia (1) A data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister, upon the recommendation of the Commissioner, by notification published in the Gazette. (2) For the purposes of subsection (1), the Minister may specify any place outside Malaysia if- (a) there is in that place in force any law which is substantially similar to this Act, or that serves the same purposes as this Act; or (b) that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by this Act. (3) Notwithstanding subsection (1), a data user may transfer any personal data to a place outside Malaysia if- (a) the data subject has given his consent to the transfer; (b) the transfer is necessary for the performance of a contract between the data subject and the data user; (c) the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which- (i) is entered into at the request of the data subject; or (ii) is in the interests of the data subject; (d) the transfer is for the purpose	

		of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights; (e) the data user has reasonable grounds for believing that in all circumstances of the case- (i) the transfer is for the avoidance or mitigation of adverse action against the data subject; (ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and (iii) if it was practicable to obtain such consent, the data subject would have given his consent; (f) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of this Act; (g) the transfer is necessary in order to protect the vital interests of the data subject; or (h) the transfer is necessary as being in the public interest in circumstances as determined by the Minister. (4) Where the Commissioner has reasonable grounds for believing that in a place as specified under subsection (1) there is no longer in force any law which is substantially similar to this Act, or that serves the same purposes as this Act- (a) the Commissioner shall make such recommendations to the Minister who shall, either by cancelling or amending the notification made under subsection (1), cause that place to cease to be a place to which personal data may be transferred under this section; and (b) the data user shall cease to	

		transfer any personal data of a data subject to such place with effect from the time as specified by the Minister in the notification. (5) A data user who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both. (6) For the purposes of this section, "adverse action", in relation to a data subject, means any action that may adversely affect the data subject's rights, benefits, privileges, obligations or interests.	
		Section 48. Functions of Commissioner (e) to determine in pursuance of section 129 whether any place outside Malaysia has in place a system for the protection of personal data that is substantially similar to that as provided for under this Act or that serves the same purposes as this Act;	
2	Personal Data Protection Regulations 2013		
3	Personal Data Protection (Registration of Data User) Regulations 2013		
4	Personal Data Protection (Fees) Regulations 2013		
5	Personal Date Protection Standard 2015		
6	Personal Data Protection (Compounding Of Offences) Regulations 2016		

7	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
8	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
9	General Code on the Practice of Personal Data Protection (2022)		
10	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)	4.10 TRANSFER OF PERSONAL DATA ABROAD 4.10.1 The Act prohibits the transfer of personal data outside of Malaysia unless the transfer is to a country with sufficient data protection laws, as specified by the Minister in a Government Gazette, which will be based on the Commissioner's recommendation to the Minister.	
		Exceptions 4.10.2 Notwithstanding the above-mentioned prohibition, the Act expressly permits the transfer of personal data abroad where: (i) (ii) (iii) (iv) (v) (vi) the Data Subject has consented to the transfer; or the transfer is necessary for the performance of a contract between the Data User and the Data Subject (for example where a customer gives the Data User an order to transfer money into the account of a third party); or the transfer is necessary to perform or conclude a contract between the Data User and third party which has been entered into at the request or in the interest of the Data Subject; or the transfer is for legal proceedings or obtaining legal advice; or the Data User has reasonable grounds for doing so; or the Data User has taken reasonable	

		precautions to ensure the personal data will not be processed in any manner which contravenes the Act; or (vii) the transfer is necessary to protect the vital interests of the Data Subject (this would relate to matters of life and death as defined in the Act); or (viii) the transfer is necessary as being in public interest as determined by the Minister.	
11	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017	4.6 Transfer of Personal Data 4.6.1 The PDPA prohibits the transfer of Personal Data by a Data User to a place outside Malaysia without the consent of Data Subject. However, Personal Data may be transferred to a country with sufficient data protection laws or for the exercise of any functions conferred on any person by or under any law.	
		Exceptions 4.6.2 However, the Data User may still transfer Personal Data to a place outside Malaysia if:- (a) the Data Subject has granted Data Subject's consent; (b) the transfer is necessary for the performance of a contract between the Data User and the Data Subject; (c) the transfer is necessary to perform a contract between a Data User and the Third Party; (d) the transfer is for legal proceedings or obtaining legal advice; (e) the Data User have reasonable grounds to believe:- (i)the transfer is for the avoidance or mitigation of adverse action against the Data Subject; (ii)it is not practicable to obtain the consent in Writing of the Data Subject to that transfer; and (iii) the Data Subject would have given Data Subject's consent if it was practicable to obtain such	

		consent; (f) the Data User have taken reasonable precautions to ensure Personal Data will not be Processed in any manner which contravenes the PDPA; (g)the transfer is necessary to protect the vital interests of the Data Subject; (h) the transfer is necessary as being in public interest as determined by the Minister; or (i) the transfer is to a country specified by the Minister. 4.6.3 The transfer of Personal Data via removable media device and cloud computing service is not permitted unless authorized in writing by an authorized officer of the organization's highest management of Data User. 4.6.4 The transfer of Personal Data via removable media device and cloud computing service should be recorded. 4.6.5 The transfer of Personal Data via cloud computing service must comply with the principles of personal data protection in Malaysia and other countries that have laws which is substantially similar personal data protection legislation or that serves the same purposes as PDPA. 4.6.6 The transfer of Personal Data conventionally via mail, hand delivery, fax and so on should be recorded.	
12	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)		
13	Personal Data Protection Code of Practice for the		

	Communications Class Data Users 2017		
14	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
15	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
16	Cybersecurity Bill 2024		

#	Regulation	Government Access
		National Security Law, Cybersecurity Law Provisions
		Provision allowed govt to access regulated data/to not comply to data regulation
1	Personal Data Protection Act 2010	Section 39. Extent of disclosure of personal data Notwithstanding section 8, personal data of a data subject may be disclosed by a data user for any purpose other than the purpose for which the personal data was to be disclosed at the time of its collection or any other purpose directly related to that purpose, only under the following circumstances: 18 (a) the data subject has given his consent to the disclosure; (b) the disclosure (i) is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations; or (ii) was required or authorized by or under any law or by the order of a court;
		Section 113. Search and seizure with warrant (1) If it appears to a Magistrate, upon written information on oath from the authorized officer and after 40 such inquiry as the Magistrate considers necessary, that there is reasonable cause to believe that- (a) any premises has been used for; or (b) there is in any premises evidence necessary to the conduct of an investigation into, the commission of an offence under this Act, the Magistrate may issue a warrant authorizing the authorized officer named in the warrant at any reasonable time by day or night and with or without assistance, to enter the premises and if need be by force. (2) Without affecting the generality of subsection (1), the warrant issued by the Magistrate may authorize the search and seizure of- (a) any computer, book, account, computerized data or other document which contains or is reasonably suspected to contain information as to any offence suspected to have been committed;

		(b) any signboard, card, letter, pamphlet, leaflet or notice representing or implying that the person is registered under this Act; or (c) any equipment, instrument or article that is reasonably believed to furnish evidence of the commission of the offence. (3) An authorized officer conducting a search under subsection (1) may, for the purpose of investigating into the offence, search any person who is in or on the premises. (4) An authorized officer making a search of a person under subsection (3) or section 114 may seize or take possession of, and place in safe custody all things other than the necessary clothing found upon the person, and any of those things which there is reason to believe were the instruments or other evidence of the offence may be detained until the discharge or acquittal of the person. (5) Whenever it is necessary to cause a woman to be searched, the search shall be made by another woman with strict regard to decency. (6) If, by the reason of its nature, size or amount, it is not practicable to remove any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article seized under this section, the authorized officer shall by any means seal such computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article in the premises or container in which it is found. (7) A person who, without lawful authority, breaks, tampers with or damages the seal referred to in subsection (6) or removes any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article under seal or attempts to do so commits an offence and shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding six months or to both.
2	Personal Data Protection Regulations 2013	
3	Personal Data Protection (Registration of Data User) Regulations 2013	
4	Personal Data Protection (Fees) Regulations 2013	
5	Personal Date Protection Standard 2015	
6	Personal Data Protection	

	(Compounding Of Offences) Regulations 2016	
7	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016	
8	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner	
9	General Code on the Practice of Personal Data Protection (2022)	
10	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)	
11	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017	
12	Code of Practice on Personal Data Protection for the Insurance and Takaful Insurance Industries in Malaysia (2017)	9. Disclosure Principle 9.1. An Insurer/Operator may only disclose the Data Subject's personal data for the purposes for which the personal data is being, or is to be collected and further processed. This means that personal data must not be collected for one purpose and then used for a different purpose. 9.2. (l)any person to whom disclosure is necessary for the purpose of investigation into any allegation of Insurance/Takaful Intermediaries' and their third party service providers' breach of any laws, rules and regulations, codes of practice including this Code, misconduct or unethical behaviours or practices;
13	Personal Data Protection Code of Practice for the Communications Class Data Users 2017	
14	Personal Data Protection Code of Practice for Private Hospitals	

	in the Healthcare Industry 2022	
15	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022	
16	Cybersecurity Bill 2024	

Penalties

#	Regulation	Corporate Punishments	Individual Punishments
		Forms of penalties (e.g., recommendations for corrective action, public penalties, fines, confiscation of assets and income, data deletion, data processing, business suspension, etc.)	Penalties (penalties, fines, demotion, etc.)
		Forms of penalties on corporate	Forms of penalties on individual
1	Personal Data Protection Act 2010	Section 5. Personal Data Protection Principles (1) The processing of personal data by a data user shall be in compliance with the following Personal Data Protection Principles, namely- (a) the General Principle; (b) the Notice and Choice Principle; (c) the Disclosure Principle: (d) the Security Principle; (e) the Retention Principle: (f)the Data Integrity Principle; and (g) the Access Principle, as set out in sections 6, 7, 8, 9, 10, 11 and 12. (2) Subject to sections 45 and 46, a data user who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.	
		Section 16. Certificate of registration	

		(4) A person who belongs to the class of data users as specified in the order made under subsection 14(1) and who processes personal data without a certificate of registration issued in pursuance of paragraph 16(1)(a) commits an offence and shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.	
		Section 18. Revocation of registration (4) A data user whose registration has been revoked under this section and who continues to process personal data thereafter commits an offence and shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.	
		Section 19. Surrender of certificate of registration (2) A person who fails to comply with subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.	
		Section 29. Non-compliance with code of practice A data user who fails to comply with any provision of the code of practice that is applicable to the data user commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding one year or to both.	
		Section 37. Notification of refusal to comply with data correction request (4) A data user who contravenes subsection (2) commits an offence and shall, on conviction, be liable to a fine not exceeding	

		one hundred thousand ringgit or to imprisonment for a term not exceeding one year or to both.	
		Section 38. Withdrawal of consent to process personal data (4) A data user who contravenes subsection (2) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding one year or to both.	
		Section 40. Processing of sensitive personal data (3) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.	
		Section 43. Right to prevent processing for purposes of direct marketing (4) A data user who fails to comply with the requirement of the Commissioner under subsection (3) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.	
		Section 66. Limitation on contracts The Commissioner shall not, without the approval of the Minister and the concurrence of the Minister of Finance, enter into any contract under which the Commissioner is to pay or receive an amount exceeding two million ringgit.	
		Section 108. Enforcement notice (8) A person who fails to comply with an enforcement notice commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.	

		Section 113. Search and seizure with warrant (7) A person who, without lawful authority, breaks, tampers with or damages the seal referred to in subsection (6) or removes any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article under seal or attempts to do so commits an offence and shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding six months or to both.	
		Section 120. Obstruction to search Any person who- (a) refuses any authorized officer access to any premise which the authorized officer is entitled to have under this Act or in the execution of any duty imposed or power conferred by this Act; (b) assaults, obstructs, hinders or delays any authorized officer in effecting any entry which the authorized officer is entitled to effect under this Act, or in the execution of any duty imposed or power conferred by this Act; or (c) refuses any authorized officer any information relating to an offence or suspected offence under this Act or any other information which may reasonably be required of him and which he has in his knowledge or power to give, commits an offence and shall, on conviction, be liable to imprisonment for a term not exceeding two years or to a fine not exceeding ten thousand ringgit or to both.	
		Section 129. Transfer of personal data to places outside Malaysia (5) A data user who contravenes	

		subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.	
		Section 130. Unlawful collecting, etc., of personal data (7) A person who commits an offence under this section shall, upon conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.	
		Section 141. Obligation of secrecy (2) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding one year or to both.	
		Section 143. Power to make regulation (3) The regulations made under this section or any other subsidiary legislation made under this Act may prescribe for any act or omission in contravention of the regulations or other subsidiary legislation to be an offence and may prescribe for penalties of a fine not exceeding two hundred and fifty thousand ringgit or imprisonment for a term not exceeding two years or to both.	
		Section 45. Exemption (1) There shall be exempted from the provisions of this Act personal data processed by an individual only for the purposes of that individual's personal, family or household affairs, including recreational purposes. (2) Subject to section 46, personal data- (a) processed for- (i) the prevention or detection of	

		crime or for the purpose of investigations; (ii) the apprehension or prosecution of offenders; or (iii) the assessment or collection of any tax or duty or any other imposition of a similar nature, shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act; (b) processed in relation to information of the physical or mental health of a data subject shall be exempted from the Access Principle and other related provisions of this Act of which the application of the provisions to the data subject would be likely to cause serious harm to the physical or mental health of the data subject or any other individual; (c) processed for preparing statistics or carrying out research shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act, provided that such personal data is not processed for any other purpose and that the resulting statistics or the results of the research are not made available in a form which identifies the data subject; (d) that is necessary for the purpose of or in connection with any order or judgement of a court shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act; (e) processed for the purpose of discharging regulatory functions shall be exempted from the General Principle, Notice and	

		Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act if the application of those provisions to the personal data would be likely to prejudice the proper discharge of those functions; or (f) processed only for journalistic, literary or artistic purposes shall be exempted from the General Principle. Notice and Choice Principle, Disclosure Principle, Retention Principle, Data Integrity Principle and Access Principle and other related provisions of this Act, provided that- (i) the processing is undertaken with a view to the publication by any person of the journalistic, literary or artistic material; (ii) the data user reasonably believes that, taking into account the special importance of public interest in freedom of expression, the publication would be in the public interest; and (iii) the data user reasonably believes that in all the circumstances, compliance with the provision in respect of which the exemption is claimed is incompatible with the journalistic, literary or artistic purposes.	
		Section 46. Power to make further exemptions (1) The Minister may, upon the recommendation of the Commissioner, by order published in the Gazette exempt- (a) the application of any of the Personal Data Protection Principles under this Act to any data user or class of data users; or (b) any data user or class of data users from all or any of the provisions of this Act. (2) The Minister may impose any	

		terms or conditions as he thinks fit in respect of any exemption made under subsection (1). (3) The Minister may at any time, on the recommendation of the Commissioner, by order published in the Gazette, revoke any order made under subsection (1). PART IV - APPOINTMENT, FUNCTIONS AND POWERS OF COMMISSIONER	
		Section 16. Certificate of registration (1) After having given due consideration to an application under subsection 15(1), the Commissioner may- (a) register the applicant and issue a certificate of registration to the applicant in such form as determined by the Commissioner; or (b) refuse the application. (2) The certificate of registration may be issued subject to such conditions or restrictions as the Commissioner may think fit to impose. (3) Where the Commissioner refuses the application for registration in pursuance of subsection (1), he shall inform the applicant by a written notice that the application has been refused and the reasons for the refusal. (4) A person who belongs to the class of data users as specified in the order made under subsection 14(1) and who processes personal data without a certificate of registration issued in pursuance of paragraph 16(1)(a) commits an offence and shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.	

2	Personal Data Protection Regulations 2013		
3	Personal Data Protection (Registration of Data User) Regulations 2013		
4	Personal Data Protection (Fees) Regulations 2013		
5	Personal Date Protection Standard 2015		
6	Personal Data Protection (Compounding Of Offences) Regulations 2016		
7	Personal Data Protection (Class Of Data Users) (Amendment) Order 2016		
8	Appointment And Revocation Of Appointment Of Personal Data Protection Commissioner		
9	General Code on the Practice of Personal Data Protection (2022)		
10	Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)		
11	Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017		
12	Code of Practice on Personal Data Protection for the Insurance and		

	Takaful Insurance Industries in Malaysia (2017)		
13	Personal Data Protection Code of Practice for the Communications Class Data Users 2017		
14	Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022		
15	Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022		
16	Cybersecurity Bill 2024		

F) Republic of the Union of Myanmar

Legal system overview

#	Regulation	Translation	Purpose of the Legal System
			What purpose does the legal system serve? (e.g. cybersecurity)
		Google translation or Translation by certain organization	
1	The Constitution	Translation by certain organization	Constitution
2	The Competition Law (2015)	Translation by certain organization	3. The objectives of this Law are as follows: (a) to protect and prevent acts that injure of public interests through monopolization or manipulation of prices by any individual or group with intent to endanger fair competition in economic activities, for the purpose of development of the national economy; (b) to be able to control unfair market competition on the internal and external trade and economic

			development; (c) to be able to prevent from abuse of dominant market power; (d) to be able to control the restrictive agreements and arrangements among businesses.
3	Competition Rules (2017)	Translation by certain organization	To prescribes Rules of filing and investigation of business competition dispute under section 56, sub-section (a) of the Competition Law
4	The Electronic Transactions Law (2004)	Translation by certain organization	3. The aims of this Law are as follows: - (a) to support with electronic transactions technology in building a modern, developed nation; Unofficial Translation Page 3 of 14 (b) to obtain more opportunities for all-round development of sectors including human resources, economic, social and educational sector by electronic transactions technologies; (c) to recognize the authenticity and integrity of electronic record and electronic data message and give legal protection thereof in matters of internal and external transactions, making use of computer network; (d) to enable transmitting, receiving and storing local and foreign information simultaneously, making use of electronic transactions technologies; (e) to enable communicating and co-operating effectively and speedily with international organizations, regional organizations, foreign countries, local and foreign government departments and organizations, private organizations and persons, making use of computer network.
5	The Electronic Transactions Law (2014)	Translation by certain organization	
6	The Electronic Transactions Law (2021)	Translation by certain organization	3. ...(shorten)... (f) To protect the personal data of the public in accordance with the Law.

7	The Telecommunications Law (2013)	Translation by certain organization	4. The objectives of this Law are as follows: (a) to enable to support the modernization and development of the nation with telecommunications technology; (b) to enable to bring out Telecommunications Service that will be able to provide high quality and worth services to the users by allowing fair and transparent competitions from domestic and abroad in the telecommunications sectors which are developing; (c) to enable to give more opportunities to the general public to use Telecommunications Services by expanding the telecommunications network in the entire country along with the telecommunications technology which is developing; (d) to enable to protect the telecommunications service providers and users in accord with law; (e) to enable to supervise telecommunications service, network facilities and telecommunications equipment which require licence for national peace and tranquility and for public security.
8	The Law Protecting the Privacy and Security of Citizens (2017)	Translation by certain organization	To give the rights and protection of privacy and security of citizens
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)	Translation by certain organization	To suspend Sections 5,7,8 in accordance with Article 420 of the State Constitution. The law shall be deemed to be effected only during the period when the State Administration Council is assigned to the State Power

			according to Article 419 of the State Constitution.
10	The Financial Institutions Law (2016)	Translation by certain organization	The aim of this Law is- (a) to obtain sustainable economic development of the State; (b) to develop the financial sector of the State; (c) to ensure that financial Institution within the State carry on financial services activities in line with the international standards ; (d) to enable the Central Bank to effectively regulate and supervise the financial institutions in accordance with the international standards; and (e) to maintain the stability, safety and soundness of the financial system and to protect the depositors' interest.
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)	Translation by certain organization	To prescribes Rules of Insurance business including license application, responsibility, supervisory party, and dispute investigation
12	Law Relating to Private Health Care Services (2007)	Translation by certain organization	The aims of this Law are as follows: (a) to develop private health care services in accordance with the national health policy; (b) to participate and carry out systematically by private health care services in the national health care system as an integral part; (c) to enable utilizing effectively the resources of private sector in providing health care to the public; (d) to enable the public to choose as desired in fulfilling their needs for health by establishing private health care services; (e) to enable provision of quality

			service at fair cost and to take responsibility.
13	(Draft) Bill - Cyber Security Law and privacy and data protection	Translation by certain organization	This law shall serve the following objectives: (a) To be able to safely and securely use cyber sources, critical information infrastructure and data stored with electronic technology. (b) To be able to protect the personal information of the public in accordance with the law (c) To be able to safeguard and protect from harassing, cyber-attacking and cyber-fraud by using electronic technology to harm the national sovereignty, peace and stability. (d) To be able to supervise in ensuring that cyber security services are systematically implemented in accord with the law. (e) To prevent cyber-crimes. (f) To support the digital economy. (g) To recognise and legally protect the authenticity and integrity of electronic information in conducting local and international communications using cyber sources.
14	E-Commerce Guidelines (September 2023)	Translation by certain organization	The objectives are as follows: (a) Understanding the provisions of applicable laws and regulations covering e-commerce and following them correctly; (b) supporting effective law enforcement to develop consumer protection, fair trading practices, and a secure e-commerce ecosystem.

#	Regulation	Form of legal system	Target Business
		Is it introduced in accordance with government ordinances and guidelines? (Is it introduced in a format that ensures lead time?)	Does the law target specific industry or in general? Is it clearly stated in the regulations?

		Regulation level	Industry
1	The Constitution	Constitution	General
2	The Competition Law (2015)	Law	Commerce
3	Competition Rules (2017)	Rules	Commerce
4	The Electronic Transactions Law (2004)	Law	General
5	The Electronic Transactions Law (2014)	Law	General
6	The Electronic Transactions Law (2021)	Law	General
7	The Telecommunications Law (2013)	Law	Telecommunication
8	The Law Protecting the Privacy and Security of Citizens (2017)	Law	General
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)	Law	General
10	The Financial Institutions Law (2016)	Law	Finance
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)	Notification	Finance
12	Law Relating to Private Health Care Services (2007)	Law	Healthcare
13	(Draft) Bill - Cyber Security Law and privacy and data protection	Law	General
14	E-Commerce Guidelines (September 2023)	Guideline	Commerce

#	Regulation	Regulatory authority	Jurisdiction
		Which regulatory authority has jurisdiction over regulation?	Cyber security, data security, personal information protection, etc.
		Name of ministry/organization	Similar to purpose?
1	The Constitution	Republic of the Union of Myanmar	Personal privacy
2	The Competition Law (2015)	The ministry assigned duty by the Union Government (Unspecified by the law)	Industrial data
3	Competition Rules (2017)	Ministry of Commerce	Industrial data
4	The Electronic Transactions Law (2004)	Ministry of Communications, Posts and Telegraphs	Data security
5	The Electronic Transactions Law (2014)	Ministry of Communications, Posts and Telegraphs	Data security
6	The Electronic Transactions Law (2021)	Ministry of Communications, Posts and Telegraphs	Personal data, Cyber security
7	The Telecommunications Law (2013)	Ministry of Communications and Information Technology of the Union Government	
8	The Law Protecting the Privacy and Security of Citizens (2017)	Ministry of Home Affairs	Personal privacy
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)	Ministry of Home Affairs	Personal privacy
10	The Financial Institutions Law (2016)	Ministry of Finance and Revenue	Personal information
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)	Ministry of Finance and Revenue	Personal information
12	Law Relating to Private Health Care Services (2007)	Ministry of Health	Personal information
13	(Draft) Bill - Cyber Security Law and privacy	Ministry of Transport and Communication	Cyber security

	and data protection		
14	E-Commerce Guidelines (September 2023)	Ministry of Commerce	Personal information, Cyber security

#	Regulation	Status	Citation
		Legislation / Public Comment / Passage / Enforcement / Amendment, etc.	
		Status of the regulation: Draft = drafting (new regulation) published = published in the gazzette but not yet enacted Enact = published in the gazzette and already enacted Amendment = enacted regulation being on amending process	URL
1	The Constitution	Enact	https://www.constituteproject.org/constitution/Myanmar_2008
2	The Competition Law (2015)	Enact	https://www.asean-competition.org/file/pdf_file/Myanmar-Competition%20Law%20(English%20Version).pdf
3	Competition Rules (2017)	Enact	https://www.commerce.gov.mm/sites/default/files/documents/2022/10/Compeition%20Rules%20(English%20Version).pdf
4	The Electronic Transactions Law (2004)	Enact	https://www.myanmartradeportal.gov.mm/uploads/legals/2018/12/Electronic%20Transactions%20Law%202004(English).pdf
5	The Electronic Transactions Law (2014)	Enact	https://www.myanmartradeportal.gov.mm/uploads/legals/2018/12/Electronic%20Transactions%20Law%202004(English).pdf
6	The Electronic Transactions Law (2021)	Enact	https://www.myanmartradeportal.gov.mm/uploads/legals/2018/12/Electronic%20Transactions%20Law%202004(English).pdf
7	The Telecommunications Law (2013)	Enact	https://www.mlis.gov.mm/mLsView.do;jsessionid=873EF072104248EAB3CBDDB2DE19F143?lawordSn=1076
8	The Law Protecting the Privacy and Security of Citizens (2017)	Enact	https://www.mlis.gov.mm/mLsView.do;jsessionid=E5E1CFF9699C13D185BF078893C38D54?lawordSn=16023

9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)	Enact	https://www.myanmar-responsiblebusiness.org/pdf/Law-Protecting-Privacy-and-Security-of-Citizens_en_unofficial.pdf
10	The Financial Institutions Law (2016)	Enact	https://www.cbm.gov.mm/sites/default/files/regulate_launder/financial_institutions_law_updated_by_cbm_20160303website-1_0.pdf
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)	Enact	https://www.mopf.gov.mm/sites/default/files/upload_pdf/2017/07/ins%20business%20rules-eng.pdf
12	Law Relating to Private Health Care Services (2007)	Enact	https://www.mlis.gov.mm/mLsView.do;jsessionid=64D9E18FBAACB36EC61C3EB93D9820E4?lawordSn=793
13	(Draft) Bill - Cyber Security Law and privacy and data protection	Draft	https://www.hrw.org/sites/default/files/media_2022/02/220127%20Cyber-Security-Bill-EN.pdf
14	E-Commerce Guidelines (September 2023)	Enact	https://www.lincolnmyanmar.com/wp-content/uploads/2024/02/E-commerce-guidelines.pdf

Definitions for basic items

#	Regulation	Type and Scope of Data	Data processing and handling
		Personal data, personal information/sensitive and important data/children and minors' data, etc. Is the scope of data clearly written in the regulations? What are the unclear points?	Processing, handling / disclosure, sharing, provision, transmission, outsourcing / use for advertising, etc.
		Specific type of data required to complied with the regulation	Provision for data processing
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)	2. The following expressions contained in this law shall have the meanings given here under: -	

		(a) Information means data, text, image, audio, video, code, computer programmes, software, application and database; (b) Electronic record means a record generated, sent, received, or stored by means of electronic, magnetic, optical, or any other similar technologies in an information system or for transmission from one information system to another; (c) Electronic data message means information generated, sent, received, or stored by means of electronic, optical, or any other similar technologies, including electronic data interchange, fax, e-mail, telegraph, telex, and telecopy. (d) Computer means a device capable of receiving, transmitting, storing, processing, or retrieving information and records, using arithmetic and logical means by manipulation of electronic, magnetic, optical, or any other similar technologies; (e) Computer network means the network system of the interconnection of computers through use of satellite or by any other technologies; (f) Electronic signature means any symbol or mark arranged personally or on his behalf by electronic technology or any other similar technologies to verify the authenticity of the source of the electronic record and the absence of amendment or substitution; (g) Certification authority means a person or an organization that has been granted a licence by the Control Board under this Law for services in respect of the electronic signature; (h) Certificate means the certificate issued to a subscriber by the certification authority as	

		an electronic data message or other record identifying the relation between the signer of an electronic signature and the electronic data message; (i) Originator means a person by whom or on whose behalf the electronic record or electronic data message purports to have been created, generated or sent. This expression does not include a person acting as an intermediary with respect to electronic record or electronic data message; (j) Addressee means a person who is intended by the originator to receive the electronic record or electronic data message. This expression does not include a person acting as an intermediary with respect to an electronic record or electronic data message; (k) Subscriber means a person who is by any technologies identified as an authentic signer of an electronic signature in the certificate;	
		4. (a) The provisions contained in this Law shall apply to any kind of electronic record and electronic data message used in the context of commercial and non-commercial activities, including domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges and storage of information. (b) This Law shall apply to any person who commits any offence actionable under this Law within the country or from inside of the country to outside of the country, or from outside of the country to inside of the country by making use of the electronic transactions technology.	

5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)	2. ...(shorten)... (l) Personal Data means information that identifies or is capable of identifying an individual. (m) Personal Data Management Officer means a person and its staff authorised by a governmental department or an organisation to be responsible for collecting, retaining, and using personal data in accordance with the law, or any existing laws. ..... (continue)	2. ...(shorten)... (n) Processing means collecting, receiving, transferring, dissemination, coordinating, restricting, destroying, documenting, archiving, storing, altering, recollection of stored data, advising, utilisation, and disclosure of personal data. (o) Cyber Source means a computer, computer system, computer program or program, network, communication device, and data. (p) Malware means a malicious code that can interfere or harm a cyber source. (q) Cyberspace means the use of cyber sources through technology-based networks. Data collection; Electronic information; Computer programs; Software Use electronic applications to access electronic information over a network or network. An environment in which you can send, communicate, distribute, or receive networked or reciprocal networks. (r) Cyber Attack means any type of attack that attempts to commit, aids to commit, incites to commit, or abets of an attack, the use of cyber sources with the intent of undermining the national administration, finance, economy, the rule of law, national security, or public safety and the livelihood of the public within the cyberspace. (s) Central Body means the Central Body of Electronic Transactions formed under this Law; (t) Ministry means the Ministry of Communications, Posts and Telegraphs; (u) Control Board means the

			Electronic Transactions Control Board formed under this Law.
7	The Telecommunications Law (2013)	3. The following expressions contained in this Law shall have the meanings given hereunder: (a) Telecommunications means transmission or reception of any information in its original or modified form by using wire, fiber optic cable or any other conducting cable or by using any means of radio wave, optical or any other forms of electromagnetic transmission; (b) Information means data, text, image, sound, code, sign, signal, any collection of data and combination of more than one thereof and similar matters; .... (continue)....	
8	The Law Protecting the Privacy and Security of Citizens (2017)	2. The following expressions in this Law shall have the meanings given hereunder: (a) Constitution means the Constitution of the Republic of the Union of Myanmar; (b) Citizen means a person who is a citizen under the Constitution or under any existing laws; (c) Personal Privacy means the right to freedom of movement, freedom of residence and freedom of speech of a citizen in accordance with law; (d) Personal Security means the security of personal affairs of a citizen. In this expression, the security of residence, or compound and building in the compound, property, correspondence and other communication of a citizen are included; (e) Ministry Concerned means the Ministry of Home Affairs;	

		(f) Person in charge means persons who have responsibility of government departments, government organizations concerned and administration.	
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection	3. The following expressions contained in this law shall have the following meanings: ...(shorten)... (h) Cyber Security means the prevention of any actions that includes destroying, disclosing, accessing, sending, distributing, using, transforming and impeding information, cyber resource, electronic information, the critical information infrastructures without approval or agreement. (i) Information means Data, Text, Image, Voice, Video, Code, Software, Application and Databases; (j) Cyber source means a computer, computer system, computer program or program, network, communication equipment and information. It also includes any other technology and associated devices that are upgraded or advanced based on them.	...(shorten)... (p) Administration means the collection, receiving, transferring, distribution, coordination, prohibition, destruction, recording, maintenance, storing, changing, retrieval of stored data, suggestions, utilisation or disclosures of personal information. ...(continue)...

		(k) Electronic information means information created or sent or received or stored by digital electronic technology or electromagnetic wave technology or any other speci c technology. (l) Critical Information Infrastructure means fundamental infrastructures that are described in Article 14. That word also includes any matter declared as 'Critical Information Infrastructure' by the Union Government or the Central Committee or the Ministry. (m) Data means any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed or has been processed in a computer or computer network and it may be, in any form, stored internally in the memory of the computer. (n) Personal information means any information which has been veri ed or veri ed about a person; (o) Person responsible for maintaining personal information means the person assigned by the government department or the organisation authorised to administer personal information under the existing law or in accordance with the provisions of this Law (p) Administration means the collection, receiving, transferring, distribution, coordination, prohibition, destruction, recording, maintenance, storing, changing, retrieval of stored data, suggestions, utilisation or disclosures of personal information. (q) Administrator of Critical Information Infrastructure means a person implementing	

		matters related to the critical information infrastructure. (r) Electronic or Digital Signature means any symbol or mark arranged personally or on his behalf by electronic technology or any other similar technologies to verify the authenticity of the source of the electronic record and the absence of amendment or substitution. (s) Electronic record means a record generated,sent, received or stored by means of electronic, magnetic, optical or any other similar technologies in an information system or for transmission from one information system to another; ...(continue)...	
14	E-Commerce Guidelines (September 2023)	4. The following expressions used in these guidelines are defined as follows: (a) "Electronic commerce or e-commerce" means the sale of goods or services over the internet or other information networks. In this expression, sales promotion, marketing, logistics, ordering, and delivery are also included. (b) "E-commerce platform entrepreneur" means a person who is responsible for enabling sales through e-commerce by two or more entrepreneurs on an e-commerce platform. (c) "E-commerce business operator" means a person who operates by way of e-commerce or a person who is authorised to so operate. In this expression, e-commerce platform entrepreneurs, entrepreneurs selling on an e-commerce platform, and sellers through social media platforms1 are also included. (d) "Personal data" means personal data about individuals engaged in electronic commerce. (e) "Drip pricing" means a price	

		statement that misleads the consumer by understating the actual price for goods or services sold through e-commerce and adding additional charges to that price after confirmation of the purchase. (f) "Commercial electronic message" means types of data messages, content on a website or in another database, hyperlinks to them, or contact information that contain proposals to sell goods or services. This expression also includes data messages sent for the following commercial purposes: (1) Information sent in connection with things such as products, goods, services, real estate, interest, land ownership; (2) Information sent to promote or advertise opportunities. ....(continue)....	

#	Regulation	Data handlers
		Classification/ distinction by responsibility (data processor, data controller)/ size of data, (national security) critical services, etc.
		Provision on type of data handler
1	The Constitution	
2	The Competition Law (2015)	2. ...(shorten)... (h) Unfair Competition means competitive practices by businesses during the business process which cause or may cause damage to the interests of the State or the legitimate rights and interests of other businesses or of consumers. (i) Business means any business, such as manufactures, distributions, purchases, sells, imports, exports and exchanges the goods, or service. (j) Businessman means the person who carries out any business or service business. In this expression, an organization that operates business or service is also included. ...(continue)...
3	Competition Rules (2017)	
4	The Electronic Transactions Law (2004)	2. The following expressions contained in this law shall have the meanings given here under: - (a) Information means data, text, image, audio, video, code, computer programmes, software, application and database; (b) Electronic record means a record generated, sent, received, or stored by means of electronic, magnetic, optical, or any other similar

		technologies in an information system or for transmission from one information system to another; (c) Electronic data message means information generated, sent, received, or stored by means of electronic, optical, or any other similar technologies, including electronic data interchange, fax, e-mail, telegraph, telex, and telecopy. (d) Computer means a device capable of receiving, transmitting, storing, processing, or retrieving information and records, using arithmetic and logical means by manipulation of electronic, magnetic, optical, or any other similar technologies; (e) Computer network means the network system of the interconnection of computers through use of satellite or by any other technologies; (f) Electronic signature means any symbol or mark arranged personally or on his behalf by electronic technology or any other similar technologies to verify the authenticity of the source of the electronic record and the absence of amendment or substitution; (g) Certification authority means a person or an organization that has been granted a licence by the Control Board under this Law for services in respect of the electronic signature; (h) Certificate means the certificate issued to a subscriber by the certification authority as an electronic data message or other record identifying the relation between the signer of an electronic signature and the electronic data message; (i) Originator means a person by whom or on whose behalf the electronic record or electronic data message purports to have been created, generated or sent. This expression does not include a person acting as an intermediary with respect to electronic record or electronic data message; (j) Addressee means a person who is intended by the originator to receive the electronic record or electronic data message. This expression does not include a person acting as an intermediary with respect to an electronic record or electronic data message; (k) Subscriber means a person who is by any technologies identified as an authentic signer of an electronic signature in the certificate;
5	The Electronic Transactions Law (2014)	
6	The Electronic Transactions Law (2021)	2. ...(shorten)... (l) Personal Data means information that identifies or is capable of identifying an individual. (m) Personal Data Management Officer means a person and its staff authorised by a governmental department or an organisation to be responsible for collecting, retaining, and using personal data in accordance with the law, or any existing laws. ..... (continue)
7	The Telecommunications Law (2013)	
8	The Law Protecting the Privacy and	

	Security of Citizens (2017)	
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)	
10	The Financial Institutions Law (2016)	
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)	
12	Law Relating to Private Health Care Services (2007)	
13	(Draft) Bill - Cyber Security Law and privacy and data protection	...(shorten)... (o) Person responsible for maintaining personal information means the person assigned by the government department or the organisation authorised to administer personal information under the existing law or in accordance with the provisions of this Law (p) Administration means the collection, receiving, transferring, distribution, coordination, prohibition, destruction, recording, maintenance, storing, changing, retrieval of stored data, suggestions, utilisation or disclosures of personal information. (q) Administrator of Critical Information Infrastructure means a person implementing matters related to the critical information infrastructure ...(shorten)... (v) Subscriber means a person who is by any technologies identi ed as an authentic signer of an electronic signature in the electronic or digital certi cate; (w) Original Sender means a person by whom or on whose behalf the information purports to have been created, generated or sent. This expression does not include a person acting as an intermediary with respect to electronic information; (x) Addressee means a person who is intended by the original sender to receive the electronic information. This expression does not include a person acting as an intermediary with respect to electronic information; (y)Digital Platform Service means any over the top (OTT) service that can provide the service to express data, information, images, voices, texts and video online by using cyber resources and similar systems or materials. (z)Digital Platform Service Provider means any individual or any entity providing digital platform service in Myanmar. Apart from Articles 58 and 62, that word does not include companies and

		organisations that hold telecommunication service licences under the telecommunication law. (aa) Cyber Security Provider means any individual or entity who is providing any cyber security services by using cyber sources or similar systems or materials with regard to the information technology system. ...(continue)...
14	E-Commerce Guidelines (September 2023)	...(shorten)... (h) "Data controller" means authorised persons or persons empowered by law, government authorities, government organisations or organisations formed separately or jointly by other organisations who/that have the right to manage personal data. (i) "Consumer" means a user who purchases goods or services through e-commerce.

Legal basis

#	Regulation		
		consent	necessary for the performance of a contract
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)	Chapter (X) Protection of Personal Data 27-bis. (a) The Personal Data Management Officer shall; (i) systematically store, protect and process personal data that he is responsible for according to its type, and level of security in accordance with the Law; (ii) prohibit the examination, disclosure, informing, dissemination, transmission, alteration, destruction, copying, or submission as evidence of the personal data of an individual without the consent of such individual, or the permission by the provision of an existing law to any individual or organization;	

		(iii) refrain from processing personal data contrary to the objectives set out in this Law; (iv) systematically destroy all personal data that are retained, within a retention period, after the designated period expires.	
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection	11. The person responsible for managing and keeping the personal information shall — (a) systematically keep, protect and manage the personal information based on its types, security levels in accordance with the law (b) not allow, disclose, inform, distribute, dispatch, modify, destroy, copy and submit as evidence of the personal information of an individual without the consent or the permission in the provision of an existing law to any individual or organisation. (c) not utilise personal	

		information for managing issues that are not in compliance with the objectives (d) systematically destroy the personal information that is collected to be used for a period of time after a certain period	
14	E-Commerce Guidelines (September 2023)	75. An e-commerce business operator shall apply the following basic principles of conduct, as appropriate, to personal data related to his business activities: (a) Limitation on collection of data. The collection of personal data and payment information shall be limited. Any personal data, including sensitive data, shall be collected in accordance with the law and by reasonable means, by identifying the person who will collect the data, or by guaranteeing that it will not be used for any other improper purpose, or by obtaining consent in advance. (b) Collecting good quality data. The personal data to be collected shall be collected only to the extent necessary to meet the purposes for which it will be used, and care shall be taken to ensure that the data is accurate and complete and up-to-date. (c) Use only for specified purposes. The purpose for which the personal data will be collected shall be determined no later than at the time the data is collected, and the use shall be limited to only that purpose if there are other conflicting purposes, and each situation where the purpose may change shall be identified. (d) Restrictions on use. Action shall be taken to prevent the disclosure of personal data, access/use, or use (even occasionally) for purposes other than the specified purpose (except in cases where the	

		subject's consent has been obtained or the use is allowed by law). The retained data may not be transferred or sold to any person or organisation, whether for a fee or free of charge. In addition, there shall be no disclosure to the public. Once the purpose of the data collection is accomplished, the data shall be kept only for a certain period beyond the original purpose or shall be destroyed, unless destruction is prohibited by law or in a situation where destruction would be contrary to the public interest. (e) Protection in terms of security. Be sure to use security safeguards appropriate to the nature of the market to protect against "risks" such as loss of access or unauthorised access, destruction, use, modification or disclosure of personal data. However, if [a security breach] happens due to the negligence of the consumer or his directly sharing with others confidential data such as his password, the e-commerce business operators shall not be held responsible. (f) Being honest and open. Establish a general policy of honesty and transparency related to development, practice, and policies regarding personal data. The policy should include data on the nature and type of personal data, the main purposes of the use of the data, and the identity and permanent address of the data controller. (g) Individual participation. Individuals have the following rights of participation as basic principles: (1) Right to obtain the data subject's data from the data controller, or right to obtain confirmation of whether or not the data controller has data	

		related to him in his possession; (2) data about the subject shall be communicated within a reasonable period of time, in a reasonable manner, and in an easy-to-understand format, and if it is necessary to pay a fee, the amount shall not be excessive; (3) If a request made pursuant to the rights in sub-clauses (1) and (2) above is rejected, the individual shall have the right to request the reason for the rejection and to appeal against such rejection; (4) The data owner has the right to complain about his data, and if his submission is successful, he has the right to have the data destroyed, corrected, completed or amended. (h) Accountability. The person responsible as data controller shall comply with the basic principles of conduct referred to above and be responsible for implementing the measures to be applied to achieve a benefit. (i) Consent. For the disclosure or use and collection of data about the subject, the consent of the subject shall be requested or the subject shall be notified that his consent is needed. (j) Challenges related to compliance. Consumers shall be able to inform the organisations' regulatory authorities and persons put in charge about challenges related to the basic principles of conduct referred to above.	

#	Regulation		
		necessary for compliance with a legal obligation	necessary in order to protect the vital interests
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		

4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection		
14	E-Commerce Guidelines (September 2023)		

#	Regulation		
		necessary for the performance of a task carried out in the public interest or in the exercise of	necessary for the purposes of the legitimate interests pursued by the controller or by a third party

		official authority vested in the controller	
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection		
14	E-Commerce Guidelines (September 2023)		

#	Regulation	opt-out	others
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection		
14	E-Commerce Guidelines		75. An e-commerce business operator shall apply the

	(September 2023)		following basic principles of conduct, as appropriate, to personal data related to his business activities: (a) Limitation on collection of data. The collection of personal data and payment information shall be limited. Any personal data, including sensitive data, shall be collected in accordance with the law and by reasonable means, by identifying the person who will collect the data, or by guaranteeing that it will not be used for any other improper purpose, or by obtaining consent in advance. (b) Collecting good quality data. The personal data to be collected shall be collected only to the extent necessary to meet the purposes for which it will be used, and care shall be taken to ensure that the data is accurate and complete and up-to-date. (c) Use only for specified purposes. The purpose for which the personal data will be collected shall be determined no later than at the time the data is collected, and the use shall be limited to only that purpose if there are other conflicting purposes, and each situation where the purpose may change shall be identified. (d) Restrictions on use. Action shall be taken to prevent the disclosure of personal data, access/use, or use (even occasionally) for purposes other than the specified purpose (except in cases where the subject's consent has been obtained or the use is allowed by law). The retained data may not be transferred or sold to any person or organisation, whether for a fee or free of charge. In addition, there shall be no disclosure to the public. Once the purpose of the data collection is

			accomplished, the data shall be kept only for a certain period beyond the original purpose or shall be destroyed, unless destruction is prohibited by law or in a situation where destruction would be contrary to the public interest. (e) Protection in terms of security. Be sure to use security safeguards appropriate to the nature of the market to protect against "risks" such as loss of access or unauthorised access, destruction, use, modification or disclosure of personal data. However, if [a security breach] happens due to the negligence of the consumer or his directly sharing with others confidential data such as his password, the e-commerce business operators shall not be held responsible. (f) Being honest and open. Establish a general policy of honesty and transparency related to development, practice, and policies regarding personal data. The policy should include data on the nature and type of personal data, the main purposes of the use of the data, and the identity and permanent address of the data controller. (g) Individual participation. Individuals have the following rights of participation as basic principles: (1) Right to obtain the data subject's data from the data controller, or right to obtain confirmation of whether or not the data controller has data related to him in his possession; (2) data about the subject shall be communicated within a reasonable period of time, in a reasonable manner, and in an easy-to-understand format, and if it is necessary to pay a fee, the amount shall not be excessive; (3) If a request made pursuant to

			the rights in sub-clauses (1) and (2) above is rejected, the individual shall have the right to request the reason for the rejection and to appeal against such rejection; (4) The data owner has the right to complain about his data, and if his submission is successful, he has the right to have the data destroyed, corrected, completed or amended. (h) Accountability. The person responsible as data controller shall comply with the basic principles of conduct referred to above and be responsible for implementing the measures to be applied to achieve a benefit. (i) Consent. For the disclosure or use and collection of data about the subject, the consent of the subject shall be requested or the subject shall be notified that his consent is needed. (j) Challenges related to compliance. Consumers shall be able to inform the organisations' regulatory authorities and persons put in charge about challenges related to the basic principles of conduct referred to above.

Rights of the data subject

#	Regulation	Right to be informed	Right of access
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		

6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection		
14	E-Commerce Guidelines (September 2023)		

#	Regulation	Right to rectification	Right to erasure
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		

5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection		
14	E-Commerce Guidelines (September 2023)		

#	Regulation		
		Right to restrict processing	Right to data portability
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		

4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection		
14	E-Commerce Guidelines (September 2023)		

#	Regulation	Right to object	Right not to be subject to a decision based solely on automated processing
1	The Constitution		

2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection		
14	E-Commerce Guidelines (September 2023)		

#	Regulation

		Right to withdraw consent	others
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		(3. Every citizen has the right to enjoy fully personal privacy and personal security of citizens as set forth in the Constitution.)
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection		
14	E-Commerce Guidelines (September 2023)		

Extraterritorial application

#	Regulation	applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction	applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security		

	Law and privacy and data protection		
14	E-Commerce Guidelines (September 2023)		

#	Regulation		
		no express territorial scope, but would require some nexus to the jurisdiction	other
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)	4. (a) The provisions contained in this Law shall apply to any kind of electronic record and electronic data message used in the context of commercial and non-commercial activities, including domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges and storage of information. (b) This Law shall apply to any person who commits any offence actionable under this Law within the country or from inside of the country to outside of the country, or from outside of the country to inside of the country by making use of the electronic transactions technology.	
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)	2. The provisions in this Law shall apply to: (a) any person, department and organization within the territory which includes the land, water and airspace of the Republic of	

		the Union of Myanmar. (b) Myanmar citizens who are anywhere beyond the limits of the Republic of the Union of Myanmar.	
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection	2. Provisions in this law shall relate to the following matters. (a) Oences committed by – anyone residing in the country or vehicles and aircrafts registered in accord with any existing law; or a Myanmar citizen: or a foreigner temporarily or permanently residing in Myanmar; or o ences committed locally and internationally. (b) Any matters of communications made with anyone either directly or indirectly with regards to the cyber resource within the national cyber space; or between national and other cyber spaces.	
14	E-Commerce Guidelines (September 2023)		

#	Regulation	Representatives of controllers or processors not established in the country
1	The Constitution	
2	The Competition Law (2015)	
3	Competition Rules (2017)	
4	The Electronic Transactions Law (2004)	
5	The Electronic Transactions Law (2014)	
6	The Electronic Transactions Law (2021)	
7	The Telecommunications Law (2013)	
8	The Law Protecting the Privacy and Security of Citizens (2017)	
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)	
10	The Financial Institutions Law (2016)	
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)	
12	Law Relating to Private Health Care Services (2007)	
13	(Draft) Bill - Cyber Security Law and privacy and data protection	

14	E-Commerce Guidelines (September 2023)	

Notification obligation

#	Regulation	Data breach notification to authorities	Data breach notification to affected individuals
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		

13	(Draft) Bill - Cyber Security Law and privacy and data protection		
14	E-Commerce Guidelines (September 2023)	79. An e-commerce business operator shall notify the relevant authority abuses of technological measures, leaks of personal data, and violations of applicable laws are found.	

Obligations of Data Fiduciaries

#	Regulation	external	external
		Notification of data processing	registration of database
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue		

	(Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection	23. The subscriber must (a) When using a valid permanent certi cate with information identifying electronic signature, care must be taken not to allow that information to be misused by others. (b) Care must be taken to ensure that the personal data and additional information are valid and accurate when using the electronic certi cate issued as the electronic signature within the permitted period. (c) If the con dentiality of the information on the electronic signature is leaked or If in a situation where the con dential information may be leaked, Notice must be given to those associated with the electronic signature without delay according to the procedure arranged by the electronic certi cation authority or with the appropriate arrangement.	
14	E-Commerce Guidelines (September 2023)		

#	Regulation	external	external
		Data protection impact assessment	Others
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		

6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection		18. The offcial responsible for managing and maintaining the critical information infrastructure shall; (a) Keep information related to critical information infrastructure in accordance with regulations, depending on the level of information; (b) follow the regulations in disseminating, producing, transferring, receiving and saving information on important information infrastructure; (c) submit the cybersecurity report to concerned ministries and organisations at least once a year.
14	E-Commerce Guidelines (September 2023)		

#	Regulation	internal	internal
		technical and organisational measures	Purpose Limitation
1	The Constitution		
2	The Competition Law (2015)	17. The acts for the purposes of unfair competition under this law include as follows; (a) misleading of consumers; (b) disclosing business secrets; (c) coercing of businessmen to each other; (d) defaming of the reputation of another business; (e) disturbing the operation of another business; (f) advertising and sale promotion for the purpose of unfair competition; (g) discriminating among businessmen; , (h) selling goods at price lesser than production cost or cost, insurance and freight (CIF) in the market; (i) abusing influence of his business, inducing or instigating of a party under contract with other businesses to breach the contract; 12 (j) exercising unfair competitive act in competition stipulated by the Commission for the interests of consumers when necessary. 19. No businessman shall, in respect of disclosing secrets of any other business, carry out any of the following acts; (a) infringing security measures protected by the lawful owners of business secrets in accessing and collecting of business secrets and information related to such secret; (b) using or revealing information of business secret without permission of lawful owner of such business; (c) deceiving a person with an obligation to maintain secrets or abusing the confidence of such	

		person in accessing, collecting, collecting or revealing of business secrets and information related to such secrets; (d) leaking business secrets and procedures of products distribution owned by other persons who conduct systematically in accordance with the Law; 13 (e) leaking economic information by infringing security measures exercised by the State-owned organization; (f) carrying out business activities or applying business licence or distributing goods by using information contained in subsection(e).	
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)	Chapter (X) Protection of Personal Data 27-bis. (a) The Personal Data Management Officer shall; (i) systematically store, protect and process personal data that he is responsible for according to its type, and level of security in accordance with the Law; (ii) prohibit the examination, disclosure, informing, dissemination, transmission, alteration, destruction, copying, or submission as evidence of the personal data of an individual without the consent of such individual, or the permission by the provision of an existing law to any individual or organization; (iii) refrain from processing personal data contrary to the objectives set out in this Law; (iv) systematically destroy all personal data that are retained,	

		within a retention period, after the designated period expires. 27-bis. (b) The investigation team, or the person mandated or instructed to act on their behalf, who receives information that includes personal data in accordance with the existing laws, shall keep the information confidential except when disclosing the information to persons permitted in accordance with the Law	
7	The Telecommunications Law (2013)	17. The business licensee shall keep information and contents securely that are transmitted or received through his telecommunications service and confidential personal information of each individual users, and shall not disclose and inform to irrelevant person except where allowed in accord with the existing laws.	
8	The Law Protecting the Privacy and Security of Citizens (2017)	4. The ministry concerned and person in charge shall protect not to deprive of personal privacy and personal security of citizens. 5. The ministry concerned and person in charge shall: (a) protect any person not to deprive of personal privacy or personal security other than it is in accordance with existing laws; (b) if they desire to enter a residence and a room used as a residence, a building or compound and buildings in a compound of a person to search and seize something, or to search and arrest any person therein under any existing laws, carry out it with at least two witnesses including any person who is an administrator, village headmen, hundred-household head or ten-household head of	

		the respective ward or village-tract.	
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)	Duty to Maintain Secrecy 81. (a) A bank shall keep secret the information relating to the affairs or the account, record, and transaction of a customer of a bank. (b) No director, officer or employee of any bank licensed institution whether during his tenure of office, or thereafter, and no person who has by any means, access to customer information, shall provide or otherwise disclose to any person, such customer information. (c) No person who has any information or document which to the person's knowledge was disclosed in contravention of sub-section (a) shall disclose the same to any other person.	
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)	31. An insurer or underwriting agent shall: (a) as regards the report of the actuarial valuation carried out in accordance with sub-section (d) of section 12 of the Law cause revaluation with another actuary to be conducted, as directed by the Supervisory Board; (b) bear the expenses to be incurred pursuant to sub-rule(a); (c) transact the life assurance business in accordance with the suggestions and recommendations contained in the actuarial valuation report; (d) keep the information and facts of a life assured confidential; (e) make provision to have assets sufficient to meet its liabilities.	

12	Law Relating to Private Health Care Services (2007)	25. The duties and obligations of the person-in-charge and health care service provider are as follows: (a) providing health care mainly for the requirement of patient's health; (b) complying in accordance with the notifications, orders and directives issued by the Central Body, the Ministry of Health and Department of Health; (c) complying in accordance with the existing laws, rules, notifications, orders and directives relating to health; (d) complying with and exercising the modern and developed medical technology and methods in accordance with the directives issued by the Central Body; (e) complying in accordance with the directives relating to the highly infectious disease and criminal cases stipulated by the Ministry of Health, from time to time; (f) if necessary, referring in time to the relevant specialist, department and hospital aiming for the benefit of the patient; (g) providing life-saving treatment to any emergency patient and making referral if necessary; (h) providing high quality service to the public at fair service charge; (i) complying with the directives of the Private Health Care Quality Control and Promotion Body and the different levels of	

		supervisory committee; (j) laying down plans to be able to appease the dissatisfaction of health care user; (k) forming the administrative sub-body, the sub-body for quality control and promotion and other necessary sub-bodies as may be required according to the size and type of hospital; (l) keeping confidential of the patient's personal health matter except on official request of the relevant government department and organization; (m) obtaining permission of the Ministry of Health, if it is required to do research by making use of patients; (n) paying stipulated taxes and revenues regularly. (o) avoiding from performing any other services without permission or licence, in carrying out private health care services permitted under the relevant licence.	
13	(Draft) Bill - Cyber Security Law and privacy and data protection	11. The person responsible for managing and keeping the personal information shall — (a) systematically keep, protect and manage the personal information based on its types, security levels in accordance with the law (b) not allow, disclose, inform, distribute, dispatch, modify, destroy, copy and submit as evidence of the personal information of an individual without the consent or the permission in the provision of an existing law to any individual or organisation. (c) not utilise personal information for managing issues	

		that are not in compliance with the objectives (d) systematically destroy the personal information that is collected to be used for a period of time after a certain period 12. The investigation team who receives information that includes personal information or the person mandated or instructed on their behalf shall keep the information con dential except disclosing the information in hand in accordance with the law. 18. The offcial responsible for managing and maintaining the critical information infrastructure shall; (a) Keep information related to critical information infrastructure in accordance with regulations, depending on the level of information; (b) follow the regulations in disseminating, producing, transferring, receiving and saving information on important information infrastructure; (c) submit the cybersecurity report to concerned ministries and organisations at least once a year. 34. The cyber security service providers shall perform the following; (a) planning and implementing cyber security preventing measures to support the Department and Cyber Security Breach Emergency Response teams; (b) providing warnings on cyber security risks and preventive guidance; (c) developing response plans and solutions against malicious codes, cyber-attacks, hacking, or other security breaches.	

		(d) Immediate implementation of appropriate emergency response, response and noti cation of stakeholders in the event of a cyber security attack; (e) Applying cyber security technology and required standards (e) Applying cyber security technology and required standards (f) Prevent leaking, damaging or loss of information of service users. (g) Immediate report to cyber security breach emergency response team and department in case of emergency. (h) Payment of prescribed license fees (i) Submission of business report as prescribed 35. Prevention, removal, destruction and cessation shall be made accordingly in a timely manner, following the provision of information by the department that a digital platform service provider in Myanmar causes any of the following on cyberspace; (a) Speech, texts, image, video, audio les, signs or other ways of expressions causing hate, disrupting unity, stabilisation and peace. (b) Misinformation and disinformation (c) Sexually explicit material that is not culturally appropriate for Myanmar society to see; Photos, Audio les, Videos, Texts, Signs, Symbols and other expressions (d) Child pornography; Photo, Video, Texts, Symbols and other expressions (e) written and verbal statement breaching any existing law (f) A legitimate complaint of the expression, writing, sending, distribution of speech, text, images, video, sound, symbols and other expressions that	

		damage an individual's social standing and livelihood	
14	E-Commerce Guidelines (September 2023)	74. An e-commerce business operator shall comply with the obligations to protect the privacy and personal data of consumers in accordance with the provisions of the Constitution of the Union, Telecommunication Law, the Law Protecting the Privacy and Security of Citizens and other laws in force as well as the basic principles of conduct in this part. 80. E-commerce business operators shall comply with provisions for reducing the risk that individual historical data of users may be breached in the business, on non-discrimination with regard to data such as race and religion, for ensuring non-discrimination in the processes of verifying registration data, that prohibit the sale or disclosure of personal data, and that prohibit the sale, rent or exchange of personal data obtained online without the permission or express consent of the consumer. 86. E-commerce business operators shall manage digital security risks well. Security measures shall be implemented to reduce or mitigate any unwanted side effects associated with consumers participating in e-commerce transactions. In addition, the provisions of the relevant laws of Myanmar shall be followed. 88. An e-commerce business operator shall implement appropriate and effective security measures in order to minimise cyber security risks. In so doing, important activities shall be given special attention,	

		such as data management, authentication process steps (mechanism), data sent (data in transmit), data retained (data at rest), protection of personal data and payment information, security controls, and network security. 89. The contents used in the e-commerce business shall be systematically maintained and protected according to the security level, and specialised management shall be implemented to prevent security breaches. 90. E-commerce business operators shall cooperate with relevant government departments and organisations in activities aimed at improving policy frameworks regarding cyber security. If necessary, they may cooperate with private organisations.	

#	Regulation	internal	internal
		Accuracy	Retention Limitation
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		Chapter (X) Protection of Personal Data 27-bis. (a) The Personal Data Management Officer shall; (i) systematically store, protect and process personal data that he is responsible for according to its type, and level of security in accordance with the Law; (ii) prohibit the examination,

			disclosure, informing, dissemination, transmission, alteration, destruction, copying, or submission as evidence of the personal data of an individual without the consent of such individual, or the permission by the provision of an existing law to any individual or organization; (iii) refrain from processing personal data contrary to the objectives set out in this Law; (iv) systematically destroy all personal data that are retained, within a retention period, after the designated period expires. 27-bis. (b) The investigation team, or the person mandated or instructed to act on their behalf, who receives information that includes personal data in accordance with the existing laws, shall keep the information confidential except when disclosing the information to persons permitted in accordance with the Law
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health		

	Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection	23. The subscriber must (a) When using a valid permanent certi cate with information identifying electronic signature, care must be taken not to allow that information to be misused by others. (b) Care must be taken to ensure that the personal data and additional information are valid and accurate when using the electronic certi cate issued as the electronic signature within the permitted period. (c) If the con dentiality of the information on the electronic signature is leaked or If in a situation where the con dential information may be leaked, Notice must be given to those associated with the electronic signature without delay according to the procedure arranged by the electronic certi cation authority or with the appropriate arrangement.	11. The person responsible for managing and keeping the personal information shall — (a) systematically keep, protect and manage the personal information based on its types, security levels in accordance with the law (b) not allow, disclose, inform, distribute, dispatch, modify, destroy, copy and submit as evidence of the personal information of an individual without the consent or the permission in the provision of an existing law to any individual or organisation. (c) not utilise personal information for managing issues that are not in compliance with the objectives (d) systematically destroy the personal information that is collected to be used for a period of time after a certain period
14	E-Commerce Guidelines (September 2023)		

#	Regulation	internal	internal
		drawing up of codes of conduct	record of processing activities
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		

8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection	15. The Central committees shall; (a) Rede ne the critical information infrastructure with the approval of the State Administration Council as necessary. (b) Instruct the ministry to inform the process of identifying and rede ning the critical information infrastructure on the speci c sectors to the o cial responsible for managing and maintaining critical information infrastructure. (c) Set up policies to keep, record and maintain the information on the important information infrastructure.)	
14	E-Commerce Guidelines (September 2023)		

#	Regulation	internal	internal
		Designation of the data protection officer	Others
1	The Constitution		

2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection		
14	E-Commerce Guidelines (September 2023)		

Data cross-border distribution

#	Regulation	Cross-border data transfer & Exceptions	Data localization
		Provisions for Transborder Data Transfer. What are the exceptions? (e.g., sufficient authorization, transfers based on contracts equivalent to Standard Contract Clauses (SCC) or Binding Corporate Rules (BCR), transfers based on corporate certification, etc.), Transborder transfer assessment (TIA)	Presence or absence of provisions, stipulations regarding the types of data that must be stored in the country
		Provisions for cross boarder data transfer	Conditions for exemption of complying to localization
1	The Constitution		
2	The Competition Law (2015)		
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)		
7	The Telecommunications Law (2013)		
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the		

	Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection	26. The original sender and Addressee receive the electronic record; Sending electronic information and electronic certi cates; Receipt and storage shall be carried out in accordance with the prescribed procedures. However, if we have a separate agreement with each other, we can act in accordance with those agreed-upon methods.	
		28. An electronic record or electronic information shall be deemed as that of the original sender if it is sent either by the original sender himself or by a person authorised to send on behalf of the sender or through an automatic information system arranged by the sender himself or by a person acting on behalf of the sender.	
		29. The Addressee shall be deemed to receivethe information or the electronic record or electronic information from the original sender if; (a) by means agreed between the Addressee and the original sender; or (b) the Addressee receives from a person related to the original sender or a person authorised to send on behalf of the original sender by means of original agreements.	
		30. During or before sending the electronic records or electronic information, the original sender or the Addressee; (a) shall be deemed of having received information for any of the following methods:	

		(1) The Addressee replying himself or by an automated system or by any other means; (2) The Addressee displays a su cient demonstration towards the original sender that he or she had received. (b) can make a separate agreement to acknowledge the receipt.	
		31. The original sender must con rm the receiptof the electronic record or receipt of the electronic information: (a) If the acknowledgement of receipt has not been received in the prescribed case, it shall be deemed that the original sender has never sent it. (b) in the case which is not speci ed, within the period speci ed separately; If no time is speci ed, the original sender may notify the recipient that he/she has not received the acknowledgement of receipt, even within a reasonable time.	
		32. If there is no separate agreement between the original sender and the Addressee of the sending and receiving time, the electronic record or electronic information shall be: (a) The time of transmission is the time of entry into the information system beyond the control of the original sender or its agent (b) The time of reception is as follows: (1) When accessing a designated information system (2) When the recipient used the non-de ned information system (3) When the recipient enters the information system if there is no speci ed information system	
		33.Original sender and Addressee: (a) If there is no separate agreement, the business location of the sender shall be considered	

		as the place of sending. The business location of the Addressee shall also be considered as the place of receipt. (b) If a business is operated in more than one place, the main business area; If there is no business location, the place of permanent residence of the person; In the case of an organisation, the place of establishment established in accordance with the law shall be considered as a permanent address	
14	E-Commerce Guidelines (September 2023)	94. An e-commerce business operator shall comply with the applicable laws, notifications, orders, directives and procedures of Myanmar throughout the process of conducting cross-border ecommerce transactions.	
		95. E-commerce business operators shall comply with the Foreign Exchange Management Regulations and instructions issued by the Central Bank of Myanmar when making payments using foreign currency for cross-border e-commerce transactions, and shall make payments only in Myanmar kyats for domestic transactions.	
		96. An e-commerce business operator who conducts cross-border e-commerce business shall comply with regional and international trade agreements and bilateral agreements of which Myanmar is a member	

#	Regulation	Government Access	Government Access
		National Security Law, Cybersecurity Law Provisions	National Security Law, Cybersecurity Law Provisions
		Provisions on requirement of localization; and Type of data required for localization	Provision allowed govt to access regulated data/to not comply to data regulation
1	The Constitution		
2	The Competition Law (2015)		

3	Competition Rules (2017)		34. In performing its functions and duties, the Investigation Committee: (a) has the right to enter and inspect building, land and workplace of the person who is investigated in accordance with the law; (b) may seal and confiscate, if necessary, money and valuable properties as proof of evidence in accordance with the duties assigned by the Commission, and deposit to the specified bank for keep it safe; (c) may examine business information, documents and evidences and confiscate them as proof of evidence in accordance with the duties assigned by the Commission if needed; (d) in confiscating evidence, shall seize before two witnesses by making three copies of the Evidence Confiscation Form (Form-2). Such form shall be signed by the person who is investigated or whose properties are seized, witnesses who involve in inspection and the investigator. A copy of the form shall be given to the person who is investigated or the person whose properties are seized. (e) if the Commission approves a temporary return of seized properties with the consent of promissory note during the investigation period, those properties shall be returned to the person whose properties are seized, by signing a secured promissory note on temporary return of evidences (Form - 3)
4	The Electronic Transactions Law (2004)		5. The provisions contained in this Law shall not apply to the following matters: (a) "Will" defined in sub-section (h) of section 2 of the Succession Act; (b) "Negotiable instrument"

			defined in section 13 of the Negotiable Instruments Act; (c) "Trust" defined in section 3 of the Trusts Act; (d) "Power of Attorney" granted under the Powers of Attorney Act; (e) Documents relating to title; (f) Instruments prescribed in any existing law to be registered; (g) Matters exempted by the Ministry by issuing notification, with the approval of the Government.
5	The Electronic Transactions Law (2014)		
6	The Electronic Transactions Law (2021)	Chapter (X) Protection of Personal Data 27-bis. (a) The Personal Data Management Officer shall; (i) systematically store, protect and process personal data that he is responsible for according to its type, and level of security in accordance with the Law; (ii) prohibit the examination, disclosure, informing, dissemination, transmission, alteration, destruction, copying, or submission as evidence of the personal data of an individual without the consent of such individual, or the permission by the provision of an existing law to any individual or organization; (iii) refrain from processing personal data contrary to the objectives set out in this Law; (iv) systematically destroy all personal data that are retained, within a retention period, after the designated period expires. 27-bis. (b) The investigation team, or the person mandated or instructed to act on their behalf, who receives information that includes personal data in accordance with the existing laws, shall keep the information confidential except when	27-bis. (c) The provisions relating to the management of personal data shall not apply in the following scenarios: (i) prevention, search and enquiry, investigation, or providing evidence before a court by a governmental department authorised by the Central Committee, the Investigative Team or a rule of law team in relation to cybersecurity, cyber-attacks, Cyber Terrorism, Cyber Misuse and cyber accidents or Cyber Crimes; (ii) search and enquiry, investigation, gathering information, filing a charge, or providing evidence before a court by a governmental department authorised by the Central Committee, the Investigative Team or a rule of law team mandated to work on a criminal matter; (iii) enquiry, investigation, gathering information or coordination of information is undertaken if cybersecurity and Cyber Crimes issues are of concerns to the state sovereignty, peace and stability or national security; (iv) when carrying out activities set out in

		disclosing the information to persons permitted in accordance with the Law	sub-section (iii), either the Central Committee, a relevant department, or organization assigned by the Central Committee having a separate authority and working on it in accordance with such standards.
7	The Telecommunications Law (2013)		40. In implementing the provisions contained in this Law: (a) the Department may: (i) examine any necessary person and require to furnish any necessary information, data, papers and documents; (ii) enter and inspect the buildings and places, and equipment where any Telecommunications Service is provided; (iii) examine, take extract and copy the accounts, papers and documents in respect of the telecommunications service; (iv) determine the procedures to be complied with by the Service Licensee in respect of filing and maintaining the accounts and documents relating to the business. (b) the inspection team formed under sub-section (c) of section 39 may exercise the powers contained in clauses (i), (ii) and (iii) of sub-section (a) according to the duties delegated by the Department.
8	The Law Protecting the Privacy and Security of Citizens (2017)		
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		
10	The Financial Institutions Law (2016)		Consumer Protection 71. (a) It shall be the responsibility and duty of the Central Bank to promote consumer protection

			and financial capability of the bank consumers and financial consumers generally. (b) For the purposes of carrying out the responsibility and duty under sub-section (a), the Central Bank shall be empowered to- (1) plan, formulate an implement a strategy for financial consumer protection in Myanmar; (2) co-ordinate consumer protection measures carried out by other financial sector regulators; (3) receive all necessary information from other financial sector regulators and financial institutions; (4) issue directions to the general financial sector in areas that are not supervised by the other financial sector regulators and where there are gaps; (5) promote an out of court dispute resolution system to deal with disputes between financial institution and its customers; (6) promote and consolidate consumer research and data collection; (7) create an effective financial literacy network of stakeholders; (8) keep the Government and public informed of the activities and issues in the area of financial consumer protection.
			Exceptions to Duty of Secrecy 82. (a) The provisions of section 81 shall not apply to the disclosure of customer information- (1) to the Central Bank, or to any director, officer or employee of the Central Bank, or to any person appointed by the Central Bank under this Law, where the 30 disclosure is for the purpose of the exercise of powers and duties of the Central Bank;

			(2) to any person rendering professional services to the Central Bank where the person is authorized in writing by the Central Bank to obtain the information from the bank; (3) which the customer, or his personal representative, has given permission in writing to disclose; (4) in a case where the customer is declared bankrupt, or, if the customer is a company, the company is being or has been wound up, in Myanmar or outside Myanmar; (5) where the information is required by a party to a bona fide commercial transaction, to assess the creditworthiness of the customer relating to such transaction; (6) where the information is required for the purposes of any criminal proceedings or in respect of any civil proceedings between a bank and its customer or his guarantor relating the customer's transaction; or between the bank and two or more parties making adverse claims to money in a customer's account; (7) in accordance with the order of a court of law; (8) where the disclosure is solely in connection with the conduct of internal audit of the bank or the performance of risk management; (9) to credit bureaus licensed by the Central Bank; (10) where disclosure is solely in connection with the performance of operational functions of the bank, where such operational functions have been outsourced; (11) where disclosure is in relation to the merger or proposed merger of the bank with another financial

			institutions; (12) where the disclosure is solely in connection with the transfer or proposed transfer of the business of the bank to another bank; (13) where the disclosure is solely in connection with the restructure, transfer or sale of a bank under Chapters XIV and XV; and (14) where such disclosure is made under the Anti-money Laundering Law and Counter Terrorism Law. (b) In any civil proceedings under sub-section (a) (6) and (7) where any information or document is likely to be disclosed in relation to a customer's account, such proceedings may, if the court, of its own motion, or on the application of a party to the proceedings, so orders, be held in camera and in such case, the information or document shall be secret as between the court and the parties thereto, and no such party shall disclose such information or document to any other person. (c) Unless the court otherwise orders, no person shall publish the name, address or photograph of any parties to such civil proceedings as are referred to in sub-section (b), or any information likely to lead to the identification of the parties thereto, either during the currency of the proceedings or at any time after they have been concluded.
			Right of Central Bank to obtain Information 144. The Central Bank may obtain necessary information from a credit bureau.
11	Notification 116/97 of the		

	Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		
13	(Draft) Bill - Cyber Security Law and privacy and data protection	37. A digital platform service provider in Myanmar shall retain the following information from the service users for up to three years from the rst date of use of the service; (a) Username, Internet Protocol (IP) address, telephone number, identi cation card number and address of the service users. (b) User record of the service user. (c) Other information as directed by the Department.	13. Personal Information Management shall not include the followings: (a) prevention, search and enquiry, investigation, submission of evidence in a court by the government agency, investigation team or rule of law team assigned by the government for cyber security, cyber-attacks, cyber terrorism, cyber misuse and cyber accident, cyber-crimes (b) search and enquiry, investigation, data collection, prosecution and submission of evidence in a court by the government agency, investigation team or rule of law team mandated to work on criminal issues (c) enquiry, investigation, data collection and info-sharing and coordination carried out if the cyber security and cyber-crimes issues are of concern to the state sovereignty, stability, national security (d) when carrying out activities in subsection (c), either the central committee or relevant ministry or department has separate authority and working on it in accordance with those de nitions.
		38. A digital platform service provider in Myanmar may provide all or part of the information contained in Article37 if the assigned person or authorised organisationis requested under any existing law.	52. Performing the provisions of Articles 49,50 and 51 with the permission of any existing law shall not be deemed to be illegal.

14	E-Commerce Guidelines (September 2023)		

Penalties

#	Regulation	Corporate Punishments	Individual Punishments
		Forms of penalties (e.g., recommendations for corrective action, public penalties, fines, confiscation of assets and income, data deletion, data processing, business suspension, etc.)	Penalties (penalties, fines, demotion, etc.)
		Forms of penalties on corporate	Forms of penalties on individual
1	The Constitution		
2	The Competition Law (2015)		41. Any person who violates the prohibitions contained in section 15, section 19, section 22, section 26, section 27, section 31 or section 32 shall, on conviction, be punished with imprisonment for a term not exceeding two years or with fine not exceeding Kyat one hundred lakhs or with both.
3	Competition Rules (2017)		
4	The Electronic Transactions Law (2004)		
5	The Electronic Transactions Law (2014)		33. Whoever commits any of the following acts by using electronic transactions technology shall, on conviction be punished with imprisonment for a term which may extend from a minimum of 5 years to a maximum of 7 years and may also be liable to a fine: (a) doing any act detrimental to the security of the State or prevalence of law and order or community peace and tranquillity or national solidarity or national economy or national culture. (b) receiving or sending and distributing any information relating to secrets of the security of the State or prevalence of law and order or community peace

			and tranquillity or national solidarity or national economy or national culture.
			34. Whoever commits any of the following acts shall, on conviction be punished with fine, or both, with a fine from 5,000,000 Kyats to 10,000,000 Kyats. If they cannot pay the fine, they shall be punished with imprisonment for a minimum term of 1 year to a maximum of 3 years: (a) sending, hacking, modifying, altering, destroying, stealing, or causing loss and damage to the electronic record, electronic data message, or the whole or part of the computer programme dishonestly; (b) intercepting of any communication within the computer network, using or giving access to any person of any fact in any communication without permission of the originator and the addressee; (c) communicating to any other person directly or indirectly with a security number, password or electronic signature of any person without permission or consent of such person; (d) creating, modifying or altering of information or distributing of information created, modified or altered by electronic technology to be detrimental to the interest of or to lower the dignity of any organization or any person.
6	The Electronic Transactions Law (2021)		38. Whoever attempts to commit any offence of this Law or conspires amounting to an offence or abets the commission of an offence shall be punished with the punishment provided for such offence in this Law. (a) If a person responsible to manage personal data is convicted of failing to manage Personal Data in accordance with the provisions under this

			law, he or she shall be punished with an imprisonment for a minimum term of one year to a maximum term up to three years, or with a fine not exceeding 10,000,000 Kyats, or with both. (b) Whoever is convicted of obtaining, disclosing, utilising, destroying, altering, disseminating or sending Personal Data to a third party without the approval shall be punished with an imprisonment for a minimum term of one year to a maximum term up to three years, or with a fine not exceeding 5,000,000 Kyats, or with both. (c) Whoever is convicted of creating misinformation or disinformation with the intent of causing public panic, distrust or social division on a Cyberspace shall be punished with an imprisonment for a minimum term of one year to a maximum term up to three years, or with a fine not exceeding 5,000,000 Kyats, or with both. (d) Whoever commits an act of Cyber Attack such as preventing access to cyber source or making it difficult, attempting to hack into a Cyber Source without permission, using more than permitted, and inserting or installing dangerous malware with the intention of hurting someone for the purposes of threatening or disturbing national sovereignty, security, peace and stability, rule of law and national solidarity shall be punished with an imprisonment for a minimum term of two years to a maximum term up to five years, or with a fine not exceeding 30,000,000 Kyats, or with both. (e) Whoever commits an act of Cyber Attack such as attempts of

			unauthorized access to and hacking cyber sources which are kept confidential for multilaterally implemented security reasons or using more than permitted, with the intent of deteriorating the relationship between the Union and other countries or for the interests of other foreign country, shall be punished with an imprisonment for a minimum term of three years to a maximum term up to seven years, or with a fine not exceeding 50,000,000 Kyats, or with both.
7	The Telecommunications Law (2013)		68. Whoever commits any of the following acts shall, on conviction, be punished with imprisonment for a term not exceeding one year or with fine or with both: (a) communications, reception, transmission, distribution or conveyance of incorrect information with dishonest or participation; (b) prohibiting, obstructing or interfering the transmission, reception, communication, conveyance or distribution of information without permission; (c) unauthorized access into the place restricted with the approval of the Department where of Telecommunications Services are operated; (d) prohibiting, obstructing or disturbing any person who has been assigned duty on any Telecommunications Service by a licensee from serving his duty.
			69. Whoever, unless for the matters concerning prosecution regarding telecommunications, and unless authorized under court order to disclose, discloses any information which is kept

			under a secured or encrypted system to any unauthorized person by any means shall, on conviction, be punished with imprisonment for a term not exceeding one year or with fine or with both.
8	The Law Protecting the Privacy and Security of Citizens (2017)		10. Whoever violates any prohibition in section 7 or section 8 shall, on conviction, be punished with imprisonment for a term which may extend from a minimum of six months to a maximum of three years and also with a fine from a minimum of three hundred thousand kyats to a maximum of one million and five hundred thousand kyats. 11. Whoever fails to perform the duty in section 9 without any reason shall, on conviction, be punished with imprisonment for a term which may extend from a minimum of one year to a maximum of five years and also with a fine which may extend from a minimum of five hundred thousand kyats to a maximum of two million and five hundred thousand kyats. 12. Whoever attempts, assigns, instructs to commit any offence in this Law, conspires and abets in the commission of any offence shall be liable to the punishment as provided in this Law for such offence.
9	Amendment of Law Protecting the Privacy and Security of the Citizens (2021)		Amend Section10 from Whoever to Any Responsible Authority 10. Any Responsible Authority who is found guilty of committing an offence under Section 7 or Section 8, shall, in addition to a sentence for a period of at least six months, and up to three years, also be required to pay a fine of between three hundred thousand (300,000) and fifteen

			hundred thousand (1,500,000) kyats.
10	The Financial Institutions Law (2016)		
11	Notification 116/97 of the Ministry of Finance and Revenue (Insurance Business Rules)		
12	Law Relating to Private Health Care Services (2007)		26. If the private health care services licence holder fails to comply with any duty contained in section 19 or has been convicted for committing any offence contained in this Law or if the person-in-charge fails to comply with the duties and obligations contained in section 25, the Central Body and the State and Divisional Supervisory Committees authorized to issue licence for relevant private health care service, may pass any of the following administrative orders on the relevant licence, holder: (a) warning; (b) imposing the stipulated fine; (c) suspension of the licence for a limited period; (d) cancellation of the licence. 27. The Central Body or the State and Divisional Supervisory Committee that takes action under section 26, shall inform the relevant Myanmar Medical Council, Dental or Oral Medical Council or Nursing and Midwifery Council to take necessary action if the health care service provider fails to comply with any of the duties and obligations contained in section 25.

13	(Draft) Bill - Cyber Security Law and privacy and data protection		47. Any of the following acts performed on a particular cyber source by anyone without the owners' permission shall be deemed unauthorised access to information; (a) Changing, modifying, or deleting a computer program or a program or data or information and its related status or properties, (b) Copying, transferring, or relocating a cyber source to one of the followings, (1) transferring a computer program or a program or data or information from its original place of storage to either another cyber source, or a device, or a storage device; (2) transferring a computer program or a program or data or information within the same cyber source or a device or a storage device but to a di erent location in its system; (3) Using a computer program or a program or data or information; (4) Obtaining data from a computer system by running a computer system, or by any other means.
			48. If any of the following acts relating to a computer system or computer program or a program or a data is performed without permission, it shall be deemed as an illegal modi cation of a quality of a particular computer system — (a) Changing any program or data stored by a respective computer system; (b) Deleting any program or data stored by a respective computer system, (c) Putting additional information to a program or data stored by a respective (d) Any action that can interrupt

			the regular functions of a computer system.
			50. A computer system or a program or data or information shall be deemed as illegal access to a computer system by a person by any means; (a) If that person is not the authorised one to oversee the Mitigated context which shall be assessed relevant with any computer system; (b) If that person is not the one who does not have permission from the responsible person to oversee the litigated context which shall be assessed relevant with any computer system;
			51. Intervention made to a computer system or computer program or a program or a data by a person with any of the following methods shall be deemed an illegal intervention. (a) If the person is not the authorised person for a speci c computer system; (b) If the person is not the authorised one to decide whether to make the aforementioned intervention or not; (c) If the person is not the one who has permission from a responsible person to make interventions for a speci c computer system.
			71. The operator of the digital platform serviceis subject to Article 35; In case of failure to comply with the provisions of Articles 36 and 54, the Department may, with the approval of the Steering Committee, impose any administrative action as follows: (a) Warning (b) imposing a ne (c) Suspension of service in Myanmar for a limited period or suspension of the license for a

			limited period. (d) Prohibition or revocation of license in Myanmar
			72. If the cyber security service provider fails to comply with the provisions ofArticles34 and 54,the Department may, with the approval of the Steering Committee, impose any administrative action as follows: (a) Warning (b) imposing a ne (c) Suspension of service in Myanmar for a limited period or suspension of the license for a limited period. (d) Prohibition or revocation of license in Myanmar
			79. If a person responsible to manage personal data is convicted of failure to manage personal data in with Articles11 and 12, he or she shall be punishableby imprisonment for a term not exceeding 3 years or a ne not exceeding 100 lakhs kyats or both.
			80. Any person, if convicted personal data of a person to another without approval, shall be punishable by imprisonment for a term not exceeding 3 years or a ne not exceeding 50 lakhs kyats or both.
			81. If a person responsible to manage critical information infrastructure is convicted of failure to perform his or her duties underArticle10 subheading (b), he or she shall be punishable by imprisonment for a term not exceeding 3 years or a ne not exceeding 100 lakhs kyats or both.
			82. Any person who is convicted of interfering, destroying, stealing, harming, illegally sending, modifying or changing electronic information, shall be punishable by imprisonment for a term not exceeding 3 years or a ne not exceeding 100 lakhs kyats or both.

			83. Any person who is convicted of interrupting a communication within a network or using data contained in a communication or disclosing data to another person, without the approvals from the original sender and Addressee, shall be punishable by imprisonment for a term not exceeding 3 years or a ne not exceeding 100 lakhs kyats or both.
			84. If a person is convicted of using a password or electronic signature of someone, without consent or agreement, directly or indirectly to communicate with another person, the person shall be punished with imprisonment for a minimum of one year and a maximum of three years or a ne not exceeding 100 lakhs kyats or both.
			87. Whoever is convicted of violating the provisionsofArticles47 and 48 shall be punished with imprisonment for a minimum of six months and a maximum of two years or a ne not exceeding 100 lakhs or both.
			88. Whoever violatesArticles49, 50 and 51, shall be punished with imprisonment for a minimum of one year and a maximum of three years or a ne not exceeding one hundred thousand kyats or both.
			91. Any person who is convicted of creating misinformation and disinformation with the intent of causing public panic, loss of trust or social division on cyberspace, shall be punished by imprisonment for a minimum of one year and a maximum of three years or with a ne not exceeding 50 lakhs kyats or both.
			93. Any person who commits acts of cyber-attack such as attempts of unauthorised access

			to and hacking cyber sources which are kept con dential for nationally, internationally or multilaterally implemented security reasons; and using more than permitted; with the intent of deteriorating the relationship between the country and other foreign countries or for the interests of another foreign country, shall be punished with imprisonment for a minimum of three years and a maximum of seven years or with a ne not exceeding 500 lakhs kyats or both.
			96. Any person who is convicted of electronically sharing sexually explicit speech, image, audio le, video, sentence, sign, symbol and other expressions shall be punished by imprisonment for a minimum of one year and a maximum of two years or with a ne not exceeding 50 lakhs kyats or both.
14	E-Commerce Guidelines (September 2023)		97. An e-commerce business operator failing to comply with the relevant legal provisions contained in the parts of these guidelines shall be taken action against in accordance with the laws in force.

G) Philippines

Legal system overview

#	Regulation	Translation	Purpose of the Legal System
			What purpose does the legal system serve? (e.g. cybersecurity)
		Google translation or Translation by certain organization	
1	Data Privacy Act of 2012		SEC. 2. Declaration of Policy. – It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital

			role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.
2	THE REVISED RULES OF CRIMINAL PROCEDURE		providing for the operation of criminal procedure.
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		Defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefor and for other purposes.
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		Defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefor and for other purposes.
5	Rule on Cybercrime Warrants		providing procedures facilitating their detection, investigation, and prosecution of cybercrime.
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		enforcing the Data Privacy Act and adopt generally accepted international principles and standards for personal data protection.

7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		providing guidance on PICs on the nature of deceptive design patterns, and its impact on the lawful processing of personal data based on the data subject's consent and in line with the general privacy principles.
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		providing a set of guidelines on evaluating requests for personal data about public officers, including personal data about an individual who is or was performing service under contract for the government that relates to the services performed.
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		providing a set of guidelines on political parties, candidates, aspirants, party-list groups or organizations and their nominees, and information society service providers on the matter of processing personal and sensitive personal information (collectively, personal data) for election campaigns or partisan political activities.
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		providing additional guidance to supplement the ASEAN Model Contractual Clauses and ASEAN Data Management Framework as to how PICs and PIPs in the Philippines may use these in their respective personal data processing.
11	NPC Advisory No. 2021-01: Data Subject Rights		providing a set of guidelines on data subject righits.
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		providing a set of guidelines on the use of CCTV systems.
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for		amending Section 4 (A) of NPC Advisory No. 2020 – 03 pertaining to the collection of information by workplaces and establishments as required for COVID-19 prevention and control

	Workplaces and Establishments Processing Personal Data for Covid-19 Response		based on existing government issuances.
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		providing additional guidance to supplement the Joint Memorandum Circular (JMC) No. 20-04-A Series of 20201 issued by the Department of Trade and Industry (DTI) and Department of Labor and Employment (DOLE) which requires workplaces and various establishments to collect employee health declaration forms and client/visitor contact tracing forms, and implement measures to manage asymptomatic and symptomatic employees in the workplace.
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		providing the parties the option to attend the proceedings remotely, in the relative safety of their chosen premises, in accordance with the Rules of Procedure, before the National Privacy Commission.
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		amending Section 1 (b) of Advisory 2020-01
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions,		issuing the policies and protocols for the promulgation and publication of Commission Decisions, Resolutions, and Orders posted in the NPC

	Resolutions and Orders on the NPC Website		website for the guidance of the public.
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		providing guidelines on Data Breach Notification Management System (DBNMS)
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		providing guidelines on Privacy Impact Assessments
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		providing guidelines on Personal Data Sheets of Government Personnel
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		providing guidelines on designation of Data Protection Officers
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		amending certain provisions of the 2021 rules of procedure of the NPC
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		providing guidelines for PICs and third parties relying on legitimate interest as a lawful basis to process personal information for a specific processing activity.

24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		providing updated requirements for the security of personal data processed by a PIC or Personal Information Processor (PIP).
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		providing the prerequisites for certification of PICs or PIPs and accreditation of CBs under the PPM Certification Program.
26	NPC Circular No. 2023-04 - Guidelines on Consent		providing guidance on what constitutes valid consent, and how it shall be obtained and managed in compliance with the DPA and its IRR.
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		providing guidelines for identification cards.
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		developing uniform curricula and modules on the legal framework of privacy law and regulations (Curriculum) and learning outcomes to train and capacitate the public.
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		providing guidelines for Schedule of Fees and Charges of the National Privacy Commission.
30	NPC Circular No. 2022-04 - Annex 1		providing the format of sworn declaration and undertaking for exemption from registration of data processing systems.
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING		providing guidelines for registration of personal data processing system, notification regarding automated decision-making or profiling, designation of data protection officer, and the national privacy commission seal of registration.

	AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		providing guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		expounding on NPC Circular No. 20-01 to respond to exigencies in the processing of personal data for loan-related transactions by lending and financing companies and other persons acting as such.
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		providing Guidelines on Administrative Fines
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		providing guidelines on the processing of personal data during public health emergencies for public health measures.

36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		providing rules on procedure of the National Privacy Commission
37	NPC Circular 2020-03 - Data Sharing Agreements		providing guidelines on the data sharing agreements.
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		providing rules on the Issuance of Cease and Desist Orders of the National Privacy Commission.
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		providing guidelines on the processing of Personal Data for Loan-Related Transactions
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		providing actionable information for accountability and performance improvement for telemedicine services, and creating evidence for informed decision-making for the DOH and NPC atpolicy level on the possible long-term use of telemedicine for service delivery.
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		providing guidelines for the collection, processing and disclosure of COVID-19-related data in pursuit of disease surveillance and response, while protecting the data privacy rights of patients and individuals and ensuring the confidentiality, integrity, and availability of their personal data.
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of		enabling patients to receive health services even while staying at home except for serious conditions, emergencies, or to avail of COVID-19-related

	Telemedicine in COVID-19 Response		health services as per standing protocols.
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		providing rules on Mediation before the National Privacy Commission
44	NPC Circular 18-02 - Guidelines on Compliance Checks		providing the guidelines for the conduct of Compliance Checks by personnel of the Commission, whichever mode it may be.
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		providing rules of procedure on requests for Advisory Opinions
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		providing Appendix of Registration of Data Processing Systems.
47	NPC Circular 17-01 - Registration of Data Processing Systems		establishing the framework for registration of data processing systems in the Philippines and imposing other requirements.
48	NPC Circular 16-04 - Rules of Procedure		providing rules of Procedure of NPC
49	NPC Circular 16-03 - Personal Data Breach Management		providing the framework for personal data breach management and the procedure for personal data breach notification and other requirements.
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		providing data sharing agreements involving government agencies
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		assisting government agencies engaged in the processing of personal data to meet their legal obligations under Republic Act No. 10173, also known as the Data Privacy Act of 2012, and its

			corresponding Implementing Rules and Regulations.

#	Regulation	Form of legal system	Target Business
		Is it introduced in accordance with government ordinances and guidelines? (Is it introduced in a format that ensures lead time?)	Does the law target specific industry or in general? Is it clearly stated in the regulations?
		Regulation level	Industry
1	Data Privacy Act of 2012	Law	General
2	THE REVISED RULES OF CRIMINAL PROCEDURE	Rule	General
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)	Law	General
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"	Rule	General

5	Rule on Cybercrime Warrants	Rule	General
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"	Rule	General
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns	Advisories	General
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers	Advisories	General
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity	Advisories	political parties, candidates, aspirants, party-list groups or organizations and their nominees, and information society service providers
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework	Advisories	General
11	NPC Advisory No. 2021-01: Data Subject Rights	Advisories	General
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-	Advisories	PICs and PIPs engaged in the processing of personal data through the use of CCTV systems

	circuit Television (CCTV) Systems		operating in public and semipublic areas
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response	Advisories	General
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response	Advisories	General
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission	Advisories	National Privacy Commission parties
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website	Advisories	National Privacy Commission
17	NPC Advisory No. 2020-01:	Advisories	National Privacy Commission

	Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)	Advisories	General
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments	Advisories	General
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel	Advisories	government agency and office
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers	Advisories	General
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC	Circulars	General
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ	Circulars	General

	Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector	Circulars	General
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program	Circulars	General
26	NPC Circular No. 2023-04 - Guidelines on Consent	Circulars	General
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards	Circulars	PICs that issue ID cards to their respective data subjects
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program	Circulars	Qualified and licensed Training Providers
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission	Circulars	General
30	NPC Circular No. 2022-04 - Annex 1	Circulars	General
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION	Circulars	General

	REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information	Circulars	Private Security Agencies
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions	Circulars	loan-related transactions by lending financing companies
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines	Circulars	General
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For	Circulars	General

	Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission	Circulars	National Privacy Commission
37	NPC Circular 2020-03 - Data Sharing Agreements	Circulars	General
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs	Circulars	General
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions	Circulars	lending or financing companies
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response	Circulars	public and private, national and local healthcare providers regulated by DOH and Philippine Health Insurance Corporation (PhilHealth) providing telemedicine services
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response	Circulars	public and private, national and local healthcare providers regulated by DOH and Philippine Health Insurance Corporation
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 -	Circulars	public and private, national and local healthcare providers regulated by DOH and Philippine Health Insurance Corporation

	Guidelines on the Use of Telemedicine in COVID-19 Response		(PhilHealth); and telemedicine providers
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission	Circulars	National Privacy Commission
44	NPC Circular 18-02 - Guidelines on Compliance Checks	Circulars	General
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions	Circulars	General
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1	Circulars	General
47	NPC Circular 17-01 - Registration of Data Processing Systems	Circulars	General
48	NPC Circular 16-04 - Rules of Procedure	Circulars	General
49	NPC Circular 16-03 - Personal Data Breach Management	Circulars	General
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies	Circulars	government agency
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies	Circulars	government agency

#	Regulation	Regulatory authority	Jurisdiction
		Which regulatory authority has jurisdiction over regulation?	Cyber security, data security, personal information protection, etc.
		Name of ministry/organization	Similar to purpose?
1	Data Privacy Act of 2012	National Privacy Commission	privacy protection
2	THE REVISED RULES OF CRIMINAL PROCEDURE	Department of Justice	criminal procedure
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)	Department of Justice	cybersecurity
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"	Department of Justice	cybersecurity
5	Rule on Cybercrime Warrants	Department of Justice	cybersecurity
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"	National Privacy Commission	privacy protection
7	NPC Advisory No. 2023-01: Guidelines on	National Privacy Commission	privacy protection

	Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers	National Privacy Commission	privacy protection
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity	National Privacy Commission	privacy protection
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework	National Privacy Commission	privacy protection
11	NPC Advisory No. 2021-01: Data Subject Rights	National Privacy Commission	privacy protection
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems	National Privacy Commission	privacy protection
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response	National Privacy Commission	privacy protection
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments	National Privacy Commission	privacy protection

	Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission	National Privacy Commission	privacy protection
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website	National Privacy Commission	privacy protection
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website	National Privacy Commission	privacy protection
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)	National Privacy Commission	privacy protection

19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments	National Privacy Commission	privacy protection
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel	National Privacy Commission	privacy protection
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers	National Privacy Commission	privacy protection
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC	National Privacy Commission	privacy protection
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest	National Privacy Commission	privacy protection
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector	National Privacy Commission	data security
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program	National Privacy Commission	privacy protection
26	NPC Circular No. 2023-04 -	National Privacy Commission	privacy protection

	Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards	National Privacy Commission	privacy protection
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program	National Privacy Commission	privacy protection
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission	National Privacy Commission	privacy protection
30	NPC Circular No. 2022-04 - Annex 1	National Privacy Commission	privacy protection
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION	National Privacy Commission	privacy protection
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the	National Privacy Commission	privacy protection

	Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions	National Privacy Commission	privacy protection
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines	National Privacy Commission	privacy protection
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures	National Privacy Commission	privacy protection
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission	National Privacy Commission	privacy protection
37	NPC Circular 2020-03 - Data Sharing Agreements	National Privacy Commission	privacy protection
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs	National Privacy Commission	privacy protection
39	NPC Circular 20-01 - Guidelines on the	National Privacy Commission	privacy protection

	Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response	Department of Health National Privacy Commission	privacy protection, public health
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response	Department of Health National Privacy Commission	privacy protection, public health
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response	Department of Health National Privacy Commission	privacy protection, public health
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission	National Privacy Commission	privacy protection
44	NPC Circular 18-02 - Guidelines on Compliance Checks	National Privacy Commission	privacy protection
45	NPC Circular 18-01 - Rules of procedure on requests for	National Privacy Commission	privacy protection

	Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1	National Privacy Commission	privacy protection
47	NPC Circular 17-01 - Registration of Data Processing Systems	National Privacy Commission	privacy protection
48	NPC Circular 16-04 - Rules of Procedure	National Privacy Commission	privacy protection
49	NPC Circular 16-03 - Personal Data Breach Management	National Privacy Commission	privacy protection
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies	National Privacy Commission	privacy protection
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies	National Privacy Commission	privacy protection

#	Regulation	Status	Citation
		Legislation / Public Comment / Passage / Enforcement / Amendment, etc.	
		Status of the regulation: Draft = drafting (new regulation) published = published in the gazzette but not yet enacted Enact = published in the gazzette and already enacted Amendment = enacted regulation being on amending process	URL

1	Data Privacy Act of 2012	Enforcement	https://privacy.gov.ph/data-privacy-act/
2	THE REVISED RULES OF CRIMINAL PROCEDURE	Enforcement	https://lawphil.net/courts/rules/rc_110-127_crim.html
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)	Enforcement	https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"	Enforcement	https://www.officialgazette.gov.ph/2015/08/12/implementing-rules-and-regulations-of-republic-act-no-10175/
5	Rule on Cybercrime Warrants	Enforcement	https://oca.judiciary.gov.ph/wp-content/uploads/2022/09/A.M.-No.-17-11-03-SC-dtd-07.03.18.pdf
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"	Enforcement	https://privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/

7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns	Enforcement	https://privacy.gov.ph/wp-content/uploads/2023/11/NPC-Advisory-No.-2023-01-Guidelines-on-Deceptive-Design-Patterns_7Nov23.pdf
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers	Enforcement	https://privacy.gov.ph/wp-content/uploads/2022/08/NPC-Advisory-No.-2022-01-Request-for-Personal-Data-of-Public-Officers.pdf
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity	Enforcement	https://privacy.gov.ph/wp-content/uploads/2021/11/Advisory_Election_Campaigning_03-Nov-21-FINAL.pdf
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework	Enforcement	https://privacy.gov.ph/wp-content/uploads/2021/06/Advisory-ASEAN-MCC-DMF_FINAL-signed.pdf
11	NPC Advisory No. 2021-01: Data Subject Rights	Enforcement	https://privacy.gov.ph/wp-content/uploads/2021/02/NPC-Advisory-2021-01-FINAL.pdf
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems	Enforcement	https://privacy.gov.ph/wp-content/uploads/2020/11/Advisory-on-CCTV-16NOV2020-FINAL.pdf
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response	Enforcement	https://privacy.gov.ph/wp-content/uploads/2020/11/Advisory-2020-03-A-FINAL.pdf

14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response	Enforcement	https://privacy.gov.ph/wp-content/uploads/2020/11/NPC-Advisory-No.-2020-03-FINAL.pdf
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission	Enforcement	https://privacy.gov.ph/wp-content/uploads/2020/10/FINAL-VERSION-Guidelines-on-the-Use-of-Videoconferencing-Technology-for-Remote-Appearance-before-the-NPC-OPC.pdf
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website	Enforcement	https://privacy.gov.ph/wp-content/uploads/2020/11/Amendment-to-Advisory-2020-01-Final.pdf
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website	Enforcement	https://privacy.gov.ph/wp-content/uploads/2020/11/NPC-Advisory-2020-01-FINAL.pdf
8	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications	Enforcement	https://privacy.gov.ph/announcement-regarding-the-submission-of-personal-data-breach-notifications-pdbn-and-annual-security-incident-reports-asir-2/

	(PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments	Enforcement	https://privacy.gov.ph/wp-content/uploads/2022/01/NPC_AdvisoryNo.2017-03.pdf
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel	Enforcement	https://privacy.gov.ph/wp-content/uploads/2022/01/NPC_Advisory_No.2017-02.pdf
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers	Enforcement	https://privacy.gov.ph/wp-content/uploads/2022/01/NPC-Advisory-2017-01-sgd.pdf
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC	Enforcement	https://privacy.gov.ph/wp-content/uploads/2024/01/NPC-Circular-2024-01-Amendments-to-the-2021-Rules-of-Procedure-of-the-NPC-FOR-PUBLICATION.pdf
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest	Enforcement	https://privacy.gov.ph/wp-content/uploads/2024/01/NPC-Circular-No.-2023-07_Guidelines-on-Legitimate-Interest_13-December-2023.pdf
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector	Enforcement	https://privacy.gov.ph/wp-content/uploads/2024/03/NPC-Circular-Repeal-16-01-Signed.pdf
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark	Enforcement	https://privacy.gov.ph/wp-content/uploads/2024/03/Prerequisites-for-the-Philippine-Privacy-Mark-Signed.pdf

	Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent	Enforcement	https://privacy.gov.ph/wp-content/uploads/2023/11/NPC-Circular-No.-2023-04_Guidelines-on-Consent_07Nov2023.pdf
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards	Enforcement	https://privacy.gov.ph/wp-content/uploads/2023/11/Published-NPC-Circular-No.-2023-03_Guidelines-on-Identification-Cards_07Nov2023.pdf
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program	Enforcement	https://privacy.gov.ph/wp-content/uploads/2023/11/Circular-on-Data-Privacy-Competency-Program-2023.09.26.pdf
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission	Enforcement	https://privacy.gov.ph/wp-content/uploads/2023/05/Schedule-of-Fees-and-Charges-of-the-National-Privacy-Commission.pdf
30	NPC Circular No. 2022-04 - Annex 1	Enforcement	https://privacy.gov.ph/wp-content/uploads/2023/05/Circular-2022-04-Annex-1-1.pdf
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION	Enforcement	https://privacy.gov.ph/wp-content/uploads/2023/05/Circular-2022-04-2.pdf

32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information	Enforcement	https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-Circular-No.-2022-%E2%80%93-03-Private-Security-Agencies.pdf
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions	Enforcement	https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-Circular-No.-2022-%E2%80%93-02-Amending-20-01-Loan-Related-Transactions.pdf
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines	Enforcement	https://privacy.gov.ph/wp-content/uploads/2022/08/NPC-CIRCULAR-NO.-2022-01-GUIDELINES-ON-ADMINISTRATIVE-FINES-dated-08-AUGUST-2022-w-SGD.pdf
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures	Enforcement	https://privacy.gov.ph/wp-content/uploads/2021/11/Circular-on-Processing-for-Public-Health-Emergencies-FINAL.pdf
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission	Enforcement	https://privacy.gov.ph/wp-content/uploads/2021/01/2021RULESOFPROCEDURE_VER8-Final-Sgd-1-1-1.pdf
37	NPC Circular 2020-03 - Data Sharing Agreements	Enforcement	https://privacy.gov.ph/wp-content/uploads/2021/01/Circular-Data-Sharing-Agreement-amending-16-02-21-Dec-2020-clean-copy-FINAL-LYA-and-JDN-signed-minor-edit.pdf

38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs	Enforcement	https://privacy.gov.ph/wp-content/uploads/2020/10/NPC-Circular-20-02_Circular-Rules-on-CDO.pdf
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions	Enforcement	https://privacy.gov.ph/wp-content/uploads/2020/10/NPC-Circular-No.-20-01.pdf
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response	Enforcement	https://privacy.gov.ph/wp-content/uploads/2021/11/MC2020-0024-1.pdf
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response	Enforcement	https://privacy.gov.ph/wp-content/uploads/2020/10/jmc2020-0002v1.pdf
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response	Enforcement	https://privacy.gov.ph/wp-content/uploads/2020/10/DOH-mc2020-0016.pdf
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission	Enforcement	https://privacy.gov.ph/wp-content/uploads/2022/01/Circular18-03_RulesonMediationwAnnexes.pdf

44	NPC Circular 18-02 - Guidelines on Compliance Checks	Enforcement	https://privacy.gov.ph/wp-content/uploads/2022/01/Circular18-02_ComplianceCheck.pdf
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions	Enforcement	https://privacy.gov.ph/wp-content/uploads/2022/01/Circular18-01_Request_forAdvisory_Opinion.pdf
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1	Enforcement	https://privacy.gov.ph/wp-content/uploads/2022/01/NPC17-01_Appendix-1.pdf
47	NPC Circular 17-01 - Registration of Data Processing Systems	Enforcement	https://privacy.gov.ph/wp-content/uploads/2022/01/NPC_Circular-17-01-Registration_final.pdf
48	NPC Circular 16-04 - Rules of Procedure	Enforcement	https://privacy.gov.ph/wp-content/uploads/2022/01/sgd-npc-circular-16-04-rules-of-procedure.pdf
49	NPC Circular 16-03 - Personal Data Breach Management	Enforcement	https://privacy.gov.ph/wp-content/uploads/2022/01/sgd-npc-circular-16-03-personal-data-breach-management.pdf
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies	Enforcement	https://privacy.gov.ph/wp-content/uploads/2022/01/Sgd-NPC-Circular-16-02-Data-Sharing-Agreements-Involving-Government-Agencies.pdf
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies	Enforcement	https://privacy.gov.ph/wp-content/uploads/2022/01/Sgd-NPC-Circular-16-01-Security-of-Personal-Data-in-Government-Agencies.pdf

Definitions for basic items

#	Regulation	Type and Scope of Data	Data processing and handling
		Personal data, personal information/sensitive and important data/children and minors' data, etc. Is the scope of data clearly written in the regulations? What are the unclear points?	Processing, handling / disclosure, sharing, provision, transmission, outsourcing / use for advertising, etc.

		Specific type of data required to complied with the regulation	Provision for data processing
1	Data Privacy Act of 2012	(g) Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual. (k) Privileged information refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication. (l) Sensitive personal information refers to personal information: (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (4) Specifically established by an executive order or an act of Congress to be kept classified.	(d) Direct marketing refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals. (j) Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.
2	THE REVISED RULES OF CRIMINAL PROCEDURE		

3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On		

	The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote		

	Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		

21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency		

	Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the		

	Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E)		

	of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data		

	Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation	Data handlers
		Classification/ distinction by responsibility (data processor, data controller)/ size of data, (national security) critical services, etc.
		Provision on type of data handler
1	Data Privacy Act of 2012	(h) Personal information controller refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes: (1) A person or organization who performs such functions as instructed by another person or organization; and (2) An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs. (i) Personal information processor refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.
2	THE REVISED RULES OF CRIMINAL PROCEDURE	
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION,	

	INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)	
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"	
5	Rule on Cybercrime Warrants	
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"	
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns	
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers	
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity	

10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework	
11	NPC Advisory No. 2021-01: Data Subject Rights	
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems	
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response	
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response	
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission	

16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website	
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website	
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)	
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments	
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel	
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers	
22	NPC Circular No. 2024-01 -	

	Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC	
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest	
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector	
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program	
26	NPC Circular No. 2023-04 - Guidelines on Consent	
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards	
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program	
29	NPC Circular No. 2023-01 - Schedule of Fees	

	and Charges of the National Privacy Commission	
30	NPC Circular No. 2022-04 - Annex 1	
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION	
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information	
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions	
34	NPC Circular No. 2022-01 -	

	GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines	
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures	
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission	
37	NPC Circular 2020-03 - Data Sharing Agreements	
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs	
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions	
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response	
41	DOH-NPC Joint Memorandum Circular No.	

	2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response	
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response	
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission	
44	NPC Circular 18-02 - Guidelines on Compliance Checks	
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions	
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1	
47	NPC Circular 17-01 - Registration of Data Processing Systems	
48	NPC Circular 16-04 - Rules of Procedure	
49	NPC Circular 16-03 - Personal	

	Data Breach Management	
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies	
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies	

Legal basis

#	Regulation		
		consent	necessary for the performance of a contract
1	Data Privacy Act of 2012	SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: (a) The data subject has given his or her consent; SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: (a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;	SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: (b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING		

	CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data		

	For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of		

	Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of		

	Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy		

	Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of		

	Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in		

	COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		

48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation		
		necessary for compliance with a legal obligation	necessary in order to protect the vital interests
1	Data Privacy Act of 2012	SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject; SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: (b) The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the	SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: (d) The processing is necessary to protect vitally important interests of the data subject, including life and health; SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: (c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

		consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information; (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.	
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC		

	ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing		

	Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of		

	Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 -		

	Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION		

	SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		

38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		

44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation		
		necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	necessary for the purposes of the legitimate interests pursued by the controller or by a third party

1	Data Privacy Act of 2012	SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: (d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing; (e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or	SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.
2	THE REVISED RULES OF		

	CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		

9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of		

	Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of		

	Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data		

	Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of		

	NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the		

	Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration		

	of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation		
		opt-out	others
1	Data Privacy Act of 2012		
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing		

	Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04:		

	Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		

17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on		

	Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING		

	SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health		

	Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No.		

	2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

Rights of the data subject

#	Regulation	Right to be informed	Right of access
1	Data Privacy Act of 2012	SEC. 16. Rights of the Data Subject. – The data subject is entitled to: (a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed; (b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: (1) Description of the personal information to be entered into the system; (2) Purposes for which they are being or are to be processed; (3) Scope and method of the personal information processing; (4) The recipients or classes of recipients to whom they are or may be disclosed; (5) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; (6) The identity and contact details of the personal information controller or its representative; (7) The period for which the information will be stored; and (8) The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission. Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification of data subject: Provided, That the notification under subsection (b) shall not	(c) Reasonable access to, upon demand, the following: (1) Contents of his or her personal information that were processed; (2) Sources from which personal information were obtained; (3) Names and addresses of recipients of the personal information; (4) Manner by which such data were processed; (5) Reasons for the disclosure of the personal information to recipients; (6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject; (7) Date when his or her personal information concerning the data subject were last accessed and modified; and (8) The designation, or name or identity and address of the personal information controller;

		apply should the personal information be needed pursuant to a subpoena or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of legal obligation;	
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC		

	ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing		

	Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of		

	Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 -		

	Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION		

	SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		

38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		

44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation	Right to rectification	Right to erasure
1	Data Privacy Act of 2012	(d) Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been	(e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are

		corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: Provided, That the third parties who have previously received such processed personal information shall he informed of its inaccuracy and its rectification upon reasonable request of the data subject;	incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC		

	ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing		

	Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of		

	Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 -		

	Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION		

	SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		

38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		

44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation	Right to restrict processing	Right to data portability
1	Data Privacy Act of 2012		SEC. 18. Right to Data Portability. – The data subject shall have the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a

			copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities and procedures for their transfer. SEC. 19. Non-Applicability. – The immediately preceding sections are not applicable if the processed personal information are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject: Provided, That the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, the immediately preceding sections are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject.
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		

4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		

11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of		

	Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of		

	Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		

31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		

35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19		

	Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving		

	Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation	Right to object	Right not to be subject to a decision based solely on automated processing
1	Data Privacy Act of 2012	(e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and	
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES		

	THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model		

	Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of		

	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the		

	National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		

30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on		

	Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and		

	Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing		

	Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation		
		Right to withdraw consent	others
1	Data Privacy Act of 2012	(e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and	(f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information. SEC. 17. Transmissibility of Rights of the Data Subject. – The lawful heirs and assigns of the data subject may invoke the rights of the data subject for, which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES		

	(Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data		

	Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01:		

	Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission -		

	2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		

31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		

35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19		

	Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving		

	Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

Extraterritorial application

#	Regulation	applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction	applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction
1	Data Privacy Act of 2012		
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		

6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the		

	Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-		

	02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government		

	and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION		

	OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		

37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before		

	the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation		
		no express territorial scope, but would require some nexus to the jurisdiction	other
1	Data Privacy Act of 2012	SEC. 6. Extraterritorial Application. – This Act applies to an act done or practice engaged	

		in and outside of the Philippines by an entity if: (a) The act, practice or processing relates to personal information about a Philippine citizen or a resident; (b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following: (1) A contract is entered in the Philippines; (2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and (3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and (c) The entity has other links in the Philippines such as, but not limited to: (1) The entity carries on business in the Philippines; and (2) The personal information was collected or held by an entity in the Philippines.	
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER		

	PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data		

	Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
17	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01:		

	Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
19	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
20	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
21	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
22	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
23	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission -		

	2021 Rules of Procedure of the NPC		
24	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
25	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
26	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
27	NPC Circular No. 2023-04 - Guidelines on Consent		
28	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
29	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
30	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
31	NPC Circular No. 2022-04 - Annex 1		

32	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
33	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
34	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
35	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		

36	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
37	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
38	NPC Circular 2020-03 - Data Sharing Agreements		
39	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
40	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
41	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19		

	Related Data for Disease Surveillance and Response		
43	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
44	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
45	NPC Circular 18-02 - Guidelines on Compliance Checks		
46	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
47	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
48	NPC Circular 17-01 - Registration of Data Processing Systems		
49	NPC Circular 16-04 - Rules of Procedure		
50	NPC Circular 16-03 - Personal Data Breach Management		
51	NPC Circular 16-02 - Data Sharing Agreements Involving		

	Government Agencies		
52	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation	
		Representatives of controllers or processors not established in the country
1	Data Privacy Act of 2012	
2	THE REVISED RULES OF CRIMINAL PROCEDURE	
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)	
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"	
5	Rule on Cybercrime Warrants	
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173,	

	ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"	
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns	
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers	
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity	
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework	
11	NPC Advisory No. 2021-01: Data Subject Rights	
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems	
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for	

	Covid-19 Response	
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response	
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission	
17	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website	
18	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website	
19	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data	

	Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)	
20	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments	
21	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel	
22	NPC Advisory No. 2017-01: Designation of Data Protection Officers	
23	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC	
24	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest	
25	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector	
26	NPC Circular No. 2023-05 - Prerequisites for	

	the Philippine Privacy Mark Certification Program	
27	NPC Circular No. 2023-04 - Guidelines on Consent	
28	NPC Circular No. 2023-03 - Guidelines on Identification Cards	
29	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program	
30	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission	
31	NPC Circular No. 2022-04 - Annex 1	
32	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION	

	SEAL OF REGISTRATION	
33	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information	
34	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions	
35	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines	
36	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures	
37	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission	
38	NPC Circular 2020-03 - Data Sharing Agreements	

39	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs	
40	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions	
41	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response	
42	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response	
43	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response	
44	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission	

45	NPC Circular 18-02 - Guidelines on Compliance Checks	
46	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions	
47	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1	
48	NPC Circular 17-01 - Registration of Data Processing Systems	
49	NPC Circular 16-04 - Rules of Procedure	
50	NPC Circular 16-03 - Personal Data Breach Management	
51	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies	
52	NPC Circular 16-01 - Security of Personal Data in Government Agencies	

Notification obligation

#	Regulation	Data breach notification to authorities	Data breach notification to affected individuals
1	Data Privacy Act of 2012	(f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the	(f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the

		circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (bat such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. (1) In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal information. (2) The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects. (3) The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.	circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (bat such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. (1) In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal information. (2) The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects. (3) The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.
2	THE REVISED RULES OF CRIMINAL PROCEDURE		

3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On		

	The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote		

	Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		

21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency		

	Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the		

	Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E)		

	of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data		

	Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

Obligations of Data Fiduciaries

#	Regulation	external	external
		Notification of data processing	registration of database
1	Data Privacy Act of 2012	SEC. 16. Rights of the Data Subject. – The data subject is entitled to: (b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: (1) Description of the personal information to be entered into the system; (2) Purposes for which they are being or are to be processed; (3) Scope and method of the personal information processing; (4) The recipients or classes of recipients to whom they are or may be disclosed; (5) Methods utilized for	

		automated access, if the same is allowed by the data subject, and the extent to which such access is authorized; (6) The identity and contact details of the personal information controller or its representative; (7) The period for which the information will be stored; and (8) The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission. Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification of data subject: Provided, That the notification under subsection (b) shall not apply should the personal information be needed pursuant to a subpoena or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of legal obligation; (e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no	

		longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and	
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01:		

	Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and		

	Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		

19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 -		

	Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the		

	Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the		

	Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for		

	Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation	external	external
		Data protection impact assessment	Others
1	Data Privacy Act of 2012		
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF		

	PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The		

	ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain		

	Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of		

	Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		

30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on		

	Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and		

	Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing		

	Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation	internal	internal
		technical and organisational measures	Purpose Limitation
1	Data Privacy Act of 2012	(f) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: Provided, That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: Provided, further, That adequate safeguards are guaranteed by said laws authorizing their processing. The personal information controller must ensure implementation of personal information processing principles set out herein. SEC. 14. Subcontract of Personal Information. – A personal information controller may subcontract the processing of personal information: Provided, That the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information processor	SEC. 11. General Data Privacy Principles. – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality. Personal information must, be:, (a) Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only; (b) Processed fairly and lawfully; (d) Adequate and not excessive in relation to the purposes for which they are collected and processed;

		shall comply with all the requirements of this Act and other applicable laws. SEC. 15. Extension of Privileged Communication. – Personal information controllers may invoke the principle of privileged communication over privileged information that they lawfully control or process. Subject to existing laws and regulations, any evidence gathered on privileged information is inadmissible. SEC. 20. Security of Personal Information. – (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing. (b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination. (c) The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation.	

		Subject to guidelines as the Commission may issue from time to time, the measures implemented must include: (1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability; (2) A security policy with respect to the processing of personal information; (3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and (4) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach. (d) The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision. (e) The employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to	

		another position or upon termination of employment or contractual relations. (f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (bat such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. (1) In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal information. (2) The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects.	

		(3) The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach. SEC. 21. Principle of Accountability. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. (a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party. (b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request. SEC. 22. Responsibility of Heads of Agencies. – All sensitive personal information maintained by the government, its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the Commission. The head of each government agency or instrumentality shall be	

		responsible for complying with the security requirements mentioned herein while the Commission shall monitor the compliance and may recommend the necessary action in order to satisfy the minimum standards. SEC. 23. Requirements Relating to Access by Agency Personnel to Sensitive Personal Information. – (a) On-site and Online Access – Except as may be allowed through guidelines to be issued by the Commission, no employee of the government shall have access to sensitive personal information on government property or through online facilities unless the employee has received a security clearance from the head of the source agency. (b) Off-site Access – Unless otherwise provided in guidelines to be issued by the Commission, sensitive personal information maintained by an agency may not be transported or accessed from a location off government property unless a request for such transportation or access is submitted and approved by the head of the agency in accordance with the following guidelines: (1) Deadline for Approval or Disapproval – In the case of any request submitted to the head of an agency, such head of the agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. In case there is no action by the head of the agency, then such request is considered disapproved;	

		(2) Limitation to One thousand (1,000) Records – If a request is approved, the head of the agency shall limit the access to not more than one thousand (1,000) records at a time; and (3) Encryption – Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be secured by the use of the most secure encryption standard recognized by the Commission. The requirements of this subsection shall be implemented not later than six (6) months after the date of the enactment of this Act. SEC. 24. Applicability to Government Contractors. – In entering into any contract that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals, an agency shall require a contractor and its employees to register their personal information processing system with the Commission in accordance with this Act and to comply with the other provisions of this Act including the immediately preceding section, in the same manner as agencies and government employees comply with such requirements.	
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION,		

	INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		

10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		

16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 -		

	Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees		

	and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 -		

	GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No.		

	2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal		

	Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation	internal	internal
		Accuracy	Retention Limitation
1	Data Privacy Act of 2012	(c) Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;	(e) Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise		

	Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-		

	circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the		

	Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on		

	Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING		

	AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		

36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of		

	Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation	internal	internal
		drawing up of codes of conduct	record of processing activities

1	Data Privacy Act of 2012		
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"	b. Data Protection Policies. Any natural or juridical person or other body involved in the processing of personal data shall implement appropriate data protection policies that provide for organization, physical, and technical security measures, and, for such purpose, take into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects. 1. The policies shall implement data protection principles both at	c. Records of Processing Activities. Any natural or juridical person or other body involved in the processing of personal data shall maintain records that sufficiently describe its data processing system, and identify the duties and responsibilities of those individuals who will have access to personal data. Records should include: 1. Information about the purpose of the processing of personal data, including any intended future processing or data sharing;

		the time of the determination of the means for processing and at the time of the processing itself. 2. The policies shall implement appropriate security measures that, by default, ensure only personal data which is necessary for the specified purpose of the processing are processed. They shall determine the amount of personal data collected, including the extent of processing involved, the period of their storage, and their accessibility. 3. The polices shall provide for documentation, regular review, evaluation, and updating of the privacy and security policies and practices.	2. A description of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing; 3. General information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data; 4. A general description of the organizational, physical, and technical security measures in place; 5. The name and contact details of the personal information controller and, where applicable, the joint controller, the its representative, and the compliance officer or Data Protection Officer, or any other individual or individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security. d. Management of Human Resources. Any natural or juridical person or other entity involved in the processing of personal data shall be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data. The said employees, agents, or representatives shall operate and hold personal data under strict confidentiality if the personal data are not intended for public disclosure. This obligation shall continue even

			after leaving the public service, transferring to another position, or upon terminating their employment or contractual relations. There shall be capacity building, orientation or training programs for such employees, agents or representatives, regarding privacy or security policies. e. Processing of Personal Data. Any natural or juridical person or other body involved in the processing of personal data shall develop, implement and review: 1. A procedure for the collection of personal data, including procedures for obtaining consent, when applicable; 2. Procedures that limit the processing of data, to ensure that it is only to the extent necessary for the declared, specified, and legitimate purpose; 3. Policies for access management, system monitoring, and protocols to follow during security incidents or technical problems; 4. Policies and procedures for data subjects to exercise their rights under the Act; 5. Data retention schedule, including timeline or conditions for erasure or disposal of records. f. Contracts with Personal Information Processors. The personal information controller, through appropriate contractual agreements, shall ensure that its personal information processors, where applicable, shall also implement the security

			measures required by the Act and these Rules. It shall only engage those personal information processors that provide sufficient guarantees to implement appropriate security measures specified in the Act and these Rules, and ensure the protection of the rights of the data subject.
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No.		

	2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		

18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of		

	Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF		

	DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the		

	National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		

43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation	internal	internal
		Designation of the data protection officer	Others
1	Data Privacy Act of 2012	SEC. 21. Principle of Accountability. – Each personal	

		information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. (a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party. (b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.	
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		

4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"	Section 26. Organizational Security Measures. Where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for organizational security: a. Compliance Officers. Any natural or juridical person or other body involved in the processing of personal data shall designate an individual or individuals who shall function as data protection officer, compliance officer or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security.	
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or		

	Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National		

	Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		

22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		

29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for		

	Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in		

	COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		

48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

Data Cross Boarder Dist

#	Regulation	Cross-border data transfer & Exceptions	Data localization
		Provisions for Transborder Data Transfer. What are the exceptions? (e.g., sufficient authorization, transfers based on contracts equivalent to Standard Contract Clauses (SCC) or Binding Corporate Rules (BCR), transfers based on corporate certification, etc.), Transborder transfer assessment (TIA)	Presence or absence of provisions, stipulations regarding the types of data that must be stored in the country
		Provisions for cross boarder data transfer	Provisions on requirement of localization; and Type of data required for localization
1	Data Privacy Act of 2012		
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME,		

	PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election		

	Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before		

	the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of		

	Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy		

	Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of		

	Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in		

	COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		

48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

#	Regulation	Government Access
		National Security Law, Cybersecurity Law Provisions
		Provision allowed govt to access regulated data/to not comply to data regulation
1	Data Privacy Act of 2012	
2	THE REVISED RULES OF CRIMINAL PROCEDURE	RULE 126 Search and Seizure Section 1. Search warrant defined. — A search warrant is an order in writing issued in the name of the People of the Philippines, signed by a judge and directed to a peace officer, commanding him to search for personal property described therein and bring it before the court. (1) Section 2. Court where application for search warrant shall be filed. — An application for search warrant shall be filed with the following: a) Any court within whose territorial jurisdiction a crime was committed. b) For compelling reasons stated in the application, any court within the judicial region where the crime was committed if the place of the commission of the crime is known, or any court within the judicial region where the warrant shall be enforced. However, if the criminal action has already been filed, the application shall only be made in the court where the criminal action is pending. (n) Section 3. Personal property to be seized. — A search warrant may

		be issued for the search and seizure of personal property: (a) Subject of the offense; (b) Stolen or embezzled and other proceeds, or fruits of the offense; or (c) Used or intended to be used as the means of committing an offense. (2a) Section 4. Requisites for issuing search warrant. — A search warrant shall not issue except upon probable cause in connection with one specific offense to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the things to be seized which may be anywhere in the Philippines. (3a) Section 5. Examination of complainant; record. — The judge must, before issuing the warrant, personally examine in the form of searching questions and answers, in writing and under oath, the complainant and the witnesses he may produce on facts personally known to them and attach to the record their sworn statements, together with the affidavits submitted. (4a) Section 6. Issuance and form of search warrant. — If the judge is satisfied of the existence of facts upon which the application is based or that there is probable cause to believe that they exist, he shall issue the warrant, which must be substantially in the form prescribed by these Rules. (5a) Section 7. Right to break door or window to effect search. — The officer, if refused admittance to the place of directed search after giving notice of his purpose and authority, may break open any outer or inner door or window of a house or any part of a house or anything therein to execute the warrant or liberate himself or any person lawfully aiding him when unlawfully detained therein. (6) Section 8. Search of house, room, or premise to be made in presence of two witnesses. — No search of a house, room, or any other premise shall be made except in the presence of the lawful occupant thereof or any member of his family or in the absence of the latter, two witnesses of sufficient age and discretion residing in the same locality. (7a) Section 9. Time of making search. — The warrant must direct that it be served in the day time, unless the affidavit asserts that the property is on the person or in the place ordered to be searched, in which case a direction may be inserted that it be served at any time of the day or night. (8) Section 10. Validity of search warrant. — A search warrant shall be

		valid for ten (10) days from its date. Thereafter it shall be void. (9a) Section 11. Receipt for the property seized. — The officer seizing property under the warrant must give a detailed receipt for the same to the lawful occupant of the premises in whose presence the search and seizure were made, or in the absence of such occupant, must, in the presence of at least two witnesses of sufficient age and discretion residing in the same locality, leave a receipt in the place in which he found the seized property. (10a) Section 12. Delivery of property and inventory thereof to court; return and proceedings thereon. — (a) The officer must forthwith deliver the property seized to the judge who issued the warrant, together with a true inventory thereof duly verified under oath. (b) Ten (10) days after issuance of the search warrant, the issuing judge shall ascertain if the return has been made, and if none, shall summon the person to whom the warrant was issued and require him to explain why no return was made. If the return has been made, the judge shall ascertain whether section 11 of this Rule has been complained with and shall require that the property seized be delivered to him. The judge shall see to it that subsection (a) hereof has been complied with. (c) The return on the search warrant shall be filed and kept by the custodian of the log book on search warrants who shall enter therein the date of the return, the result, and other actions of the judge. A violation of this section shall constitute contempt of court.(11a) Section 13. Search incident to lawful arrest. — A person lawfully arrested may be searched for dangerous weapons or anything which may have been used or constitute proof in the commission of an offense without a search warrant. (12a) Section 14. Motion to quash a search warrant or to suppress evidence; where to file. — A motion to quash a search warrant and/or to suppress evidence obtained thereby may be filed in and acted upon only by the court where the action has been instituted. If no criminal action has been instituted, the motion may be filed in and resolved by the court that issued the search warrant. However, if such court failed to resolve the motion and a criminal case is subsequent filed in another court, the motion shall be resolved by the latter court. (n)
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION,	Section 12. Real-Time Collection of Traffic Data. — Law enforcement authorities, with due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system. Traffic data refer only to the communication's origin, destination,

	SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)	route, time, date, size, duration, or type of underlying service, but not content, nor identities. All other data to be collected or seized or disclosed will require a court warrant. Service providers are required to cooperate and assist law enforcement authorities in the collection or recording of the above-stated information. The court warrant required under this section shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce and the showing: (1) that there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, or is being committed, or is about to be committed: (2) that there are reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and (3) that there are no other means readily available for obtaining such evidence.
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"	Section 10. Powers and Functions of Law Enforcement Authorities. – The NBI and PNP cybercrime unit or division shall have the following powers and functions: Investigate all cybercrimes where computer systems are involved; Conduct data recovery and forensic analysis on computer systems and other electronic evidence seized; Formulate guidelines in investigation, forensic evidence recovery, and forensic data analysis consistent with industry standard practices; Provide technological support to investigating units within the PNP and NBI including the search, seizure, evidence preservation and forensic recovery of data from crime scenes and systems used in crimes, and provide testimonies; Develop public, private sector, and law enforcement agency relations in addressing cybercrimes; Maintain necessary and relevant databases for statistical and/or monitoring purposes; Develop capacity within their organizations in order to perform such duties necessary for the enforcement of the Act; Support the formulation and enforcement of the national cybersecurity plan; and Perform other functions as may be required by the Act.
5	Rule on Cybercrime Warrants	Section 6. Search, Seizure and Examination of Computer Data Section 6.1. Warrant to Search, Seize and Examine Computer Data (WSSECD). – A Warrant to Search, Seize and Examine Computer Data (WSSECD) is an order in writing issued in the name of the People of the Philippines, signed by a judge, upon application of law enforcement authorities, authorizing the latter to search the particular place for items to be seized and/or examined. Section 6.2. Contents of Application for a WSSECD. – The verified

		application for a WSSECD, as well as the supporting affidavits, shall state the essential facts similar to those in Section 4.3 of this Rule, except that the subject matter is the computer data sought to be searched, seized, and examined, and all other items related thereto. In addition, the application shall contain an explanation of the search and seizure strategy to be implemented, including a projection of whether or not an off-site or on-site search will be conducted, taking into account the nature of the computer data involved, the computer or computer system's security features, and/or other relevant circumstances, if such information is available. Section 6.3. Issuance and Form of WSSECD. – If the judge is satisfied that there is probable cause to believe that the facts upon which the application for WSSECD exists, he shall issue the WSSECD, which must be substantially in the form prescribed under "Annex C" of this Rule. Section 6.4. Off-site and On-site Principle; Return of Items Seized Off-site. – Law enforcement authorities shall, if the circumstances so allow, endeavor to first make a forensic image of the computer data on-site as well as limit their search to the place specified in the warrant. Otherwise, an off-site search may be conducted, provided that a forensic image is, nevertheless, made, and that the reasons for the said search are stated in the initial return. A person whose computer devices or computer system have been searched and seized off-site may, upon motion, seek the return of the said items from the court issuing the WSSECD: Provided, that a forensic image of the computer data subject of the WSSECD has already been made. The court may grant the motion upon its determination that no lawful ground exists to otherwise withhold the return of such items to him. Section 6.5. Allowable Activities During the Implementation of the WSSECD. – Pursuant to Section 15, Chapter IV of RA 10175, the interception of communications and computer data may be conducted during the implementation of the WSSECD: Provided, that the interception activities shall only be limited to communications and computer data that are reasonably related to the subject matter of the WSSECD; and that the said activities are fully disclosed, and the foregoing relation duly explained in the initial return. Likewise, law enforcement authorities may order any person, who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein, to provide, as is reasonable, the necessary information to enable the undertaking of the search, seizure and examination. Section 6.6. Initial Return. – Within ten (10) days from the issuance of the WSSECD, the authorized law enforcement officers shall submit an initial return that contains the following information:

		1. A list of all the items that were seized, with a detailed identification of: (a) the devices of the computer system seized, including the name, make, brand, serial numbers, or any other mode of identification, if available; and (b) the hash value of the computer data and/or the seized computer device or computer system containing such data; 2. A statement on whether a forensic image of the computer data was made on-site, and if not, the reasons for making the forensic image off-site; 3. A statement on whether the search was conducted on-site, and if not, the reasons for conducting the search and seizure off-site; 4. A statement on whether interception was conducted during the implementation of the WSSECD, together with (a) a detailed identification of all the interception activities that were conducted; (b) the hash value/s of the communications or computer data intercepted; and (c) an explanation of the said items' reasonable relation to the computer data subject of the WSSECD; 5. List of all the actions taken to enforce the WSSECD, from the time the law enforcement officers reached the place to be seized until they left the premises with the seized items and reached the place where the items seized were stored and secured for examination; and 6. A reasonable estimation of how long the examination of the items seized will be concluded and the justification therefor. It is the duty of the issuing judge to ascertain if the initial return has been made, and if none, to summon the law enforcement authority to whom the WSSECD was issued and require him to explain why no initial return was made, without prejudice to any action for contempt as provided under Section 2.6 of this Rule. Section 6.7. Period to Examine and Order to Return. -After the initial return is submitted to the court pursuant to the WSSECD, the court shall issue an order fixing the period to conclude the examination of all the items seized, which period may be extended not exceeding thirty (30) days, upon motion, for justifiable reasons. Section 6.8. Final Return on the WSSECD. – Within forty-eight (48) hours after the expiration of the period to examine as provided under Section 6.7 of this Rule, the authorized law enforcement officers shall submit a final return on the WSSECD to the court that issued it, and simultaneously turn-over the custody of the seized computer data, as well as all other items seized and/or the communications or computer data intercepted in relation thereto, following the procedure under Section 7.1 of this Rule.
6	IMPLEMENTING RULES AND	

	REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"	
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns	
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers	
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity	
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework	
11	NPC Advisory No. 2021-01: Data Subject Rights	
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems	
13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and	

	Establishments Processing Personal Data for Covid-19 Response	
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response	
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission	
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website	
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website	
18	NPC Advisory No. 2018-01, 2018-02: Announcement	

	regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)	
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments	
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel	
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers	
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC	
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest	
24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector	

25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program	
26	NPC Circular No. 2023-04 - Guidelines on Consent	
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards	
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program	
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission	
30	NPC Circular No. 2022-04 - Annex 1	
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL	

	PRIVACY COMMISSION SEAL OF REGISTRATION	
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information	
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions	
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines	
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures	
36	NPC Circular 2021-01 - 2021 Rules of Procedure of the National Privacy Commission	
37	NPC Circular 2020-03 - Data	

	Sharing Agreements	
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs	
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions	
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response	
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response	
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in COVID-19 Response	
43	NPC Circular 18-03 - Rules on Mediation before the National	

	Privacy Commission	
44	NPC Circular 18-02 - Guidelines on Compliance Checks	
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions	
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1	
47	NPC Circular 17-01 - Registration of Data Processing Systems	
48	NPC Circular 16-04 - Rules of Procedure	
49	NPC Circular 16-03 - Personal Data Breach Management	
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies	
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies	

Penalties

#	Regulation	Corporate Punishments	Individual Punishments
		Forms of penalties (e.g., recommendations for corrective action, public penalties, fines, confiscation of assets and income, data deletion, data	Penalties (penalties, fines, demotion, etc.)

		processing, business suspension, etc.)	
		Forms of penalties on corporate	Forms of penalties on individual
1	Data Privacy Act of 2012	SEC. 34. Extent of Liability. – If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and lie or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.	SEC. 25. Unauthorized Processing of Personal Information and Sensitive Personal Information. – (a) The unauthorized processing of personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law. (b) The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law. SEC. 26. Accessing Personal Information and Sensitive Personal Information Due to Negligence. – (a) Accessing personal information due to negligence shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos

			(Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law. (b) Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law. SEC. 27. Improper Disposal of Personal Information and Sensitive Personal Information. – (a) The improper disposal of personal information shall be penalized by imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection. (b) The improper disposal of sensitive personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than One hundred thousand pesos (Php100,000.00)

			but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection. SEC. 28. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. – The processing of personal information for unauthorized purposes shall be penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws. The processing of sensitive personal information for unauthorized purposes shall be penalized by imprisonment ranging from two (2) years to seven (7) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws. SEC. 29. Unauthorized Access or Intentional Breach. – The penalty

			of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored. SEC. 30. Concealment of Security Breaches Involving Sensitive Personal Information. – The penalty of imprisonment of one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such security breach. SEC. 31. Malicious Disclosure. – Any personal information controller or personal information processor or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

			SEC. 32. Unauthorized Disclosure. – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall he subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00). (b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00). SEC. 33. Combination or Series of Acts. – Any combination or series of acts as defined in Sections 25 to 32 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00). SEC. 35. Large-Scale. – The maximum penalty in the scale of penalties respectively provided for the preceding offenses shall be imposed when the personal

			information of at least one hundred (100) persons is harmed, affected or involved as the result of the above mentioned actions. SEC. 36. Offense Committed by Public Officer. – When the offender or the person responsible for the offense is a public officer as defined in the Administrative Code of the Philippines in the exercise of his or her duties, an accessory penalty consisting in the disqualification to occupy public office for a term double the term of criminal penalty imposed shall he applied. SEC. 37. Restitution. – Restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.
2	THE REVISED RULES OF CRIMINAL PROCEDURE		
3	AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES (Republic Act No. 10175)		
4	Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime		

	Prevention Act of 2012"		
5	Rule on Cybercrime Warrants		
6	IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"		
7	NPC Advisory No. 2023-01: Guidelines on Deceptive Design Patterns		
8	NPC Advisory No. 2022-01: Guidelines On Requests For Personal Data Of Public Officers		
9	NPC Advisory No. 2021-03: Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity		
10	NPC Advisory No. 2021-02: Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework		
11	NPC Advisory No. 2021-01: Data Subject Rights		
12	NPC Advisory No. 2020-04: Guidelines on the Use of Closed-circuit Television (CCTV) Systems		

13	NPC Advisory No. 2020-03-A: Amending NPC Advisory No. 2020 –03 on the Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
14	NPC Advisory No. 2020-03: Guidelines for Workplaces and Establishments Processing Personal Data for Covid-19 Response		
15	NPC Advisory No. 2020-02: Guidelines on the Use of Videoconferencing Technology for the Remote Appearance and Testimony of Parties Before the National Privacy Commission		
16	NPC Advisory No. 2020-01-A: Amending Certain Provisions of NPC Advisory No. 2020-01: Protocols for the Publication of Decisions, Resolutions and Orders on the NPC Website		
17	NPC Advisory No. 2020-01: Protocols for the Publication of Decisions,		

	Resolutions and Orders on the NPC Website		
18	NPC Advisory No. 2018-01, 2018-02: Announcement regarding the submission of Personal Data Breach Notifications (PDBN) and Annual Security Incident Reports (ASIR)		
19	NPC Advisory No. 2017-03: Guidelines on Privacy Impact Assessments		
20	NPC Advisory No. 2017-02: Access to Personal Data Sheets of Government Personnel		
21	NPC Advisory No. 2017-01: Designation of Data Protection Officers		
22	NPC Circular No. 2024-01 - Amendments to Certain Provisions of the 2021 Rules of Procedure of the National Privacy Commission - 2021 Rules of Procedure of the NPC		
23	NPC Circular No. 2023-07 - Guidelines on Legitimate Interest - FAQ Guidelines on Legitimate Interest		

24	NPC Circular No. 2023-06 - Security of Personal Data in the Government and the Private Sector		
25	NPC Circular No. 2023-05 - Prerequisites for the Philippine Privacy Mark Certification Program		
26	NPC Circular No. 2023-04 - Guidelines on Consent		
27	NPC Circular No. 2023-03 - Guidelines on Identification Cards		
28	NPC Circular 2023-02 Data Privacy Competency Program - FAQ Data Privacy Competency Program		
29	NPC Circular No. 2023-01 - Schedule of Fees and Charges of the National Privacy Commission		
30	NPC Circular No. 2022-04 - Annex 1		
31	NPC Circular No. 2022-04 - REGISTRATION OF PERSONAL DATA PROCESSING SYSTEM, NOTIFICATION REGARDING AUTOMATED DECISION-		

	MAKING OR PROFILING, DESIGNATION OF DATA PROTECTION OFFICER, AND THE NATIONAL PRIVACY COMMISSION SEAL OF REGISTRATION		
32	NPC Circular No. 2022-03 - Guidelines for Private Security Agencies on the Proper Handling of Customer and Visitor Information		
33	NPC Circular No. 2022-02 - Amending Certain Provisions of NPC Circular No. 20-01 on the Guidelines on the Processing of Personal Data for Loan-Related Transactions		
34	NPC Circular No. 2022-01 - GUIDELINES ON ADMINISTRATIVE FINES - FAQs on the Guidelines on Administrative Fines		
35	NPC Circular 2021-02 - Guidelines On The Processing Of Personal Data During Public Health Emergencies For Public Health Measures		
36	NPC Circular 2021-01 - 2021		

	Rules of Procedure of the National Privacy Commission		
37	NPC Circular 2020-03 - Data Sharing Agreements		
38	NPC Circular 20-02 - Rules on the Issuance of Cease and Desist Orders - FAQs		
39	NPC Circular 20-01 - Guidelines on the Processing of Personal Data for Loan-Related Transactions		
40	DOH-NPC Joint Memorandum Circular No. 2020-0003 - Guidelines on the Monitoring and Evaluation (M&E) of the Use of Telemedicine in COVID-19 Response		
41	DOH-NPC Joint Memorandum Circular No. 2020-0002 - Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response		
42	DOH-NPC Joint Memorandum Circular No. 2020-0001 - Guidelines on the Use of Telemedicine in		

	COVID-19 Response		
43	NPC Circular 18-03 - Rules on Mediation before the National Privacy Commission		
44	NPC Circular 18-02 - Guidelines on Compliance Checks		
45	NPC Circular 18-01 - Rules of procedure on requests for Advisory Opinions		
46	NPC Circular 17-01 Appendix 1 - Registration of Data Processing Systems Appendix 1		
47	NPC Circular 17-01 - Registration of Data Processing Systems		
48	NPC Circular 16-04 - Rules of Procedure		
49	NPC Circular 16-03 - Personal Data Breach Management		
50	NPC Circular 16-02 - Data Sharing Agreements Involving Government Agencies		
51	NPC Circular 16-01 - Security of Personal Data in Government Agencies		

H) Singapore

Legal system overview

#	Regulation	Translation	Purpose of the Legal System
			What purpose does the legal system serve? (e.g. cybersecurity)
		Google translation or Translation by certain organization	
1	Personal Data Protection Act 2012		The purpose of this Act is to govern the collection, use and disclosure of personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.
2	Public Sector (Governance) Act 2018		An Act to provide for a consistent governance framework across public bodies in Singapore and to support a whole-of-government approach to the delivery of services in the Singapore public sector, and to make consequential and related amendments to certain other Acts.
3	Telecommunications Act 1999		providing for the operation and provision of telecommunication systems and services in Singapore, and for matters connected therewith.
4	CRIMINAL PROCEDURE CODE 2010		providing for the operation of criminal procedure.
5	Cybersecurity Act 2018		An Act to require or authorise the taking of measures to prevent, manage and respond to cybersecurity threats and incidents, to regulate owners of critical information infrastructure, to regulate cybersecurity service providers,

			and for matters related thereto, and to make consequential or related amendments to certain other written laws.
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		Relating to the safety, health and welfare of persons at work in workplaces.
7	Banking Act 1970		An Act to provide for the licensing and regulation of the businesses of banks, merchant banks and related institutions, and the credit card and charge card business of banks, merchant banks and other institutions, and matters related thereto.
8	PERSONAL DATA PROTECTION REGULATIONS 2021		Subsidiary Legislation of PDPA
9	Personal Data Protection (Appeal) Regulations 2021		Subsidiary Legislation of PDPA (Appeal)
10	Personal Data Protection (Composition of Offences) Regulations 2021		Subsidiary Legislation of PDPA (Composition of Offences)
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		Subsidiary Legislation of PDPA (Do Not Call Registry)
12	Personal Data Protection (Enforcement) Regulations 2021		Subsidiary Legislation of PDPA (Enforcement)
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		Subsidiary Legislation of PDPA (Notification of Data Breaches)
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		Subsidiary Legislation of PDPA (Prescribed Healthcare Bodies)

15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		Subsidiary Legislation of PDPA (Prescribed Law Enforcement Agencies)
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		Subsidiary Legislation of PDPA (Prescribed Law Enforcement Agency)
17	Personal Data Protection (Statutory Bodies) Notification 2013		Subsidiary Legislation of PDPA (Statutory Bodies)
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment		clarifying how the data protection provisions in the Personal Data Protection Act 2012 ("PDPA") apply to children's personal data in the digital environment.
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		Providing: 1.Organisations with more clarity on the use of personal data to train or develop AI to support their efforts to implement AI; 2.Guidance on information to be provided to consumers when seeking consent; 3.Guidance to third-party developers of bespoke AI Systems who may occupy the role of data intermediaries on their obligations under the PDPA; and 4.Guidance on best practices to support businesses in their compliance with the PDPA.
20	Introduction to the Guidelines		providing guidance on the manner in which the Commission will interpret provisions of the PDPA.
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act		elaborating on and providing illustrations for the key obligations in the PDPA and interpretation of key terms in the PDPA.

22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		elaborating on how the PDPA applies to particular issues and domains.
23	Advisory Guidelines on Enforcement of Data Protection Provisions		providing and elaborating on the PDPC's interpretation of enforcement on provisions relating to the data protection under the PDPA.
24	Joint Advisory on ALTDOS		providing the observed tactics, techniques and procedures employed by recent threat actor ALTDOS to compromise their victims' networks, and consider implementing the recommended measures to mitigate the threat posed.
25	Advisory Guidelines on the Do Not Call Provisions		providing an explanation of how the DNC Provisions, which are set out in Part 9 of the PDPA, may apply in different scenarios.
26	Advisory Guidelines on Application of PDPA to Election Activities		highlighting how key provisions of the PDPA apply to political parties and election candidates when carrying out election activities.
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		clarifying how the PDPA applies to organisations' collection, use and disclosure of NRIC (or copies of NRIC), and retention of physical NRICs by organisations.
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		providing greater clarity on whether an organisation may require an individual to give his consent for marketing purposes.
29	Advisory Guidelines for Management Corporations		clarifying how the Data Protection Provisions in the PDPA apply to MCSTs' collection, use and disclosure of personal data, as well as suggesting good data protection practices in certain scenarios.
30	Advisory Guidelines for the Education Sector		addressing the unique circumstances faced by the education sector in complying with the PDPA.

31	Advisory Guidelines for the Social Service Sector		clarifying how the Data Protection Provisions in the PDPA apply to social service agencies' collection, use and disclosure of personal data, as well as suggesting good data protection practices in certain scenarios.
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		providing guidance on ensuring compliance with the Data Protection Provisions when in-vehicle recording devices ("IVRDs").
33	Advisory Guidelines for the Real Estate Agency Sector		addressing the unique circumstances faced by the real estate agency sector in complying with the PDPA.
34	Advisory Guidelines for the Healthcare Sector		clarifying how the Data Protection Provisions in the PDPA apply to healthcare institutions' collection, use and disclosure of personal data, as well as suggesting good data protection practices in certain scenarios.
35	Advisory Guidelines for the Telecommunication Sector		addressing the unique circumstances faced by the telecommunication sector in complying with the Personal Data Protection Act 2012 ("PDPA").
36	Joint Technical Advisory on LockBit 3.0		highlighting the observed Tactics, Techniques and Procedures (TTPs) employed by LockBit to compromise their victims' networks and providing some recommended measures for organisations to mitigate the threat posed.
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		clarifying the duties and responsibilities that a selfemployed agent who is a representative ("tied agent") of a direct life insurer shall observe in respect of the Personal Data Protection Act 2012 (PDPA).

#	Regulation	Form of legal system	Target Business
		Is it introduced in accordance with government ordinances and	Does the law target specific industry or in general? Is it clearly stated in the regulations?

		guidelines? (Is it introduced in a format that ensures lead time?)	
		Regulation level	Industry
1	Personal Data Protection Act 2012	Law	General
2	Public Sector (Governance) Act 2018	Law	public bodies in Singapore
3	Telecommunications Act 1999	Law	telecommunication service
4	CRIMINAL PROCEDURE CODE 2010	Law	General
5	Cybersecurity Act 2018	Law	General
6	Workplace Safety and Health (Medical Examinations) Regulations 2011	Regulation	workplaces in which persons are employed in any hazardous occupation
7	Banking Act 1970	Law	Bank
8	PERSONAL DATA PROTECTION REGULATIONS 2021	Regulation	General
9	Personal Data Protection (Appeal) Regulations 2021	Regulation	General
10	Personal Data Protection (Composition of Offences) Regulations 2021	Regulation	General
11	Personal Data Protection (Do Not Call Registry) Regulations 2013	Regulation	Telecommunications service provider
12	Personal Data Protection (Enforcement) Regulations 2021	Regulation	General
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021	Regulation	General
14	Personal Data Protection (Prescribed Healthcare	Notification	Healthcare bodies

	Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014	Notification	Law Enforcement Agencies
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020	Notification	Law Enforcement Agencies
17	Personal Data Protection (Statutory Bodies) Notification 2013	Notification	Statutory Bodies
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment	Advisory Guidelines	General
19	Advisory Guidelines on use of Personal Data in AI Recommendatio n and Decision Systems	Advisory Guidelines	General
20	Introduction to the Guidelines	Advisory Guidelines	General
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act	Advisory Guidelines	General
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics	Advisory Guidelines	General
23	Advisory Guidelines on Enforcement of Data Protection Provisions	Advisory Guidelines	General

24	Joint Advisory on ALTDOS	Advisory Guidelines	General
25	Advisory Guidelines on the Do Not Call Provisions	Advisory Guidelines	General
26	Advisory Guidelines on Application of PDPA to Election Activities	Advisory Guidelines	political parties and election candidates
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers	Advisory Guidelines	General
28	Advisory Guidelines on Requiring Consent for Marketing Purposes	Advisory Guidelines	General
29	Advisory Guidelines for Management Corporations	Sector-Specific Advisory Guidelines	management corporations of strata title plans (MCST)
30	Advisory Guidelines for the Education Sector	Sector-Specific Advisory Guidelines	Education sector
31	Advisory Guidelines for the Social Service Sector	Sector-Specific Advisory Guidelines	Social Service Sector
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire	Sector-Specific Advisory Guidelines	Transport Services for Hire
33	Advisory Guidelines for the Real Estate Agency Sector	Sector-Specific Advisory Guidelines	Real Estate Agency Sector
34	Advisory Guidelines for the Healthcare Sector	Sector-Specific Advisory Guidelines	Healthcare Sector

35	Advisory Guidelines for the Telecommunication Sector	Sector-Specific Advisory Guidelines	Telecommunication Sector
36	Joint Technical Advisory on LockBit 3.0	Industry-led Guidelines	General
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act	Industry-led Guidelines	selfemployed agent who is a representative of a direct life insurer

#	Regulation	Regulatory authority	Jurisdiction
		Which regulatory authority has jurisdiction over regulation?	Cyber security, data security, personal information protection, etc.
		Name of ministry/organization	Similar to purpose?
1	Personal Data Protection Act 2012	Personal Data Protection Commission	Personal Information, Data security
2	Public Sector (Governance) Act 2018	Public Service Commission	governance framework
3	Telecommunications Act 1999	Info-communications Media Development Authority	Personal Information, Data security, Competition
4	CRIMINAL PROCEDURE CODE 2010	Minister for Law	criminal procedure
5	Cybersecurity Act 2018	Commissioner of Cybersecurity	Cybersecurity
6	Workplace Safety and Health (Medical Examinations) Regulations 2011	Minister for Manpower	Workplace Safety, Health
7	Banking Act 1970	Monetary Authority	Finance
8	PERSONAL DATA PROTECTION REGULATIONS 2021	Personal Data Protection Commission	Personal Information, Data security
9	Personal Data Protection (Appeal) Regulations 2021	Personal Data Protection Commission	Personal Information, Data security
10	Personal Data Protection (Composition of	Personal Data Protection Commission	Personal Information, Data security

	Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013	Minister for Communications and Information	Personal Information, Data security
12	Personal Data Protection (Enforcement) Regulations 2021	Personal Data Protection Commission	Personal Information, Data security
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021	Personal Data Protection Commission	Personal Information, Data security
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015	Minister for Health	Personal Information, Data security
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014	Minister for Home Affairs	Personal Information, Data security
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020	Prime Minister	Personal Information, Data security
17	Personal Data Protection (Statutory Bodies) Notification 2013	Minister for Communications and Information	Personal Information, Data security
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment	Personal Data Protection Commission	Personal Information, Data security
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems	Personal Data Protection Commission	Personal Information, Data security

20	Introduction to the Guidelines	Personal Data Protection Commission	Personal Information, Data security
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act	Personal Data Protection Commission	Personal Information, Data security
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics	Personal Data Protection Commission	Personal Information, Data security
23	Advisory Guidelines on Enforcement of Data Protection Provisions	Personal Data Protection Commission	Personal Information, Data security
24	Joint Advisory on ALTDOS	Cyber Security Agency of Singapore (CSA) Personal Data Protection Commission (PDPC) Singapore Police Force (SPF)	Personal Information, Cyber security
25	Advisory Guidelines on the Do Not Call Provisions	Personal Data Protection Commission	Personal Information, Data security
26	Advisory Guidelines on Application of PDPA to Election Activities	Personal Data Protection Commission	Personal Information, Data security
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers	Personal Data Protection Commission	Personal Information, Data security
28	Advisory Guidelines on Requiring Consent for Marketing Purposes	Personal Data Protection Commission	Personal Information, Data security
29	Advisory Guidelines for Management Corporations	Personal Data Protection Commission	Personal Information, Data security
30	Advisory Guidelines for	Personal Data Protection Commission	Personal Information, Data security

	the Education Sector		
31	Advisory Guidelines for the Social Service Sector	Personal Data Protection Commission	Personal Information, Data security
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire	Personal Data Protection Commission	Personal Information, Data security
33	Advisory Guidelines for the Real Estate Agency Sector	Personal Data Protection Commission	Personal Information, Data security
34	Advisory Guidelines for the Healthcare Sector	Personal Data Protection Commission	Personal Information, Data security
35	Advisory Guidelines for the Telecommunication Sector	Personal Data Protection Commission	Personal Information, Data security
36	Joint Technical Advisory on LockBit 3.0	Cyber Security Agency of Singapore (CSA) Personal Data Protection Commission (PDPC) Singapore Police Force (SPF)	Personal Information, Cyber security
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act	Life Insurance Association	Personal Information, Data security

#	Regulation	Status	Citation
		Legislation / Public Comment / Passage / Enforcement / Amendment, etc.	
		Status of the regulation: Draft = drafting (new regulation) published = published in the gazzette but not yet enacted Enact = published in the gazzette and already enacted Amendment = enacted regulation being on amending process	URL

1	Personal Data Protection Act 2012	Enforcement	https://sso.agc.gov.sg/Act/PDPA2012
2	Public Sector (Governance) Act 2018	Enforcement	https://sso.agc.gov.sg/Acts-Supp/5-2018/Published/20180305?DocDate=20180305
3	Telecommunications Act 1999	Enforcement	https://sso.agc.gov.sg/Act/TA1999
4	CRIMINAL PROCEDURE CODE 2010	Enforcement	https://sso.agc.gov.sg/Act/CPC2010
5	Cybersecurity Act 2018	Enforcement	https://sso.agc.gov.sg/Acts-Supp/9-2018/
6	Workplace Safety and Health (Medical Examinations) Regulations 2011	Enforcement	https://sso.agc.gov.sg/SL/WSHA2006-S516-2011?DocDate=20110909&ProvIds=Sc-
7	Banking Act 1970	Enforcement	https://sso.agc.gov.sg/Act/BA1970
8	PERSONAL DATA PROTECTION REGULATIONS 2021	Enforcement	https://sso.agc.gov.sg/SL-Supp/S63-2021/Published/20210129?DocDate=20210129
9	Personal Data Protection (Appeal) Regulations 2021	Enforcement	https://sso.agc.gov.sg/SL/PDPA2012-S65-2021?DocDate=20210129
10	Personal Data Protection (Composition of Offences) Regulations 2021	Enforcement	https://sso.agc.gov.sg/SL/PDPA2012-S70-2021?DocDate=20210129
11	Personal Data Protection (Do Not Call Registry) Regulations 2013	Enforcement	https://sso.agc.gov.sg/SL/PDPA2012-S709-2013?DocDate=20210129
12	Personal Data Protection (Enforcement) Regulations 2021	Enforcement	https://sso.agc.gov.sg/SL/PDPA2012-S62-2021?DocDate=20220930
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021	Enforcement	https://sso.agc.gov.sg/SL/PDPA2012-S64-2021?DocDate=20210930
14	Personal Data Protection (Prescribed Healthcare	Enforcement	https://sso.agc.gov.sg/SL/PDPA2012-S90-2015?DocDate=20210129

	Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014	Enforcement	https://sso.agc.gov.sg/SL/PDPA2012-S368-2014?DocDate=20210129
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020	Enforcement	https://sso.agc.gov.sg/SL/PDPA2012-S272-2020?DocDate=20210205
17	Personal Data Protection (Statutory Bodies) Notification 2013	Enforcement	https://sso.agc.gov.sg/SL/PDPA2012-S149-2013?DocDate=20191108
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-on-the-pdpa-for-children's-personal-data-in-the-digital-environment_mar24.pdf
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-on-the-use-of-personal-data-in-ai-recommendation-and-decision-systems.pdf
20	Introduction to the Guidelines	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/introduction-to-the-guidelines.pdf
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/ag-on-key-concepts/advisory-guidelines-on-key-concepts-in-the-pdpa-17-may-2022.pdf
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/ag-on-selected-topics/advisory-guidelines-on-the-pdpa-for-selected-topics-17-may-2022.pdf

23	Advisory Guidelines on Enforcement of Data Protection Provisions	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-on-enforcement-of-dp-provisions_1oct2022.pdf
24	Joint Advisory on ALTDOS	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/joint-advisory-on-altdos-(1).pdf
25	Advisory Guidelines on the Do Not Call Provisions	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-on-the-dnc-provisions-1-feb-2021.pdf
26	Advisory Guidelines on Application of PDPA to Election Activities	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-on-the-application-of-pdpa-to-election-activities_28july2023.pdf
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-for-nric-numbers---310818.pdf
28	Advisory Guidelines on Requiring Consent for Marketing Purposes	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisoryguidelinesonrequiringconsentformarketing8may2015.pdf
29	Advisory Guidelines for Management Corporations	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-for-management-corporations-17-may-2022.pdf
30	Advisory Guidelines for the Education Sector	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/legislation-and-guidelines/finalised-education-guidelines_31aug2018.pdf
31	Advisory Guidelines for the Social Service Sector	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-

			for-the-social-service-sector_18-january-2024.pdf
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/sector-specific-advisory/advisory-guidelines-on-in-vehicle-recordings_updated-22-may-2018.pdf
33	Advisory Guidelines for the Real Estate Agency Sector	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/sector-specific-advisory/real-estate.pdf
34	Advisory Guidelines for the Healthcare Sector	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-for-the-healthcare-sector-sep-2023.pdf
35	Advisory Guidelines for the Telecommunication Sector	Enforcement	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/sector-specific-advisory/finalised-advisory-guidelines-on-application-of-pdpa-to-telecom-sector.pdf
36	Joint Technical Advisory on LockBit 3.0	Enacted	https://www.csa.gov.sg/docs/default-source/publications/singcert/2023/joint-technical-advisory-on-lockbit-3.0.pdf?sfvrsn=46c2367_1
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act	Enacted	https://www.lia.org.sg/media/1230/mu-6215-code-of-conduct-on-pdpa.pdf

Definitions for basic items

#	Regulation	Type and Scope of Data	Data processing and handling
		Personal data, personal information/sensitive and important data/children and minors' data, etc. Is the scope of data clearly written in the regulations? What are the unclear points?	Processing, handling / disclosure, sharing, provision, transmission, outsourcing / use for advertising, etc.
		Specific type of data required to complied with the regulation	Provision for data processing

1	Personal Data Protection Act 2012	"personal data" means data, whether true or not, about an individual who can be identified — (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access; "derived personal data" — (a) means personal data about an individual that is derived by an organisation in the course of business from other personal data, about the individual or another individual, in the possession or under the control of the organisation; but (b) does not include personal data derived by the organisation using any prescribed means or method; "user activity data", in relation to an organisation, means personal data about an individual that is created in the course or as a result of the individual's use of any product or service provided by the organisation; "user-provided data", in relation to an organisation, means personal data provided by an individual to the organisation. "business contact information" means an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his or her personal purposes;	"processing", in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following: (a) recording; (b) holding; (c) organisation, adaptation or alteration; (d) retrieval; (e) combination; (f) transmission; (g) erasure or destruction;
2	Public Sector (Governance) Act 2018		

3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		

16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment	e. "geolocation" refers to the ability to determine the physical location of a device.	a. "age assurance" refers to methods for ascertaining a person's age and includes self-declaration, age estimation, and age verification; b. "age estimation" refers to the estimation of an individual's age or age range; c. "age verification" refers to the verification of an individual's age or confirmation that an individual is above a certain age (e.g. below 18 years of age);
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act	Personal data Personal data is defined in the PDPA as "data, whether true or not, about an individual who can be identified — a) from that data; or b) from that data and other information to which the organisation has or is likely to have access". The term "personal data" is not intended to be narrowly construed and may cover different types of data about an individual and from which an individual can be identified, regardless of whether such data is true or accurate, or whether the data	Collection, Use and Disclosure Part 4 of the PDPA sets out the obligations of organisations relating to the collection, use and disclosure of personal data. The PDPA does not define the terms "collection", "use" and "disclosure". These terms would apply as they are commonly understood to cover the common types of activities undertaken by organisations in respect of personal data that may fall under collection, use or disclosure respectively. In general, the terms "collection", "use" and "disclosure" may be understood to have the following meanings:

		exists in electronic or other form. The PDPA does not apply in relation to certain categories of personal data which are expressly excluded from the application of the PDPA. These are highlighted in the sections later. Please also refer to the chapter on "Anonymisation" in the Advisory Guidelines on the PDPA for Selected Topics, which describes the considerations and conditions under which personal data may be anonymised and no longer considered personal data for the purposes of the PDPA. When is data considered "personal data"? The most basic requirement for data to constitute personal data is that it is information about an identifiable individual. There are two principal considerations. First, is the purpose of information to be data about an individual or which relates to the individual. Examples include information about an individual's health, educational and employment background, as well as an individual's activities such as spending patterns. There will be situations where the personal data is incidental to the purpose of the information. For example, an internal investigations report that incidentally includes names and appointments of key actors involved in the incident under investigations. The content of individuals' communications, such as email messages and text messages, in and of themselves will generally not be considered personal data, unless they contain information about an individual that can identify the individual. Second, the individual should be identifiable from the data.	a) Collection refers to any act or set of acts through which an organisation obtains control over or possession of personal data. b) Use refers to any act or set of acts by which an organisation employs personal data. A particular use of personal data may occasionally involve collection or disclosure that is necessarily part of the use. c) Disclosure refers to any act or set of acts by which an organisation discloses, transfers or otherwise makes available personal data that is under its control or in its possession to any other organisation. Organisations should bear in mind that collection, use and disclosure may take place actively or passively. Both forms of collection, use and disclosure are subject to the same obligations under the PDPA although what may be considered reasonable purposes may vary based on the circumstances of the collection, use or disclosure. Example: When applying for an insurance plan, Karen is interviewed by an insurance agent who asks her for various personal details, as well as information about her health. This is a form of active collection of personal data. In comparison, Karen attends a reception and writes her name in the unattended guestbook placed near the entrance. This is a form of passive collection of personal data.

		However, not all data that relates to an individual may identify the individual. For example, a residential address could also relate to another individual who resides there, and it may not be possible to identify a specific individual from the residential address. Data constitutes personal data if it is data about an individual who can be identified from that data on its own, or from that data and other information to which the organisation has or is likely to have access. For example, a mailing list of email addresses may not be personal data on its own, but if the list contains customer IDs that can be linked to records in the Customer Relationship Management ("CRM") system, then the list may be considered personal data. A practical approach is to first identify the set of information under consideration (e.g. information recorded in documents and stored in files, or stored in electronic databases or IT systems). Next, organisations should apply the analysis in the preceding paragraphs and ask: (a) is the purpose of this set of information about individuals; and (b) can individuals be identified from this set of information or other information they have access to. In general, organisations should avoid making assessments in the abstract. The following paragraphs set out a few of the Commission's considerations in determining personal data. Number of data elements in the dataset and availability of other information The rule of thumb is that there should be at least two data elements in the dataset before individuals can be identified. Sometimes, more than	

		two data elements may be required before an individual can be identified. This depends very much on the specificity and nature of the data elements. For example, the combination of name and NRIC number is usually sufficient to identify individuals, but email addresses may need to be combined with customer shopping preferences and purchase history before individuals can be identified from this combination of data elements. In determining whether the dataset is personal data, an organisation should not overlook the availability of other information it has or is likely to have access to. For example, a unique customer ID that can link a mailing list to the CRM system. In general, the Commission will apply a "practicability" threshold in determining whether an organisation is likely to have access to other data that will identify an individual. As such, an organisation will not be considered to have access to other information if it is not practicable (e.g. where it requires huge costs, time, resources) even though it is theoretically or technically possible for the organisation to gain access to such information. Nature of data Certain types of data, by their nature or use, are more likely to identify an individual. This includes data that has been assigned exclusively to an individual for the purposes of identifying the individual (e.g. NRIC or passport number of an individual), or data of a biological nature (e.g. DNA, facial image, fingerprint, iris prints). In general, fewer data elements are required for a dataset to	

		constitute personal data if it contains data points or data elements that are more unique to an individual. In contrast, generic information, such as gender, nationality, age or blood group, will unlikely be able to identify a particular individual. Nevertheless, such information may still constitute part of the individual's personal data if it is combined with other information such that it can be associated with, or made to relate to, an identifiable individual. Purpose of the dataset or document The purpose of the dataset or document is another relevant factor to consider in determining whether it contains personal data. One of the purposes (which need not be the dominant or primary purpose) of the dataset or document should be to record or communicate information about an individual before the collection of information is considered personal data. For example: a) Content of email messages is not personal data unless the content was intended to convey additional information about an individual (e.g., employment or medical history of an individual): Re Executive Coach International Pte. Ltd [2017] SGPDPC 3, Re Interflour Group Pte Ltd [2017] PDP Digest; b) Private communications (e.g. WhatsApp messages and chats) are not necessarily personal data in and of themselves: Re Black Peony [2017] PDP Digest, in relation to screenshots of WhatsApp messages disclosed on the Internet; c) Customer database, including extracts compiled in a document will constitute personal data: Re K Box Entertainment Group Pte Ltd	

		[2016]; and d) Communications content to name/blacklist specific individuals will constitute personal data, but the purpose of the communication may be reasonably acceptable: Re Jump Rope [2016]. Example: Organisation ABC conducts a street intercept survey to collect information from passers-by on the average amount spent on household items per month, their full name, gender, and age range. The dataset constitutes personal data of the individuals as they can be identified from the dataset. If ABC only collects information on the average amount spent on household items, gender, and age range, the dataset may not constitute personal data as it is unlikely to identify the individuals. Example: Organisation DEF conducts a street intercept survey and collects the following information from passers-by: • Age range • Gender • Occupation • Place of work Although each of these data points, on its own, would not be able to identify an individual, DEF should be mindful that the dataset, comprising a respondent's age range, gender, occupation and place of work may be able to identify the respondent. Respondent A is a female individual who is between 20 and 30 years of age and works as a retail salesperson at a particular shopping mall in Orchard Road. This dataset may not be able to identify Respondent A since	

		there could be many female salespersons in their 20s working in retail outlets at Orchard Road. Respondent B is a male individual who is between 20 and 30 years of age and works as a security officer at a specific office building on Bencoolen Street. This dataset may be able to identify respondent B if there are no other male security officers in their 20s working at Bencoolen Street. Given that some of the respondents' datasets are likely to identify the respondents, DEF should treat the datasets as personal data and ensure they comply with the Data Protection Provisions. Example: Organisation GHI collects data of its employees (i.e. educational information, blood type, full name). GHI also keeps a record of its minutes of meeting, containing information that was shared by certain employees. When assessed holistically, the combination of employee records and company data will constitute personal data of the employees. However, the minutes of meeting on its own, will unlikely be deemed as containing personal data of the employees in the meeting as such information is not the objective of the minutes (i.e. to keep official record of actions and decisions made at a meeting). Truth and accuracy of personal data It should be noted that the PDPA's definition of personal data does not depend on whether the data is true or accurate. If organisations collect personal data which is	

		inaccurate, or if the data collected has changed such that it is no longer true, such data will still be personal data, and organisations are required to comply with the Data Protection Provisions under the PDPA. As explained in greater detail in the section on the Data Protection Provisions, organisations have an obligation in certain situations to make a reasonable effort to ensure that personal data collected is accurate and complete (the "Accuracy Obligation"). Personal data relating to more than one individual Information about one individual may contain information about another individual. In that circumstance, the same information could be personal data of both individuals. Example: An adventure camp company records emergency contact information for all the participants in the adventure camp. This emergency contact information comprises the name, address and telephone number of the individual whom the organisation will contact in the event of an emergency. Bernie's emergency contact is her husband, Bernard, and she provides his contact details to the company as her emergency contact information. Bernard's name, address and telephone number form part of the personal data of Bernie. As such, the company is holding personal data about two individuals. In addition, since Bernard's personal data also forms part of Bernie's personal data (specifically, the details of her emergency contact), organisations would need to protect it as part of Bernie's	

		personal data. Excluded personal data The PDPA does not apply to, or applies to a limited extent to, certain categories of personal data. The PDPA does not apply to the following categories of personal data: a) Personal data that is contained in a record that has been in existence for at least 100 years; and b) Personal data about a deceased individual who has been dead for more than 10 years. For personal data about a deceased individual who has been dead for 10 years or less, the PDPA applies to a limited extent. For such personal data, only the provisions relating to the disclosure and protection of personal data will apply. These provisions are considered further below. Business contact information The Data Protection Provisions do not apply to business contact information. Business contact information is defined in the PDPA as "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his or her personal purposes". Organisations are not required to obtain consent before collecting, using or disclosing any business contact information or comply with any other obligation in the Data Protection Provisions in relation to business contact information. Example: At the registration booth of a	

		corporate seminar, Sharon drops her business name card into a glass bowl by the side of the registration booth as she wishes to be on the seminar organiser's mailing list for future invitations to similar seminars. Sharon's business name card contains her name, position, business telephone number, business address, business electronic mail address and business fax number. As Sharon did not provide her business name card solely for personal purposes, the information on the card will be considered business contact information. Accordingly, the seminar organiser does not need to seek Sharon's consent to contact her about future seminars through her business contact information. The seminar organiser is also not required to care for such information or provide access to and correction of the business contact information collected. The definition of business contact information is dependent on the purpose for which such contact information may be provided by an individual as it recognises that an individual may provide certain work-related contact information solely for personal purposes. In such situations, the information would not constitute business contact information and organisations would be required to comply with the Data Protection Provisions in respect of such information. However, in most circumstances, the Commission is likely to consider personal data provided on business/name cards as business contact information. Example: Sharon is signing up for a gym membership. She provides her	

		business name card to the gym staff so that they can record her name and contact details in order to register her for the package. In this case, the information provided by Sharon would not be business contact information as she is providing it solely for her personal purposes. The PDPA would apply to the information contained in her business name card. Since sole proprietorships and partnerships are also businesses, the contact information of sole proprietors and partners is considered business contact information where such information has not been provided solely for personal purposes. Example: Damien is a choral instructor who is the sole proprietor of a music studio. He decides to engage a salesperson, Tom, to assist him in searching for a suitable property unit as a second branch. Damien passes his contact details to Tom so that Tom can update him from time to time on property units which he might like. Tom shares Damien's contact details with his colleagues, so that more salespersons can assist Damien with his property search. Damien's consent to the sharing of his contact information is not required because it is business contact information. As Damien has provided his contact details for the purpose of a property search for his business, this information is considered business contact information and can be passed on by Tom subsequently without Damien's prior consent. In turn, other persons can also collect, use and disclose Damien's business	

		contact information freely, without requiring Damien's consent. Derived personal data Derived personal data is defined under the PDPA to refer to personal data about an individual that is derived by an organisation in the course of business from other personal data about the individual or another individual, in the possession or under the control of the organisation. It generally refers to new data elements created through the processing of personal data (e.g. through mathematical, logical, statistical, computational, algorithmic, or analytical methods based on the application of business-specific rules). Derived data is a general term but in the context of data portability, it does not include personal data derived by the organisation using any prescribed means or methods which are commonly known and used by the industry (e.g. simple mathematical averaging or summation). Personal data of deceased individuals As noted earlier, the term "individual" includes both living and deceased individuals. Hence, the provisions of the PDPA will apply to protect the personal data of deceased individuals to the extent provided in the PDPA. Specifically, the PDPA provides that the obligations relating to the disclosure and protection of personal data will apply in respect of the personal data about an individual who has been dead 10 years or less. These provisions relate to the following matters, which are explained in greater detail later in the section on the Data Protection Provisions:	

		a) Notification of purposes for disclosure of personal data (part of the "Notification Obligation" as explained later); b) Obtaining consent for disclosure of personal data (part of the "Consent Obligation" as explained later); c) Disclosing personal data for purposes which a reasonable person would consider appropriate in the circumstances (part of the "Purpose Limitation Obligation" as explained later); d) Making a reasonable effort to ensure the accuracy and completeness of personal data that is likely to be disclosed to another organisation (part of the "Accuracy Obligation" as explained later); and e) Making reasonable security arrangements to protect personal data (part of the "Protection Obligation" as explained later). The above obligations will apply in respect of the personal data of a deceased individual for 10 years from the date of death. This is intended to minimise any adverse impact of unauthorised disclosure of such data on family members of the deceased. When complying with their obligations under the PDPA, organisations should take note of the individuals who may act on behalf of the estate of the deceased individual in respect of matters relating to the deceased's personal data, as prescribed in regulations to be issued under the PDPA. Other than the provisions noted above, organisations do not have additional obligations relating to personal data of deceased individuals. Organisations should note that while the PDPA does not apply to personal data of individuals who have been	

		deceased for more than 10 years, there may still be other legal or contractual requirements that organisations should be mindful of. Control, not ownership, of personal data Personal data, as used in the PDPA, refers to the information comprised in the personal data and not the physical form or medium in which it is stored, such as a database or a book. The PDPA provides data subjects with some extent of control over personal data, for example controlling the purpose of use through consent and withdrawal of consent, accessing and requesting for a copy of personal data or for corrections to be made. The PDPA does not specifically confer any property or ownership rights on personal data per se to individuals or organisations and also does not affect existing property rights in items in which personal data may be captured or stored. For example, an individual John Tan lives at Block 123 Ang Mo Kio Avenue 456. The fact that the individual's name is John Tan and that he lives at Block 123 Ang Mo Kio Avenue 456 is personal data of John Tan. However, John Tan does not own the information contained in the name "John Tan" or the information contained in the address "Block 123 Ang Mo Kio Avenue 456". If John Tan's name and address are written on a letter that is intended to be posted to him, the PDPA does not affect ownership rights to the letter which bears John Tan's name and address. Similarly, if organisation A takes a photograph of John Tan, the identifiable image of John Tan would constitute his personal	

		data. However, John Tan would not be conferred ownership rights to that photograph under the PDPA. Instead, ownership would depend on existing laws such as property law and copyright law. Regardless of ownership rights, organisations must comply with the PDPA if they intend to collect, use or disclose personal data about an individual.	
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions		
26	Advisory Guidelines on Application of PDPA to Election Activities		
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		6 Definition of "marketing purposes" 6.1 These Guidelines will focus on the application of sections 14(2)(a) and 46(1) to situations where organisations wish to require an individual's consent for: (a) sending marketing materials to the individual (whether by post, text, voice call, email or

			otherwise); or (b) using the individual's personal data for any other marketing activities by the organisation (e.g. publishing customers' personal data in publicity materials). 6.2 For ease of reference within these Guidelines only, the purposes listed in 6.1 (a) and (b) above will be referred to as "marketing purposes".
29	Advisory Guidelines for Management Corporations		Collection, use or disclosure of personal data by MCSTs 2.2 MCSTs carry out duties and functions as set out in the BMSMA, for example, to properly maintain the common property. In the course of performing their duties and functions under the BMSMA, MCSTs are required to collect personal data of individuals for a number of specific purposes. For instance, MCSTs are required to collect the name and address of the subsidiary proprietor, the name of any mortgagee of the lot, and the name of the representative of the subsidiary proprietor where such subsidiary proprietor is a company, for the purposes of preparing and maintaining a strata roll.7 Subsidiary proprietors are also required to give written notice to the MCST of their addresses in Singapore for the service of notices8, as well as to provide the names and addresses of the proxy giver or proxy holder in the proxy form9 . Under the BMSMR, MCSTs are required to collect the names, NRIC/FIN numbers and addresses of elected members of the council and executive committee of the MCST. 2.3 If a MCST is required or authorised to collect, use or disclose personal data without consent under the BMSMA,

			BMSMR or other laws10, it may do so without obtaining consent from the individual11. Otherwise, consent must be obtained in accordance with the PDPA. For example, if the MCST wishes to collect mobile numbers of subsidiary proprietors for inclusion into the strata roll or other purposes (e.g. issuing car decals), the MCST would have to notify and seek consent from the relevant individuals for the purposes, as the BMSMA12 does not require such information to be collected in the strata roll. In the case of email addresses, as the BMSMA provides for MCSTs to serve notices to subsidiary proprietors by email (in addition to post)13, subsidiary proprietors may provide their email address for this purpose, and the email address of subsidiary proprietors may be included as personal data as part of the information in the strata roll for the purpose of serving notices on the relevant subsidiary proprietors. However, if subsidiary proprietors provide their email address to the MCST for purposes such as issuing car decals, consent will need to be sought from the subsidiary proprietor to include the email addresses in the strata roll for other purposes. 2.4 Example: Disclosure of personal data to subsidiary proprietors Mary is a resident at estate ABC. Recently, her apartment ceiling started leaking water and she wishes to get in touch with the owner of the unit above hers to resolve the issue. She approaches the MCST to obtain the mobile number of the unit owner. As consent is needed from the unit owner to disclose his mobile number for this

			purpose, the MCST notifies the unit owner and obtains his consent to disclose his mobile number to Mary for this purpose.
30	Advisory Guidelines for the Education Sector		
31	Advisory Guidelines for the Social Service Sector		
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector	2 Personal data 2.1 Personal data is defined in the PDPA as "data, whether true or not, about an individual who can be identified – a) from that data; or b) from that data and other information to which the organisation has or is likely to have access." 2.2 While some data may necessarily relate to an individual, other data may not, on its own, relate to an individual. Such data would not constitute personal data unless it is associated with, or made to relate to, a particular individual. Generic information that does not relate to a particular individual may also form part of an individual's personal data when combined with personal data or other information to enable an individual to be identified. 2.3 The Commission understands that the types of personal data1 that are typically collected by estate agent(s)2 or salesperson(s)3 may include, but are not limited to, the full name, NRIC number, marital status, contact details and residential	

		addresses of client(s)4 and/or other parties to the transaction. Estate agent(s) or salesperson(s) may also obtain documents containing personal data such as personal cheques from their client(s) and/or other parties to the transaction. 2.4 In some situations, the information collected, used or disclosed by estate agents or salespersons may not be personal data. 2.5 Example: When information is personal data Estate agent ABC analyses the data of properties bought or sold through its salespersons to gather insights into the property market. The raw data includes personal data about the buyers and sellers of the properties. ABC would also like to publish aggregated statistics of sales for public reference on developments in the property market. ABC anonymises the raw data by removing the identifying information and the means of re-identification, such that the remaining data does not identify any particular individual in itself or in combination with other information that the organisation has or is likely to have access to. In this case, ABC would not be disclosing personal data. However, as a good practice, ABC should consider the possibility of factors beyond its control which may pose a challenge in keeping data anonymised. Please refer to the chapter in the Advisory Guidelines for Selected Topics relating to Anonymisation for more information. 2.6 Example: Using personal data Estate agent ABC is marketing the launch of a new	

		development. It distributes flyers to all the mailboxes of properties located in the vicinity of the new launch, addressed generically to "The Resident". In this case, ABC has not collected or used the personal data of any individual residing in the vicinity in the distribution of the flyers. 2.7 Estate agent ABC is marketing a newly-launched development. It mails flyers specifically to former clients of its salespersons by using the name and address of the former clients. In this case, ABC has used the personal data of these former clients to market the new launch.	
34	Advisory Guidelines for the Healthcare Sector		
35	Advisory Guidelines for the Telecommunicati on Sector	2 Personal Data 2.1 Personal data is defined in the PDPA as "data, whether true or not, about an individual who can be identified – a) from that data; or b) from that data and other information to which the organisation has or is likely to have access." 2.2 While some data will always relate to an individual, other data may not, on its own, relate to an individual. Such data would not constitute personal data unless it is associated with, or made to relate to, a particular individual. Generic information that does not relate to a particular individual may also form part of an individual's personal data when combined with personal data or other information to enable an individual to be identified. Telephone numbers and International Mobile Equipment Identity ("IMEI") numbers 2.3 Where an individual	

		is identifiable from the data, such as a combination of the individual's name, address and telephone number, then such data is personal data. In cases where the individual cannot be identified from that data alone (such as a device identifier in itself), such data may still be personal data if the organisation has or is likely to have access to other information that will allow the individual to be identified when taken together with that data. Please also refer to the section on Anonymisation in the Advisory Guidelines on Selected Topics for more details on the conditions under which personal data may be anonymised and hence no longer considered to be personal data for purposes of the PDPA. 2.4 In the telecommunication context, an individual's mobile telephone number is likely to be personal data as it may uniquely identify, or be uniquely associated with, that individual. A telephone number that is shared by more than one individual (e.g. a landline shared by several residents in a dwelling) may also be considered personal data if, in the particular circumstances, combination with other information results in the identification of an individual. What constitutes personal data is elaborated on in the Key Concepts Guidelines. 2.5 Various numbers are used in connection with the operation of a telecommunication network, for example, to identify particular equipment that is connected to the network. Examples of such numbers include Internet Protocol ("IP") addresses and IMEI numbers. In general, such numbers are not used to directly identify an individual and hence	

		would not, on their own, be considered personal data. However, they may potentially be part of personal data relating to an individual when combined with other information. 2.6 Example: IMEI numbers The IMEI number refers to the unique number assigned to mobile devices such as mobile telephones. IMEI numbers are used to identify mobile devices in a network. As with any other network identifier such as an IP address, an IMEI number may not be personal data when viewed in isolation, because it simply identifies a network device. However, as each mobile device typically has a unique IMEI number, an IMEI number has the potential to form part of a set of data that in combination relates to an identifiable individual. For example, where a large number of unique data points are tagged to the same IMEI number such that an individual can be identified (such as through his surfing habits or location profile), then the IMEI number and the set of unique data points would be considered personal data of the individual.	
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		

#	Regulation	Data handlers
		Classification/ distinction by responsibility (data processor, data controller)/ size of data, (national security) critical services, etc.
		Provision on type of data handler

1	Personal Data Protection Act 2012	"organisation" includes any individual, company, association or body of persons, corporate or unincorporated, whether or not — (a) formed or recognised under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore; "data intermediary" means an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation; "prescribed healthcare body" means a healthcare body prescribed for the purposes of the Second Schedule by the Minister charged with the responsibility for health; "prescribed law enforcement agency" means an authority charged with the duty of investigating offences or charging offenders under written law, prescribed for the purposes of sections 21(4) and 26D(6) and the Second Schedule by the Minister charged with the responsibility for that authority; "public agency" includes — (a) the Government, including any ministry, department, agency, or organ of State; (b) any tribunal appointed under any written law; or (c) any statutory body specified under subsection (2);
2	Public Sector (Governance) Act 2018	
3	Telecommunications Act 1999	
4	CRIMINAL PROCEDURE CODE 2010	
5	Cybersecurity Act 2018	
6	Workplace Safety and Health (Medical Examinations) Regulations 2011	
7	Banking Act 1970	
8	PERSONAL DATA PROTECTION REGULATIONS 2021	
9	Personal Data Protection (Appeal) Regulations 2021	
10	Personal Data Protection (Composition of	

	Offences) Regulations 2021	
11	Personal Data Protection (Do Not Call Registry) Regulations 2013	
12	Personal Data Protection (Enforcement) Regulations 2021	
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021	
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015	
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014	
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020	
17	Personal Data Protection (Statutory Bodies) Notification 2013	
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment	
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems	

	Introduction to the Guidelines	
	Advisory Guidelines on Key Concepts in the Personal Data Protection Act	Organisations The PDPA defines an organisation as "any individual, company, association or body of persons, corporate or unincorporated whether or not formed or recognised under the law of Singapore; or resident, or having an office or a place of business, in Singapore". The term "organisation" broadly covers natural persons, corporate bodies (such as companies) and unincorporated bodies of persons (such as associations), regardless of whether they are formed or recognised under the law of Singapore or whether they are resident or have an office or place of business in Singapore. Every organisation is required to comply with the PDPA in respect of activities relating to the collection, use and disclosure of personal data in Singapore unless they fall within a category of organisations that is expressly excluded from the application of the PDPA. An organisation should ensure that it is able to adduce evidence to establish and demonstrate that it complied with the obligations under the PDPA in the event of an investigation. Although individuals are included in the definition of an organisation, they would generally not be required to comply with the PDPA if they fall within one of the excluded categories as elaborated below. Excluded organisations The PDPA provides that the Data Protection Provisions do not impose any obligations on the following entities. These categories of organisations are therefore excluded from the application of the Data Protection Provisions: a) Any individual acting in a personal or domestic capacity; b) Any employee acting in the course of his or her employment with an organisation; and c) Any public agency. In addition, organisations which are data intermediaries are partially excluded from the application of the Data Protection Provisions, as explained further below. Organisations which are not within an excluded category should note that they are required to comply with the PDPA when dealing with an organisation that is within an excluded category. Example: A travel agency collects personal data from Tom about his wife, Jane, when Tom books a travel package for a family holiday. Tom is not subject to the Data Protection Provisions as he is acting in a personal or domestic capacity. However, the travel agency must comply with all the Data Protection Provisions with regard to both Tom's and Jane's personal data, unless one or more exceptions apply. In this case, the travel agency can collect Jane's personal data without her consent as the exception in paragraph 8 under Part 3 of the First Schedule applies – that is, the travel agency does not need to seek Jane's consent because her personal data was provided by Tom to the travel agency to provide a service for Tom's personal and domestic purposes. However, the travel agency must comply with all its other obligations under the Data Protection Provisions, for

		example, adopting reasonable security arrangements to comply with the Protection Obligation in respect of Tom's and Jane's personal data. Individuals acting in a personal or domestic capacity Although individuals are included in the definition of an organisation, they benefit from two significant exclusions in the PDPA. The first is in relation to individuals who are acting in a personal or domestic capacity. Such individuals are not required to comply with the Data Protection Provisions. An individual acts in a personal capacity if he or she undertakes activities for his or her own purposes. The term "domestic" is defined in the PDPA as "related to home or family". Hence, an individual acts in a domestic capacity when undertaking activities for his home or family. Examples of such activities could include opening joint bank accounts between two or more family members or purchasing life insurance policies on one's child. Individuals acting as employees The second significant exclusion for individuals in the PDPA relates to employees who are acting in the course of their employment with an organisation. Employees are excluded from the application of the Data Protection Provisions. The PDPA defines an employee to include a volunteer. Hence, individuals who undertake work without an expectation of payment would fall within the exclusion for employees. Notwithstanding this exclusion for employees, organisations remain primarily responsible for the actions of the employees (including volunteers) which result in a contravention of the Data Protection Provisions. Public agencies The PDPA defines a public agency to include the following: a) the Government, including any ministry, department, agency, or organ of State; b) a tribunal appointed under any written law; or c) a statutory body specified by the Minister by notice in the Gazette2. Public agencies are excluded from the application of the Data Protection Provisions. Organisations that provide services to public agencies may either have obligations under the PDPA as data controllers or as data intermediaries. Data intermediaries The PDPA defines a data intermediary as "an organisation that processes personal data on behalf of another organisation but does not include an employee of that other organisation". In line with the exclusion for employees (noted above), a data intermediary does not include an employee. Obligations of data intermediaries The PDPA provides that a data intermediary that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will

		only be subject to the Data Protection Provisions relating to (a) protection of personal data (later referred to as the "Protection Obligation"); (b) retention of personal data (later referred to as the "Retention Limitation Obligation"); and (c) notifying the organisation of data breaches as part of notification of data breaches (later referred to as the "Data Breach Notification Obligation"), and not any of the other Data Protection Provisions. A data intermediary remains responsible for complying with all Data Protection Provisions in respect of other activities which do not constitute processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing. The term "processing" is defined in the PDPA as "the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following: a) recording; b) holding; c) organisation, adaptation or alteration; d) retrieval; e) combination; f) transmission; g) erasure or destruction." Items (a) to (g) above represent an indicative but non-exhaustive list of activities which could be considered processing. From the above list, it may be seen that activities which form part of processing by a data intermediary may also form part of collection, use or disclosure by the organisation on whose behalf they are acting. Please refer to the section below on "Collection, Use and Disclosure" for more details on this. As will be seen later, notwithstanding the partial exclusion for some data intermediaries, the PDPA provides that organisations shall have the same obligations under the PDPA in respect of personal data that is processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself. Considerations for organisations using data intermediaries Section 4(3) provides that an organisation has the same obligations under the PDPA in respect of personal data processed on its behalf by a data intermediary as if the personal data were processed by the organisation itself. As such, it is good practice for an organisation to undertake an appropriate level of due diligence to assure itself that a potential data intermediary is capable of complying with the PDPA. When engaging a data intermediary, an organisation should make clear in its contract the scope of work that the data intermediary is to perform on its behalf and for its purposes. For instance, if the organisation requires the data intermediary to process personal data on its behalf to respond to access or correction requests by individuals, the organisation should include contractual clauses to ensure that the data intermediary's scope of work and level of responsibilities are clear. The data intermediary has independent obligations to protect and cease retention of personal data that it has received for processing under the contract. Where a data breach is discovered by

		a data intermediary that is processing personal data on behalf and for the purposes of another organisation, the data intermediary is required to notify the organisation without undue delay from the time it has credible grounds to believe that the data breach has occurred. The organisation remains liable for any breach of the Data Protection Provisions for any processing by a data intermediary on its behalf and for its purposes3. Overseas transfers of personal data Where an organisation engages a data intermediary to process personal data on its behalf and for its purposes, the organisation is responsible for complying with the Transfer Limitation Obligation in respect of any overseas transfer of personal data. This is regardless of whether the personal data is transferred by the organisation to an overseas data intermediary or transferred overseas by the data intermediary in Singapore as part of its processing on behalf and for the purposes of the organisation. The Transfer Limitation Obligation requires that an organisation ensures that personal data transferred overseas is protected to a standard comparable with the Data Protection Provisions. The onus is on the transferring organisation to undertake appropriate due diligence and obtain assurances when engaging a data intermediary to ensure that it is capable of doing so. In undertaking its due diligence, transferring organisations may rely on data intermediaries' extant protection policies and practices, including their assurances of compliance with relevant industry standards or certification. Example: Company A uses a CRM cloud service that is offered by a service provider from the US. In using this service, Company A has to transfer personal data to the US. Company A must comply with the Transfer Limitation Obligation by ensuring that the service provider is able to afford adequate protection to the personal data transferred. Example: Company B uses a cloud storage solution ("CSS") offered by a service provider in Singapore. In providing this service, the CSS provider has to transfer personal data to its other servers in London and Hong Kong. As the CSS provider is carrying out this transfer on behalf of and for the purposes of Company B, Company B must comply with the Transfer Limitation Obligation. The CSS provider will nonetheless remain responsible for compliance with the Protection, Retention and Data Breach Notification (in relation to notifying Company B of data breaches without undue delay) Obligations in respect of the personal data that it transfers on behalf of and for the purposes of Company B. Determination of who the data intermediary is There is a diverse range of scenarios in which organisations may be considered data intermediaries for another organisation. An organisation may be a data intermediary of another even if the written contract between the organisations does not clearly identify the data intermediary as such. The PDPA's definition of "data intermediary"

		would apply in respect of all organisations that process personal data on behalf of another. Hence it is very important that an organisation is clear as to its rights and obligations when dealing with another organisation and, where appropriate, include provisions in their written contracts to clearly set out each organisation's responsibilities and liabilities in relation to the personal data in question including whether one organisation is to process personal data on behalf of and for the purposes of the other organisation. If Organisation A engages Organisation B to provide services relating to any processing of personal data on behalf of A and for A's purposes, then B may be considered a data intermediary of A in relation to the processing of such personal data. In such a case, A should ensure that its written contract with B clearly specifies B's obligations and responsibilities in order to ensure its own compliance with the PDPA. It is important to note that if B uses or discloses personal data in a manner which goes beyond the processing required by A under the contract, then B will not be considered a data intermediary in respect of such use or disclosure. Since B has exercised its own judgement in determining the purpose and manner of such use and disclosure of the personal data, B will be required to comply with all Data Protection Provisions. In the situation where two or more organisations ("Organisations A and B") engage an organisation ("Organisation C") for the processing of personal data on behalf of and for the purposes of Organisations A and B, then Organisation C may be considered to be both Organisations A's and B's data intermediary in relation to such processing. Organisations A and B are both responsible for compliance with the Data Protection Provisions in relation to the personal data processed on their behalf. Where Organisation B is a data intermediary of Organisation A, Organisation A is responsible for the personal data collected, used and disclosed by B regardless of whether such personal data was actually transmitted to A, for example, personal data of prospective clients of A that may only reside with B. Example: Organisation ABC is a market research firm that has been engaged by Organisation XYZ. The written contract specifies that ABC has been engaged to collect personal data on behalf of XYZ and produce a report, exclusively for the use of XYZ, which illustrates the correlation between investment habits and income, profession and marital status of at least 1,000 working Singaporeans aged 25 – 40. In addition to types of investments made, income, profession and marital status, the contract specifies that ABC has to collect the telephone number and residential address of each person surveyed. The contract neither specifies the methods or processes ABC should undertake to collect the data and produce the report, nor the specific individuals that ABC are to survey. However, all raw data collected are to be given to XYZ and ABC is not permitted to keep any copies of the data or use it for any other purpose. In this situation, ABC may still be considered a data intermediary of XYZ insofar as it is processing personal data for the sole purpose of producing the

		report for XYZ. As ABC is XYZ's data intermediary, XYZ has the same obligations under the PDPA in respect of the personal data processed by ABC. Hence, XYZ may wish to include additional requirements in its contract to ensure that ABC fulfils XYZ's obligations under the PDPA. Example: Organisation XYZ provides courier services. Organisation ABC engages XYZ to deliver a parcel and signs a contract with XYZ for delivery of the parcel. ABC provides XYZ with the name, address and telephone number of the person to whom the parcel is to be delivered. In this case, XYZ will be considered ABC's data intermediary under the PDPA as it is processing personal data on behalf of ABC. Insofar as XYZ is processing the intended recipient's personal data on behalf of and for the purposes of ABC pursuant to the written contract between XYZ and ABC, XYZ will only be subject to the provisions in the PDPA relating to the Protection, Retention Limitation and Data Breach Notification (in relation to notifying ABC of data breaches without undue delay) Obligations in respect of such personal data. It is possible for an organisation that is part of a corporate group of organisations to act as a data intermediary for other members of the group. Example: Organisation XYZ undertakes payroll administration for a number of organisations, including organisations that belong to the same corporate group to which XYZ belongs. XYZ holds records of such organisations' employees, such as the employees' full names, duration of employment, salary and bank account numbers. XYZ processes such personal data solely for the purpose of payroll administration pursuant to instructions contained within its written contracts with these other organisations. Hence, XYZ is considered a data intermediary for these other organisations in relation to its processing of such personal data. An organisation can be considered a data intermediary in respect of a set of personal data while at the same time be bound by all Data Protection Provisions in relation to other sets of personal data. Example: In the example above, XYZ is a data intermediary in relation to its processing of personal data of the employees of other organisations for payroll administration purposes. However, in respect of the personal data of XYZ's own employees, XYZ is not a data intermediary, and it is required to comply with all the Data Protection Provisions. XYZ holds records of such organisations' employees, such as the employees' full names, salary and bank account numbers. XYZ does not take reasonable security arrangements to ensure that those records are secure, and unauthorised disclosure occurs to one of XYZ's employees. XYZ may be liable under the Protection Obligation for failing to protect personal data in its possession or control through the provision of reasonable security arrangements. In relation to network service providers, the Commission notes

		previous industry feedback clarifying the liabilities of network service providers that merely act as conduits for the transmission of personal data and highlights that section 67(2) of the PDPA amends the Electronic Transactions Act ("ETA") such that network service providers will not be liable under the PDPA in respect of third party material in the form of electronic records to which it merely provides access. Under the ETA, such access includes the automatic and temporary storage of the third party material for the purpose of providing access. "Agents" who may be data intermediaries Generally, the legal relationship of agency refers to a relationship that exists between two persons, an agent and a principal. An agent is considered in law to represent the principal, in such a way so as to be able to affect the principal's legal position in respect of contracts and certain other dealings with third parties, so long as the agent is acting within the scope of his authority ("legal definition of "agent""). Persons that carry the title of "agent" (e.g. "Insurance agent" or "Property agent") can fall within or outside the "legal definition of agent" depending on the particular circumstances at hand. Whether a person is an "agent" does not depend on whether he uses the title "agent" as part of his job title, e.g. a "sales agent", but on whether he is acting on behalf of the other person in a particular matter or transaction. Persons who fall within the "legal definition of agent" or who carry the title of "agent" have to comply with all obligations in the PDPA except to the extent that it is processing personal data on behalf of and for purposes of another organisation pursuant to a contract which is evidenced or made in writing (i.e. they are considered to be data intermediaries for another organisation). In short, there is no difference in how an agent or any other organisation is treated under the PDPA in relation to whether they qualify as a data intermediary. As good practice, organisations should ensure that their agents are made aware of and exercise proper data protection practices in relation to the handling of personal data.
	Advisory Guidelines on the Personal Data Protection Act for Selected Topics	
	Advisory Guidelines on Enforcement of Data Protection Provisions	
	Joint Advisory on ALTDOS	
	Advisory Guidelines on the Do Not Call Provisions	PART V: DEFINITION OF SENDER Overview of Part V This Part relates to what constitutes sending a message to a Singapore telephone number, who is a "sender" who is responsible for complying with the DNC Provisions as defined in section 36(1) of

		the PDPA, and the exclusions as provided under section 36 (2) and (3). Clarity is also provided for senders of specified messages in a joint offering scenario. Sending a specified message to a Singapore telephone number It is important to understand what constitutes the sending of a message to a Singapore telephone number under the PDPA, as this goes towards determining whether the DNC Provisions apply. Section 36(1) of the PDPA defines the term "send" as referring to: a) the sending of the message; b) causing or authorising the sending of the message; or c) the making of a voice call containing the message, or causing or authorising the making of such a voice call24. Related to the above, the PDPA provides that a message may be sent in different forms. Hence, section 36(1) of the PDPA defines "message" to include a message in sound, text, visual or other form. From the above definitions, it is important to note that the DNC Provisions apply equally to all means by which a sender may send a specified message to a Singapore telephone number. These include, for example, voice calls, SMS, or any data applications (such as 'Whatsapp', 'iMessage' or 'Viber') which use a Singapore telephone number. However, the DNC Provisions do not apply to specified messages which are not sent to a Singapore telephone number, e.g. location-based broadcasts that are pushed to mobile phones through data-enabled smart phone applications or data applications that do not use a Singapore telephone number to send messages. For the avoidance of doubt, the DP Provisions may still apply to such specified messages which are not sent to a Singapore telephone number. Meaning of "sender" The DNC Provisions contain obligations in relation to the sending of a specified message. Hence a person who sends a message, referred to in the PDPA as the "sender", is responsible for complying with the DNC Provisions. In brief, the term "sender" is defined in section 36(1) of the PDPA as follows: a) the person who actually sends the message or makes a voice call containing the message; b) the person who causes the message to be sent or the voice call to be made; and c) the person who authorises the sending of the message or the making of the call. Hence it is important to note that in addition to the person who actually sent the message or made the call containing the message, persons who caused or authorized the sending of the message or the making of the call are also senders for the purposes of the DNC Provisions and must comply with these provisions. This means that if Person A authorises the sending of the message by Person B, Person A would be considered a sender. Section 37 (3) and (4) of the PDPA clarifies when a person is considered to have authorised another to send a message. These

		provisions state: Subject to subsection (4), a person who authorises another person to offer, advertise or promote the first person's goods, services, land, interest or opportunity shall be deemed to have authorised the sending of any message sent by the second person that offers, advertises or promotes that first person's goods, services, land, interest or opportunity. For the purposes of subsection (3), a person who takes reasonable steps to stop the sending of any message referred to in that subsection shall be deemed not to have authorised the sending of the message. Under section 37 (3) and (4), if Person A authorises Person B to promote his goods, services, land, interest or opportunity, Person A would be deemed to have authorised the sending of any message for that purpose, unless Person A had taken reasonable steps to prevent Person B from doing so. The determination of whether reasonable steps had been taken depends on the specific facts in question. For example, reasonable steps may include requiring, as a condition of the authorisation given, that Person B shall not promote Person A's goods by sending specified messages addressed to Singapore telephone numbers. A person should note that he would be subject to the DNC Provisions if he falls within the definition of a "sender", even if the message was sent on behalf of or for another person's purposes.
	Advisory Guidelines on Application of PDPA to Election Activities	
	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers	
	Advisory Guidelines on Requiring Consent for Marketing Purposes	
	Advisory Guidelines for Management Corporations	2.1 A MCST comprises the subsidiary proprietors of all lots within the specific strata title plan (an "estate"), which could be residential buildings such as apartments and condominiums, or commercial buildings such as shopping malls, offices and medical centres. Accordingly, a MCST is considered an organisation6 under the PDPA. Managing agent as data intermediary 2.5 MCSTs may appoint managing agents to carry out one or more of its duties or functions. Given that managing agents may process

		personal data on behalf of MCSTs, managing agents may be considered data intermediaries14 in relation to the personal data that they process on behalf of the MCSTs. A data intermediary that processes personal data pursuant to a written contract15 will only be subject to the Protection Obligation and Retention Limitation Obligation of the Data Protection Provisions. The organisation for which the personal data is processed (i.e. the MCST) remains responsible for complying with all the Data Protection Provisions. Accordingly, as a good practice, MCSTs should ensure that it undertakes the necessary due diligence to assure itself that a potential managing agent is capable of complying with the PDPA, and enter into suitable data processing agreements with such managing agent if it contemplates such managing agent to undertake data processing functions on its behalf. Data intermediaries are responsible for complying with all the Data Protection Provisions in respect of other activities which do not constitute the processing of personal data on behalf of and for the purposes of another organisation.
	Advisory Guidelines for the Education Sector	
	Advisory Guidelines for the Social Service Sector	10 Organisations and Data Intermediaries 10.1 Generally, organisations20 that SSAs typically work with (such as sponsors, donors or service providers) will also be subject to the Data Protection Obligations, unless they fall within a category of organisations that is expressly excluded. For example, organisations which are data intermediaries are partially excluded from the application of the Data Protection Provisions, as explained further below. 10.2 A data intermediary is an organisation that processes personal data on behalf of another organisation, but excludes an employee of that other organisation. In some situations, SSAs may engage data intermediaries to process personal data. The PDPA provides that a data intermediary that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will only be subject to the Protection Obligation, Retention Limitation Obligation and the Data Breach Notification Obligation, and not any of the other Data Protection Provisions. 10.3 A data intermediary remains responsible for complying with all Data Protection Provisions in respect of other activities that do not constitute processing of personal data on behalf of and for the purposes of another organisation that is pursuant to a contract evidenced or made in writing. 10.4 In any case, under section 4(3) of the PDPA, the organisation that engages the data intermediary would still have the same obligations under the PDPA in respect of personal data processed on its behalf as if the personal data were processed by the organisation itself. 10.5 SSAs should note that whether an organisation charges a SSA for its services generally does not affect whether that organisation is

		a data intermediary of the SSA. Please refer to Chapter 6 of the Key Concepts Guidelines for more information on when an organisation is considered a data intermediary, as well as the obligations applicable to data intermediaries and the organisations that engage data intermediaries, under the PDPA. 10.6 Example: Engaging a data intermediary to manage payroll Company 789, which is owned by one of SSA GHI's Board Members, provides probono services to process the payroll for all employees working in SSA GHI's various centres in Singapore. Company 789 holds records of SSA GHI's employees such as their full names, NRIC numbers, duration of employment, salary and bank account details. Company 789 is processing the personal data solely for the purposes of payroll administration pursuant to a written agreement with SSA GHI. Treatment In this case, Company 789 is considered a data intermediary processing personal data on behalf of and for the purposes of SSA GHI pursuant to a contract evidenced or made in writing. The fact that Company 789 does not charge SSA GHI for its services does not affect Company 789's status. Company 789 will be subject only to the Protection Obligation, Retention Limitation Obligation, and Data Breach Notification Obligation under the PDPA in respect of such processing, while SSA GHI will have the same obligations under the PDPA in respect of the personal data of SSA GHI's employees processed on its behalf by Company 789, as if the personal data were processed by SSA GHI itself. 10.7 Example: Engaging a data intermediary to host personal data on cloud SSA 123 engages Company ABC, based in Singapore, to develop a HR management system for its employees. This system utilizes a cloud storage solution, provided and administered by Company ABC, for the storage of data. After development, SSA 123 stores its employees' personal data, such as their full names, NRIC numbers, salary and bank account details, on the HR management system. Company ABC provides these services, including the cloud storage solution, to SSA 123 pursuant to a written agreement between both parties. Treatment In this case, Company ABC is considered a data intermediary processing personal data on behalf of and for the purposes of SSA 123 pursuant to a contract evidenced or made in writing.21 Company ABC will be subject only to the Protection Obligation, Retention Limitation Obligation, and Data Breach Notification Obligation under the PDPA in respect of such processing, while SSA 123 will have the same obligations under the PDPA in respect of the personal data of their employees processed on its behalf by Company ABC, as if the personal data were processed by SSA 123 itself. To comply with the Protection Obligation, Company ABC can ensure that the cloud storage solution has industry standards like ISO27001, the ability to produce technical audit reports such as the

		SOC-2 upon request and Tier 3 of the Multi-Tiered Cloud Security ("MTCS") Certification Scheme. In particular, SSA 123 must comply with the Transfer Limitation Obligation if, in providing the cloud storage service, Company ABC has to transfer the personal data to its servers located overseas. SSA 123 may do so by ensuring that the cloud storage solution utilised by Company ABC accords a comparable standard of protection to the transferred personal data. One option is for SSA 123 to ensure that Company ABC uses a cloud storage solution that has legally enforceable obligations. For example, the cloud storage solution is certified under the APEC CBPR system in the overseas country, which will ensure that the clients' personal data stored in the overseas data centres are protected to a standard comparable to the PDPA. SSA 124 and Company ABC can refer to the list of CBPR-certified organisations on the APEC website (www.cbprs.org).22
	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire	
	Advisory Guidelines for the Real Estate Agency Sector	Organisations and Data Intermediaries 3.10 If salespersons are not employees of the estate agents that they represent, they may not fall within the exclusion from the Data Protection Provisions for employees acting in the course of their employment. In such cases, salespersons may instead be considered separate organisations from estate agents and would be required to comply with the Data Protection Provisions as if they were separate organisations from the estate agents they represent. 3.11 The PDPA does, however, provide that a data intermediary13 that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will only be subject to the Protection Obligation and Retention Limitation Obligation and not any of the other Data Protection Provisions. 3.12 A data intermediary remains responsible for complying with all Data Protection Provisions in respect of other activities that do not constitute processing of personal data on behalf of and for the purposes of another organisation that is pursuant to a contract evidenced or made in writing. 3.13 In any case, under section 4(3) of the PDPA, the organisation that engages the data intermediary would still have the same obligations under the PDPA in respect of personal data processed on its behalf as if the personal data were processed by the organisation itself. 3.14 For the real estate agency sector, whether a salesperson may be considered a data intermediary of an estate agent depends largely on the working arrangements14 between the salesperson and the estate agent. 3.15 Please refer to the Key Concepts Guidelines for a discussion on the criteria for and obligations of data intermediaries. 3.16 Example: Whether a salesperson is a data intermediary

		processing personal data on behalf of and for purposes of an estate agent pursuant to a contract evidenced or made in writing Jack intends to sell his apartment and informs Sarah, a salesperson with estate agent ABC, that he wishes to engage estate agent ABC to market his apartment to potential buyers. Pursuant to her agreement signed with estate agent ABC, Sarah provides Jack a copy of the estate agency agreement and delivers the completed agreement (which includes personal data such as Jack's full name, NRIC and address) to estate agent ABC. In this scenario, Sarah is considered to be a data intermediary processing personal data on behalf of and for the purposes of ABC pursuant to a contract made in writing and will not be subject to the other Data Protection Provisions other than the Protection Obligation and Retention Limitation Obligation. ABC will have the same obligations under the PDPA in respect of the personal data processed on its behalf by Sarah, as if the personal data were processed by ABC itself. 3.17 Boris, a salesperson with estate agent DEF, uses personal data of his clients who purchased property in a particular neighbourhood to create a profile of prospective clients that may be interested in properties in that neighbourhood for his own use. Such activities fall outside the scope of the activities that Boris is to carry out on behalf of DEF. In this case, Boris is not considered to be a data intermediary processing personal data on behalf of and for the purposes of DEF pursuant to a contract made in writing. 3.18 There are several obligations within the Data Protection Provisions which require organisations to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. Organisations are required to make the information about their data protection policies available. For more information, please refer to the latest Key Concepts Guidelines and the latest Advisory Guidelines on the PDPA for Selected Topics.
	Advisory Guidelines for the Healthcare Sector	
	Advisory Guidelines for the Telecommunication Sector	
	Joint Technical Advisory on LockBit 3.0	
	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore	

	Personal Data Protection Act	

Legal basis

#	Regulation		
		consent	necessary for the performance of a contract
1	Personal Data Protection Act 2012	Consent required 13. An organisation must not, on or after 2 July 2014, collect, use or disclose personal data about an individual unless — (a) the individual gives, or is deemed to have given, his or her consent under this Act to the collection, use or disclosure, as the case may be; or	Deemed consent 15.—(1) An individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation for a purpose if — (a) the individual, without actually giving consent mentioned in section 14, voluntarily provides the personal data to the organisation for that purpose; and (b) it is reasonable that the individual would voluntarily provide the data. (2) If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organisation to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation. (3) Without limiting subsection (2) and subject to subsection (9), an individual (P) who provides personal data to an organisation (A) with a view to P entering into a contract with A is deemed to consent to the following where reasonably necessary for the conclusion of the contract between P and A: (a) the disclosure of that personal data by A to another organisation (B); (b) the collection and use of that personal data by B;

			(c) the disclosure of that personal data by B to another organisation. [40/2020] (4) Where an organisation collects personal data disclosed to it by B under subsection (3)(c), subsection (3)(b) and (c) applies to the organisation as if the personal data were disclosed by A to the organisation under subsection (3)(a). [40/2020] (5) Subsections (3) and (4) apply to personal data provided before 1 February 2021 by an individual to an organisation with a view to the individual entering into a contract with the organisation — (a) on or after 1 February 2021; or (b) which contract was entered into before 1 February 2021 and remains in force on that date, as if subsections (3) and (4) — (c) were in force when the personal data was so provided; and (d) had continued in force until 1 February 2021. [40/2020] (6) Without limiting subsection (2) and subject to subsection (9), an individual (P) who enters into a contract with an organisation (A) and provides personal data to A pursuant or in relation to that contract is deemed to consent to the following: (a) the disclosure of that personal data by A to another organisation (B), where the disclosure is reasonably necessary — (i) for the performance of the contract between P and A; or (ii) for the conclusion or performance of a contract between A and B which is entered into at P's request, or which a reasonable person

			would consider to be in P's interest; (b) the collection and use of that personal data by B, where the collection and use are reasonably necessary for any purpose mentioned in paragraph (a); (c) the disclosure of that personal data by B to another organisation, where the disclosure is reasonably necessary for any purpose mentioned in paragraph (a). [40/2020] (7) Where an organisation collects personal data disclosed to it by B under subsection (6)(c), subsection (6)(b) and (c) applies to the organisation as if the personal data were disclosed by A to the organisation under subsection (6)(a). [40/2020] (8) Subsections (6) and (7) apply to personal data provided before 1 February 2021 by an individual to an organisation in relation to a contract that the individual entered into before that date with the organisation, and which remains in force on that date, as if subsections (6) and (7) — (a) were in force when the personal data was so provided; and (b) had continued in force until 1 February 2021. [40/2020] (9) Subsections (3), (4), (5), (6), (7) and (8) do not affect any obligation under the contract between P and A that specifies or restricts — (a) the personal data provided by P that A may disclose to another organisation; or (b) the purposes for which A may disclose the personal data provided by P to another organisation.

			[40/2020] Deemed consent by notification 15A.—(1) This section applies to the collection, use or disclosure of personal data about an individual by an organisation on or after 1 February 2021. [40/2020] (2) Subject to subsection (3), an individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation if — (a) the organisation satisfies the requirements in subsection (4); and (b) the individual does not notify the organisation, before the expiry of the period mentioned in subsection (4)(b)(iii), that the individual does not consent to the proposed collection, use or disclosure of the personal data by the organisation. [40/2020] (3) Subsection (2) does not apply to the collection, use or disclosure of personal data about the individual for any prescribed purpose. [40/2020] (4) For the purposes of subsection (2)(a), the organisation must, before collecting, using or disclosing any personal data about the individual — (a) conduct an assessment to determine that the proposed collection, use or disclosure of the pe
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		

5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		

17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment	Giving valid consent under the PDPA Section 13 of the PDPA provides that organisations are allowed to collect, use, or disclose an individual's personal data if the individual gives his or her consent for the collection, use, or disclosure of it. 4.2 The PDPC considers that a child between 13 and 17 may give valid consent, when the policies on the collection, use and disclosure of the child's personal data, as well as the withdrawal of consent, are readily understandable by them. This includes ensuring that the child understand the consequences of providing and withdrawing consent. However, where an organisation has reason to believe that a child does not have sufficient understanding of the nature and consequences of giving consent, the organisation should obtain consent from the child's parent or guardian. 4.3 There may be instances where an organisation will consider a higher age of consent more appropriate in its business context. For example, an organisation in an education setting may assess that it is more prudent to obtain consent from a parent of a 13-year-old rather than to directly seek the consent of a 13-year-old. In such cases, the organisation should proceed to do so. 4.4 Organisations should also ensure that children are able to withdraw consent for their personal data as easily as providing consent for their	

		personal data. 4.5 Where the child is below 13 years of age, the organisation must obtain consent from the child's parent or guardian5. The parent or guardian should be notified of the purpose(s) for which the child's personal data will be collected, used, and disclosed. 4.6 The PDPC considers consent that was previously obtained from an individual (or parent / legal guardian) when he / she was a child to remain valid when the individual reaches 18 years of age.	
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems	9 Consent and Notification Obligations 9.1 Unless deemed consent or exceptions to the Consent Obligation apply, e.g., Legitimate Interests Exception, pursuant to Section 13 of the PDPA, consent will be required for the collection and use of personal data to provide recommendations, predictions, or decisions. This is referred to as the Consent Obligation. 9.2 The Consent Obligation is complemented by the Notification Obligation, which requires that users be notified of the purpose of the collection and intended use of their personal data when seeking their consent. Section 20 of the PDPA sets out organisations' obligations to inform individuals of the purposes for which their personal data is collected, used, and disclosed. Among other things, Section 20(1) requires an organisation to inform the individual of: a) The purposes for the collection, use and disclosure of their personal data, on or before collecting the personal data; or b) Any purpose for the use or disclosure of personal data	

		which has not been informed under sub-paragraph(a) above before such use or disclosure of personal data for that purpose. 9.3 As set out in the Advisory Guidelines on Key Concepts in the PDPA, consent should be meaningful, and Notification requires giving individuals information about the types of personal data that will be collected and processed and the purpose for the processing, e.g., to recommend books, songs, or movies. 9.4 The raison d'etre for the Consent and Notification Obligations is to enable individuals to provide meaningful consent. Organisations should place themselves in the shoes of consumers and craft notifications that will enable individuals to understand how personal data will be processed to achieve the intended purpose. Notifications need not be overly technical or detailed and should be proportionate to the risks of each use-case, e.g., taking into account potential harm to the individual and the level of autonomy of the AI System. 9.5 Organisations are encouraged to provide information on the following, to the extent practicable, in crafting notifications: a) The function of their product that requires collection and processing of personal data (e.g., recommendation of movies); b) A general description of types of personal data that will be collected and processed (e.g., movie viewing history); c) Explain how the processing of personal data collected is relevant to the product feature (e.g., analysis of users' viewing history to make movie	

		recommendations); and d) Identify specific features of personal data that are more likely to influence the product feature (e.g., whether movie was viewed completely, viewed multiple times, etc). 9.6 The provision of such information could be through notification pop-ups or included in more detailed written policies that are publicly accessible or made available to end users on request. Organisations should decide the mode of providing such information, based on their own assessment of how this supports their business objectives vis-à-vis user experience. Example: A bank uses AI to assist in credit scoring when assessing whether to approve applications for credit cards. It prepared a policy document entitled "Bank's Credit Assessment Policy Statement" which provides information about what personal data it collects from applicants and how they are processed by AI when the bank assesses applications. The policy document is provided to applicants who request for the information. Example: An organisation provides personalised recommendations for content to an individual on its online social media platform. To provide information to individuals as to why specific content is shown to them, the organisation has provided a pop up containing a link to a page to explain why this content is shown and ranked highly on the content feed for the user. The page includes information on why that content is shown, what information has the largest influence over the order of posts in the user's	

		content feed, such as past interactions or membership in specific groups on the platform etc. 9.7 It may also be useful to consider "layering" information. This means displaying the most relevant information more prominently and providing more details elsewhere. For example, notification pop-ups could provide a link to publicly accessible privacy policies; additionally, privacy policies may be structured to have details organised in expanding sections or separate tabs. The Commission recognises that industry is also developing disclosure best practices, such as model cards and system cards15. Information necessary to meet the Consent and Notification Obligations may also be provided through such model and/or system cards, if the organisation adopts this practice or assesses it to be useful. Example: An organisation provides a video streaming service. It informs users that its service uses AI to provide recommendations. Through its notification pop-up, it informs users that it collects and analyses users' declaration of topics of interest, browsing activities and media consumption data to recommend videos that users may be interested in. Users are provided the option to consent or decline the use of this feature. The notification pop-up contains a link to its privacy policy, which contains a section that provides information about what declared topics of interest, browsing activity and media consumption data are collected and analysed. This includes the topic	

		classification of videos that users watch, duration and proportion of the video that is played, how many times the video is played, whether the video is watched in a preview window or in actual size, etc. The organisation also explains that the topics of videos that users watch in full are most likely to influence future recommendations. Example: A social media platform provides an AI system card to its users to explain how its AI System uses user activity data to generate recommendations for its content feed. The system card contains a step-by-step walk through on how the AI System gathers user activity data and broadly processes it in its AI System with other parameters to generate personalised output for a content feed. 9.8 Notwithstanding the above, the Commission recognises that organisations may need to protect commercially sensitive and/or proprietary information, as well as the security of AI Systems. Where organisations assess that it is necessary to limit or omit detail and, if appropriate, provide a more general explanation instead, it is good practice for these decisions to be justified and documented clearly internally. Legitimate Interests Exception 9.9 "Legitimate Interests" generally refer to any lawful interests of an organisation or other person (including other organisations). Paragraphs 2 to 10 under Part 3 of the First Schedule to the PDPA relate to specific purposes that would be considered "Legitimate Interests", e.g., evaluative purposes; for managing or	

		terminating an employment relationship. To rely on this exception, organisations must assess and ensure that the legitimate interests outweigh any adverse effect. 9.10 An example of a Legitimate Interest for processing personal data without consent would be the use of personal data as input in an AI System for the purposes of detecting or preventing illegal activities. 9.11 Organisations may wish to refer to the Commission's Advisory Guideline on Key Concepts in the PDPA for guidance on how to make an adverse effect assessment. Organisations who rely on this exception must make it known to individuals that they are relying on this exception to collect and use personal data.	
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act	PART III: THE DATA PROTECTION PROVISIONS Overview of the Data Protection Provisions Organisations are required to comply with the Data Protection Provisions in Parts 3 to 6A of the PDPA. When considering what they should do to comply with the Data Protection Provisions, organisations should note that they are responsible for personal data in their possession or under their control4. In addition, when an organisation employs a data intermediary to process personal data on its behalf and for its purposes, organisations have the same obligations under the PDPA as if the personal data were processed by the organisation itself5. Broadly speaking, the Data Protection Provisions contain ten main obligations which	

		organisations are required to comply with if they undertake activities relating to the collection, use or disclosure of personal data. These obligations may be summarised as follows. The sections of the PDPA which set out these obligations are noted below for reference. a) The Consent Obligation (PDPA sections 13 to 17): An organisation must obtain the consent of the individual before collecting, using or disclosing his personal data for a purpose. b) The Purpose Limitation Obligation (PDPA section 18): An organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, have been notified to the individual concerned. c) The Notification Obligation (PDPA section 20): An organisation must notify the individual of the purpose(s) for which it intends to collect, use or disclose the individual's personal data on or before such collection, use or disclosure of the personal data. d) The Access and Correction Obligations (PDPA sections 21, 22 and 22A): An organisation must, upon request, (i) provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year; and (ii) correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation. e) The Accuracy Obligation (PDPA section 23): An	

		organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be used by the organisation to make a decision that affects the individual concerned or disclosed by the organisation to another organisation. f) The Protection Obligation (PDPA section 24): An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent (i) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (ii) the loss of any storage medium or device on which personal data is stored. g) The Retention Limitation Obligation (PDPA section 25): An organisation must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that (i) the purpose for which the personal data was collected is no longer being served by retention of the personal data; and (ii) retention is no longer necessary for legal or business purposes. h) The Transfer Limitation Obligation (PDPA section 26): An organisation must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA. i) The Data Breach Notification Obligation (PDPA sections 26A to 26E): An organisation must assess whether a data breach is notifiable and notify the affected	

		individuals and/or the Commission where it is assessed to be notifiable. j) The Accountability Obligation (PDPA sections 11 and 12): An organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available. Some of the ten obligations mentioned above may have other related requirements which organisations must comply with. In addition, some of the ten obligations are subject to exceptions or limitations specified in the PDPA. The following sections of these Guidelines consider each of the above obligations in greater detail, together with the additional requirements and exceptions or limitations that may apply. The Consent Obligation The PDPA recognises that organisations need to collect, use and disclose personal data for reasonable purposes7 that are articulated in the PDPA through deemed consent and exceptions to the consent obligation. For all other purposes, section 13 of the PDPA provides that organisations are allowed to collect, use or disclose an individual's personal data if the individual gives his consent for the collection, use or disclosure of his personal data. This obligation to obtain the individual's consent is referred to in these Guidelines as the Consent Obligation. This obligation does not apply where the collection, use or disclosure of an individual's personal data is required or	

		authorised under the PDPA or any other written law. However, organisations may still need to comply with other requirements of the Data Protection Provisions. Please refer to Annex A for further information on the framework for the collection, use or disclosure of personal data, to obtain consent in a way that is meaningful to individuals. Obtaining consent from an individual Section 14(1) of the PDPA states how an individual gives consent under the PDPA. An individual has not given consent unless the individual has been notified of the purposes for which his personal data will be collected, used or disclosed and the individual has provided his consent for those purposes. If an organisation fails to do so, any consent obtained from the individual would be invalid. Consent can be obtained in several ways. Consent that is obtained in writing or recorded in a manner that is accessible is referred to in these Guidelines as 'express consent'. Such consent provides the clearest indication that the individual has consented to notified purposes of the collection, use or disclosure of his personal data. In situations where it may be impractical for the organisation to obtain express consent in writing, it may choose to obtain verbal consent. As good practice, organisations can consider adopting the following practices in cases when consent is obtained verbally, to prove that verbal consent had been given, in the event of disputes: a) Confirm the consent in writing with the individual (which may be in electronic form or other form of documentary evidence); or	

		b) Where appropriate in the circumstances, make a written note (which may be in electronic form or other form of documentary evidence) of the fact that an individual had provided verbal consent. Example: Written consent after signing up for services over the telephone An individual wishes to sign up for certain services with a service provider over the telephone. The service provider may request the individual's consent for the collection and use of his personal data for the service provider's purposes and obtain the personal data from the individual over the telephone. It would be good practice for the service provider to subsequently contact the individual and confirm his consent in writing. For example, by sending an email to the individual setting out the description of the personal data provided by the individual, and recording his consent to the collection, use and disclosure by the service provider for the service provider's purposes (which may be set out in its terms and conditions and/or other information provided in the email). Depending on the facts in some cases, the Commission may consider that consent is inferred or implied from the circumstances or the conduct of the individual in question. This is a form of consent where the individual does, in fact, consent to the collection, use and disclosure of his personal data (as the case may be) by his conduct, although he has not expressly stated his consent in written or verbal form8. Organisations that wish to rely on the individual's consent to	

		send specified messages to Singapore telephone numbers should ensure that the individual has given clear and unambiguous consent beforehand. Consent for the sending of specified messages to Singapore telephone numbers should be evidenced in written or other accessible form. For this purpose, verbal consent alone would be insufficient. Obtaining consent from a person validly acting on behalf of an individual Section 14(4) of the PDPA provides that consent may be given, or deemed to have been given, by any person validly acting on behalf of the individual for the collection, use or disclosure of the individual's personal data. Regulations issued under the PDPA will also provide for some specific situations in which an individual person may give consent on behalf of another. In order to obtain consent from a person validly acting on behalf of an individual, the person would similarly have to be notified of the purposes for which the individual's personal data will be collected, used and disclosed and the person must have given consent for those purposes on behalf of the individual. The following sections elaborate on when consent is not validly given and deemed consent would also apply. When consent is not validly given Section 14(2) of the PDPA sets out additional obligations that organisations must comply with when obtaining consent. This subsection provides that an organisation providing a product or service to an individual must not, as a condition of providing the product or service, require	

		the individual to consent to the collection, use or disclosure of his personal data beyond what is reasonable to provide the product or service. The subsection also prohibits organisations from obtaining or attempting to obtain consent by providing false or misleading information or using deceptive or misleading practices. Section 14(3) provides that any consent obtained in such circumstances is not valid. Hence an organisation may not rely on such consent, and if it collects, uses or discloses personal data in such circumstances, it would have failed to comply with the Consent Obligation. For the avoidance of doubt, organisations may collect, use or disclose personal data for purposes beyond those that are reasonable for providing the product or service to the individual by obtaining the individual's consent in accordance with the PDPA, so long as organisations do not make it a condition of providing the product or service. Example: Sarah wants to sign up for a spa package. The terms and conditions include a provision that the spa may share her personal data with third parties, including selling her personal data to third party marketing agencies. Sarah does not wish to consent to such a disclosure of her personal data and requests the spa not to disclose her personal data to third party marketing agencies. The spa refuses to act on her request and informs her that the terms and conditions are standard, and that all customers must agree to all the terms and conditions. Sarah	

		is left either with the choice of accepting all the terms and conditions (i.e. giving consent for use and disclosure of her data as described) or not proceeding with the sign up. In this case, even if Sarah consents to the disclosure of her data to third party marketing agencies, the consent would not be considered valid since it is beyond what is reasonable for the provision of the spa's services to its customers, and the spa had required Sarah's consent as a condition for providing its services. Instead of requiring Sarah to consent to the disclosure and sale of her personal data to third parties as a condition of providing the service, the spa should separately request Sarah's consent to do so. That is, Sarah should be able to sign up for the spa package without having to consent to the disclosure and sale of her personal data to third parties. The spa is then free to ask Sarah if she would consent, and if she does, would be considered to have obtained valid consent. Section 14(2)(a) may not prohibit certain situations in which an organisation may seek to require consent. For example, organisations may provide offers, discounts or lucky draw opportunities to individuals that are conditional on the collection, use or disclosure of their personal data for specified purposes. In any event, organisations are reminded that their practices would be subject to other requirements of the Data Protection Provisions including, in particular, the requirement that the organisation's	

		purposes must be what a reasonable person would consider appropriate in the circumstances. When collecting personal data through a form, it is good practice for organisations to indicate which fields that collect personal data are compulsory and which are optional, and to state the purposes for which such personal data will be collected, used and/or disclosed. It follows from section 14(2)(a) that an organisation may require an individual to consent to the collection, use or disclosure of his personal data as a condition of providing a product or service where it is reasonably required in order to provide the product or service. For more information on requiring consent for the collection, use or disclosure of personal data for marketing purposes, please refer to the Advisory Guidelines on Requiring Consent for Marketing Purposes. In particular, where an organisation would be unable to provide the product or service to the individual if the individual did not consent (or withdrew consent) to the collection, use or disclosure of his personal data for that purpose, the organisation should give due consideration to whether the personal data requested is necessary or integral to providing the product or service. Example: An individual wishes to obtain certain services from a telecom service provider and is required by the telecom service provider to agree to its terms and conditions for provision of the services. The telecom service provider can stipulate, as a condition of providing those services, that the individual	

		agrees to the collection, use and disclosure of specified items of personal data which is reasonably required by the telecom service provider to supply the subscribed services to the individual. Such items of personal data may include the name and address of the individual as well as personal data collected in the course of providing the services such as the individual's location data. Section 14(2)(b) addresses the situation where an organisation obtains or attempts to obtain consent by providing false or misleading information or using misleading and deceptive practices. Such practices may include situations where the purposes are stated in vague or inaccurate terms, in an illegible font or placed in an obscure area of a document or a location that is difficult to access. Deemed consent Sections 15 and 15A of the PDPA provide for different forms of deemed consent, namely (a) deemed consent by conduct; (b) deemed consent by contractual necessity; and (c) deemed consent by notification. Further, where an individual gives or is deemed to have given consent for disclosure of his personal data by one organisation ("A") to another organisation ("B") for a purpose, the individual is deemed to consent to the collection of his personal data by B for that purpose. Deemed consent by conduct Deemed consent by conduct applies to situations where the individual voluntarily provides his personal data to the organisation. The purposes are limited to those that are objectively obvious and	

		reasonably appropriate from the surrounding circumstances. Pursuant to section 15(1), consent is deemed to have been given by the individual's act of providing his personal data. An individual may be regarded as voluntarily providing personal data where the individual takes certain actions that allow the data to be collected, without actually giving consent. Consent is deemed to be given to the extent that the individual intended to provide his personal data and took the action required for the data to be collected by the organisation. Example: Deemed consent for processing of payment Sarah makes a visit to a spa for a facial treatment. After the treatment is complete, the cashier tells her that the facial would cost her $49.99. She hands over her credit card to the cashier to make payment. The cashier need not ask for Sarah's consent to collect, use or disclose her credit card number and any other related personal data (e.g. name on credit card) required to process the payment transaction. Sarah is deemed to have consented to the collection, use and disclosure of her credit card number and other related personal data for processing of the payment as she voluntarily provided the personal data and it is reasonable that Sarah would provide the personal data to pay for her facial. Example: Deemed consent for health check-up Eva goes for a health check-up at a clinic and is given information on the tests that will be conducted, which involves the collection of her blood pressure, height and weight. By proceeding	

		with the tests, Eva is deemed to consent to the collection of her personal data by the clinic for the purposes of the health check-up. Example: Deemed consent for taxi booking Tina calls a taxi operator's hotline to book a taxi. The customer service officer asks for her name and number to inform her of the taxi number, which Tina provides voluntarily. Tina is deemed to have consented to the taxi company using her name and number to call or text her when her taxi arrives. However, if the taxi operator runs a limousine service and wants to use Tina's information to market this service to her, Tina would not be deemed to have consented to the use of her personal data for this purpose. This is because Tina is providing her personal data for booking a taxi for a single trip, and not for receiving marketing information about the limousine service. Deemed consent by contractual necessity The second situation in which consent may be deemed is where an individual provides his personal data to one organisation ("A") for the purpose of a transaction and it is reasonably necessary for A to disclose the personal data to another organisation ("B") for the necessary conclusion or performance of the transaction between the individual and A. Deemed consent by contractual necessity under section 15(3) extends to disclosure by B to another downstream organisation ("C") where the disclosure (and collection) is reasonably necessary to fulfil the contract between the individual and A. To be clear, deemed	

		consent by contractual necessity allows further use or disclosure of personal data by C and other organisations downstream (refer to Diagram 1 below) where the use or disclosure is reasonably necessary to conclude or perform the contract between the individual and A. Diagram 1: Example: Deemed consent for processing of payment In an example above, Sarah is deemed to consent to a spa collecting, using or disclosing her credit card details to process the payment for her facial. In the course of processing the payment, her credit card details are transmitted to the spa's bank which handles the payment. Since Sarah is deemed to consent to the disclosure of her credit card details by the spa to its bank, deemed consent by contractual necessity would apply to all other parties involved in the payment processing chain who collects or uses Sarah's personal data, where the collection, use or disclosure is reasonably necessary to fulfil the contract between Sarah and the spa. These parties include, for example, Sarah's bank, the spa's bank, the banks' processers and the credit card scheme's payment system providers. Example: Deemed consent for processing of GIRO deduction and tax relief Benjamin donates $5,000 to a charity organisation and provides his personal data (i.e. NRIC number, residential address, bank account details) through an online donation form on the charity organisation's website. The form clearly states the purposes of collection, use or disclosure of donors' personal data – for the charity organisation to	

		process the donation (e.g. through GIRO deduction from the bank) and for tax relief purposes. Since Benjamin consents to the collection, use and disclosure of his personal data by the charity organisation for the notified purposes, deemed consent by contractual necessity would apply to all other parties involved in the GIRO and tax relief processing chain who collects, uses or discloses Benjamin's personal data, where the collection, use or disclosure is reasonably necessary to fulfil the transaction between Benjamin and the charity organisation. These parties include, for example, Benjamin's bank, the charity organisation's bank, the banks' processers, and the tax authority. Example: Deemed consent for processing of payment and delivery Bella orders furniture from a retailer through an e-commerce platform and provides her personal data (e.g. credit card details, contact number and residential address) for the purchase and delivery of goods. She also selects the option to have her furniture delivered to her home by a delivery company. The retailer can rely on deemed consent by contractual necessity to disclose Bella's personal data to the delivery company as the disclosure is reasonably necessary to fulfil the transaction between Bella and the retailer. The delivery company and all other parties involved in Bella's transaction with the retailer would also be able to rely on deemed consent by contractual necessity to collect, use or further disclose personal data where reasonably necessary to fulfil the	

		transaction between Bella and the retailer. These parties include, for instance, the e-commerce company, the online payment gateway in which payment for the transaction is processed, the relevant banks and logistics service partners (e.g. sub-contractors in the entire delivery chain, including the last mile delivery to Bella's home). Deemed consent by notification Section 15A of the PDPA provides that an individual may be deemed to have consented to the collection, use or disclosure of personal data for a purpose that he had been notified of, and he has not taken any action to opt out of the collection, use or disclosure of his personal data. Deemed consent by notification is useful where the organisation wishes to use or disclose existing data for secondary purposes that are different from the primary purposes for which it had originally collected the personal data for, and it is unable to rely on any of the exceptions to consent (e.g. business improvement, research) for the intended secondary use. This is subject to the organisation assessing and determining that the following conditions are met, taking into consideration the types of personal data involved and the method of collection, use or disclosure of the personal data in the manner set out below: a) Conduct an assessment to eliminate or mitigate adverse effects: Section 15A(4)(a) of the PDPA provides that an organisation must, before collecting, using or disclosing any personal data about an individual, conduct an assessment to determine that the proposed collection, use or	

		disclosure of personal data is not likely to have an adverse effect on the individual. The assessment for relying on deemed consent by notification will also have to take into consideration the method of notification and opt-out period (see paragraphs 12.23(b) and (c)). Apart from identifying the likely adverse effects, the organisation's assessment should consider any measures to be taken by the organisation to eliminate, reduce the likelihood of or mitigate the adverse effects identified. Organisations may wish to use the Assessment Checklist for Deemed Consent by Notification (at Annex B) to conduct the assessment. Please refer to the Personal Data Protection Regulations 2021 and paragraphs 12.64 – 12.69 below on conducting the assessment. b) Organisation must take reasonable steps to ensure that notification provided to individuals is adequate: Section 15A(4)(b) of the PDPA provides that an organisation must take reasonable steps to bring the following matters to the attention of the individual: (i) the organisation's intention to collect, use or disclose the personal data; (ii) the purpose of such collection, use or disclosure; and (iii) a reasonable period within which, and a reasonable manner by which, an individual can opt out of the collection, use or disclosure of his personal data for this purpose. The Commission does not prescribe the method by which the individual should be notified, but the organisation must ensure the notification is adequate and effective in making the individual aware of the proposed collection, use or	

		disclosure of his personal data9. Organisations may choose to rely on a single mode or multiple modes of communication in notifying individuals adequately. Some considerations for determining the appropriate mode(s) of communication include: (i) The usual mode of communication between the individual and the organisation. (ii) Whether direct communication channels such as mail, email messages, telephone calls or SMS10 are available. Notification provided through interactive portals and applications may also be considered. These could include push notifications sent through mobile applications. These also include dashboards or consent portals where individuals can keep track of their interactions with the organisation, including their preferences on purposes for which they consent to the collection, use or disclosure of their personal data. However, organisations should note that these channels may not always be effective (e.g. contact information may not be updated). (iii) Number of individuals to be notified. In particular, where the organisation intends to reach out to a large number of individuals, and assesses that direct communication channels are not effective, other forms of mass communication channels may be considered. These include a micro-site on the organisation's corporate website, notification through the organisation's social media channels, and notifications through printed or other news media. Example: Providing appropriate notification to users of mobile application	

		A health app company provides a mobile application that collects, uses and discloses personal data relating to individuals' lifestyle and wellness (e.g. number of steps walked, height, weight, age and gender). Users are able to view their activity data (e.g. sleep patterns, periods of activity, number of calories lost) through the mobile application. The health app company intends to use the lifestyle and wellness data collected from its users to provide a personalised weight loss programme for its users. It intends to use the users' personal data to provide the personalised programme through the application installed on their devices. It assesses that there is no likely adverse effect to users in using their personal data for this purpose. Thereafter, each user can decide whether to participate after viewing the personalised programme (in which case express consent will be obtained). The health app company decides that the best way to notify users is through the mobile application as it is a direct and effective way to communicate with users who are monitoring their activity through the application. To ensure inactive users of the application are notified, it notifies users by email and through its social media channels. c) Organisation must provide a reasonable opt-out period: The organisation must provide a reasonable period for the individual to opt out before it proceeds to collect, use or disclose the personal data. Consent for the collection, use or disclosure of personal data is deemed to be given only after the opt-out period has lapsed. Any collection, use or disclosure	

		of personal data for the purposes that have been notified should commence only after the expiry of the opt-out period. Deemed consent by notification should not be relied on where individuals would not have a reasonable opportunity and period to opt out (e.g. security monitoring of premises using video cameras). The Commission does not prescribe a specific opt-out period, and organisations shall assess and determine a reasonable period for individuals to opt out of the collection, use or disclosure of personal data. Some considerations for determining the reasonableness of the optout period include: (i) The nature and frequency of interaction with the individual. For instance, where an organisation sends push notifications through a mobile application used by individuals to track and update monthly medical check-up information, the opt-out period should not be shorter than one month. (ii) The communications and opt-out channels used. Direct communications channels, particularly those that have a track record of being effective in reaching the intended customer base, may justify a shorter opt-out period than mass communications channels. Opt-out methods that are easily accessible and easy to use may also justify a shorter opt-out period (e.g. providing for opt-out via email or hyperlink). After the opt-out period has lapsed and the individual no longer wishes to consent to the purpose, the individual can withdraw his consent for the collection, use or disclosure of personal data. Under the Personal Data	

		Protection Regulations 2021, the organisation must retain a copy of its assessment throughout the period that the organisation collects, uses or discloses personal data based on deemed consent by notification. When requested by the Commission, the organisation must provide to the Commission its assessment for collecting, using or disclosing personal data based on deemed consent by notification. The organisation is not required to provide its assessment to individuals who request for it as it may contain commercially sensitive information. Example: Hotel's sharing of personal data with partners A hotel chain wishes to rely on deemed consent by notification to disclose personal data of its members (e.g. frequency and length of hotel stays, type of rooms, preferences and reviews) to travel website company to develop online travel resources and customised travel packages. The personal data it shares will not be used to obtain consent for sending direct marketing messages to members. The hotel chain assesses that there is no likely adverse effect to its members in disclosing their personal data for this purpose. The hotel chain also assesses that emailing members on the intended sharing of their personal data is an appropriate and effective method of notification, as it regularly sends emails to its members regarding membership points, rewards and offers. It also assesses that 10 days is a reasonable period for individuals to opt out. The hotel chain sends an email to its members which notifies them of the intended disclosure of their personal data to the	

		travel website company for the purpose and provides a contact number for any queries on the intended disclosure. A hyperlink is provided in the email for members to opt out of it, and the hotel chain requests that members who wish to opt out do so within 10 days from the date of the email. Members who do not opt out within the 10-day opt-out period are deemed to have consented to the collection, use and disclosure of their personal data for this purpose. The hotel chain will need to allow and facilitate any withdrawal of consent from members after the 10-day opt-out period. Example: Banks' use of voice data for customer authentication A bank collects voice data of customers when they call the bank's contact centre for managing disputes. Customers are informed that their voice data is collected for this purpose. The bank intends to use the collected voice data (i.e. voiceprint) as an alternate means of authentication to complement existing verification methods (e.g. where the customer misplaces his credenti	
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions	Obtaining clear and unambiguous consent As noted in the previous section, a person is not required to check with the DNC Registry before	

		sending a specified message to a Singapore telephone number if the person has obtained a clear and unambiguous consent evidenced in written or other form from the subscriber or user of the number for the sending of the message to that number. The PDPA does not define the terms 'clear' and 'unambiguous' as the determination of whether consent was clear and unambiguous will depend on the specific facts in question. Facts that would determine if consent was clear and unambiguous would include: a) whether the person had notified the user or subscriber clearly and specifically that specified messages would be sent to his or her Singapore telephone number; and b) whether the user or subscriber gave consent to receive specified messages through some form of positive action. Clear and unambiguous consent is unlikely to be construed to have been obtained from a mere failure to opt out through inaction on the part of the user or subscriber. Please refer to the section on "Failure to opt out" in the Key Concepts Guidelines for more information. Examples of when persons would be considered to have obtained clear and unambiguous consent are provided below. Persons who wish to contact individuals to obtain clear and unambiguous consent for the sending of specified messages should do so in a manner which does not involve the sending of a specified message to a Singapore telephone number, unless such persons comply with the DNC Provisions. Such persons will also have to comply with the DP Provisions. Please	

		refer to the section on "Offers to send specified messages" in Chapter 3 for more details. Sending specified messages to Singapore telephone numbers obtained through third party sources In some instances, a person A may obtain the Singapore telephone number of an individual C through third party source B (e.g. third party referrer) for the purpose of sending specified messages to C. To be clear, under such circumstances, person A is still required to comply with the DNC provisions when sending C specified messages to the Singapore telephone number, unless person A has obtained clear and unambiguous consent from C for person A to send specified messages to that number. In such circumstances, person A could obtain from B evidence of clear and unambiguous consent given by C for the sending of specified messages by A, or obtain such consent from C directly. (Refer to paragraphs 3.12 and 3.13 above.) For instance, a direct marketing firm that wishes to obtain a list of Singapore telephone numbers of individuals from a third party source for the sending of marketing messages, could obtain a copy of the consent form documenting clear and unambiguous consent from the individuals for the direct marketing firm to send specified messages to their telephone numbers. In addition, the DP Provisions in the PDPA require organisations to obtain the individual's consent before collecting, using or disclosing personal data of the individual17. Recycled numbers The Commission notes that in	

		certain circumstances, persons may obtain clear and unambiguous consent from a subscriber ("original subscriber") of a particular telephone number, which is subsequently terminated by the original subscriber and allocated to a new individual. Similarly, a user ("original user") of a telephone number may cease to use the number (without any change in the subscriber) and the subscriber may permit a new user to use the number. In these circumstances, the termination of the number or change in the user of the number does not automatically or on its own invalidate the consent provided by the original subscriber or original user18. However, persons cannot rely on the consent obtained from the original subscriber or original user to send specified messages to that telephone number, once they are aware that the subscriber or user who consented to the sending of specified messages to that telephone number is no longer the subscriber or user of that telephone number. Clear and unambiguous consent obtained for the wrong telephone number In certain circumstances, clear and unambiguous consent may be obtained for the sending of specified messages to a wrong telephone number on the part of the person obtaining consent or on the part of the person giving consent. Consent evidenced in written or other form Section 43(4) requires consent obtained for the purposes of section 43 to be evidenced in written or other form so as to be accessible for subsequent reference.	

		Written form may include documents or other form of records in physical or electronic form. A person should note that the requirement to obtain consent in evidential form applies to both online and offline situations. If the consent required under section 43 is not evidenced in written form, it must be recorded in a form which is accessible for subsequent reference. This means that the consent must be captured in a manner or form which can be retrieved and reproduced at a later time in order to confirm that such consent was obtained. Possible forms include an audio or video recording of the consent given. The Commission recognises that persons may seek to obtain consent to send specified messages to Singapore telephone numbers in a variety of different ways, and that would consequently affect the form in which the evidence takes. For example, persons may seek to obtain consent by asking individuals to: a) respond to a pop-up on a webpage; b) respond to pop-ups or other form of notifications within mobile applications; c) fill out and submit a web form; d) fill out and submit a physical form; e) indicate their choice by signing or ticking against a check box printed on a letter or service agreement; or f) call or send an SMS to the person. Generally speaking, where consent was obtained by way of a physical document, persons should retain the original document as evidence of the	

		consent. Where consent was obtained through electronic means, persons should retain documentation or system logs capturing the following information: a) the individual's choice (i.e. whether the individual provided consent or not); b) date and time when the individual expressed his choice; c) the webpage / pop-up / online form (or equivalent) which the relevant individual was looking at when providing consent; and d) the clauses which the individual consented to (including the terms and conditions applicable to the consent which the individual provided). How long persons should retain documentary evidence of clear and unambiguous consent Persons should retain evidence of clear and unambiguous consent from an individual for as long as they intend to rely on such consent to send specified messages to that individual's Singapore telephone number. In considering how long to retain documentary evidence of consent obtained for the sending of specified messages, persons should have regard to the Retention Limitation Obligation in section 25 of the PDPA. Section 25 requires an organisation to cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data, and retention is no longer necessary for legal or	

		business purposes. Where a complaint in relation to a specified message sent arises and the sender has ceased to retain documentary evidence of the consent, the Commission would assess the strength of the remaining evidence (including consideration of evidence as to whether a specified message was sent) in investigating the complaint. Consent given before the prescribed day As an individual may have consented to receive specified messages sent to his or her Singapore telephone number before the DNC Provisions took effect, the PDPA recognises such consent for the purposes of the DNC Provisions. In particular, section 47(4) provides that for the purposes of the DNC Provisions, a subscriber or user of a Singapore telephone number is deemed to have given his or her consent to a person to send a specified message to that number if – a) the subscriber or user had consented to the sending of the message before the DNC Provisions came into operation; and b) such consent had not been withdrawn on or after the date on which the DNC Provisions came into operation. The Commission is of the view that persons obtaining consent from individuals before the prescribed day to receive specified messages should also fulfil the section 43(4) requirements – i.e. that the consent be clear and unambiguous and evidenced in written or other form. Withdrawing clear and unambiguous consent	

		Any consent given by the subscriber or user of a Singapore telephone number to a person for the purposes of the DNC Provisions may be withdrawn by the user or subscriber by providing notice to the person19. The "prescribed period" (as set out in section 47(3)) within which persons must effect a withdrawal of consent is 21 days. Section 47(1) of the PDPA provides that a subscriber or user of a Singapore telephone number may withdraw any consent given to a person for the sending of any specified message to that number by giving notice to the person. Section 47(3) provides that a person that receives such a notice must cease (and cause its agents to cease) sending any specified messages to that number after the expiry of the prescribed period, which are prescribed in Regulations. Persons should cease the sending of all specified messages which fall within the scope of a withdrawal notice. In determining the effect of any notice to withdraw consent, the Commission will consider all relevant facts of the situation. This could include but is not limited to matters like: a) the actual content of the notice of withdrawal; b) whether the intent to withdraw consent was clearly expressed; and c) the channel through which the notice was sent. In facilitating any notice to withdraw consent, an organisation should act reasonably and in good faith. Considerations for determining the scope of a notice to withdraw consent obtained under the DNC	

		Provisions (i.e. consent to send marketing messages to a Singapore telephone number) are similar to that for the DP Provisions. Please refer to Chapter 12 of the Key Concepts Guidelines for more details on withdrawal of consent under the DP Provisions. Effect of withdrawal when clear and unambiguous consent was obtained for more than one channel The Commission notes that persons may obtain clear and unambiguous consent to send specified messages to a Singapore telephone number for one channel only (e.g. the consent obtained was solely to receive specified messages via fax), or for more than one channel (e.g. the consent was obtained for the sending of specified messages through voice calls, fax and text messages). Where the persons state the availability of a facility for notifying a withdrawal of consent (e.g. "send 'UNSUB' to [Singapore telephone number]"), the persons should clearly indicate the scope of withdrawal. Where the withdrawal notice contains a general withdrawal message, without indicating clearly the scope of the withdrawal, the Commission will consider any withdrawal of consent via a particular channel to only apply to all specified messages sent via that channel. Please see the examples below for more details. No withdrawal by subsequent registration with the DNC Registry A subscriber or user of a Singapore telephone number who has given consent (which meets the requirements specified in the PDPA) to a	

		person may subsequently register his or her number with the DNC Registry as he or she does not want to receive marketing messages from other persons. In such a situation, the PDPA recognises that the consent given before registration with the DNC Registry will continue to be effective for the purposes of the DNC Provisions. In particular, section 47(5) of the PDPA provides that where a subscriber or user of a Singapore telephone number consents to a person sending a specified message to that number on or after the commencement of the DNC Provisions and subsequently adds that number to a DNC Register, the addition of the number shall not be regarded as a withdrawal of consent for the purposes of the DNC Provisions. Reading section 47 (4) and (5) together, the addition of a Singapore telephone number on a DNC Register does not amount to withdrawal of consent given before the commencement of the DNC Provisions. Individuals wishing to withdraw consent to the sending of specified messages to their Singapore telephone number should withdraw consent by giving reasonable notice to the organisation under section 16 of the PDPA. Requiring consent for telemarketing as a condition for providing goods and services Section 46(1) of the PDPA provides that a person shall not, as a condition of supplying goods, services, land, interest or opportunity, require a subscriber or user of a Singapore telephone number to consent for the sending of a specified message to that Singapore telephone	

		number or any other Singapore telephone number beyond what is reasonable to provide the goods, services, land, interest or opportunity. The Commission notes that some organisations may wish to require consent from individuals for the sending of a specified message to their Singapore telephone number ("receive specified messages"), as a condition of providing goods, services, land, interest or opportunity. Factors that determine whether requiring consent for a particular purpose is reasonable would include the nature of the goods, services, land, interest or opportunity provided. Generally, consent for the sending of any type of specified messages would not appear to be something that is considered to be reasonably required for the provision of most types of goods, services, land, interest or opportunity. Hence, organisations should generally give individuals the option to consent to the receiving of specified messages from the organisation, and should not deny the individual the goods, services, land, interest or opportunity simply because he does not consent to the receiving of marketing messages. For more information on requiring consent for the collection, use or disclosure of personal data for marketing purposes, please refer to the Advisory Guidelines on Requiring Consent for Marketing Purposes. Other obligations relating to consent The DNC Provisions include a few additional obligations which persons are required to comply with in connection with obtaining	

		consent. Section 46 prohibits persons from obtaining or attempting to obtain consent for sending a specified message to a Singapore telephone number by providing false or misleading information with respect to the sending of the message or by using deceptive or misleading practices. Section 46 provides that any consent given in such circumstances is not validly given. Secondly, section 47(2) provides that a person shall not prohibit a subscriber or user of a Singapore telephone number from withdrawing consent to the sending of a specified message to that Singapore telephone number. However, this provision does not affect any legal consequences arising from such withdrawal. As the requirements of sections 46 and 47(2) are similar to those provided in the DP Provisions please refer to the chapter on the "Consent Obligation" in the Key Concepts Guidelines for more information.	
26	Advisory Guidelines on Application of PDPA to Election Activities		
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for Marketing Purposes	2 Obtaining consent under the Data Protection Provisions 2.1 Section 13 of the PDPA, on the requirement to obtain consent, states that: An organisation shall not, on or after the appointed day, collect,	

		use or disclose personal data about an individual unless – (a) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or (b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law. 2.2 Section 13 of the PDPA prohibits organisations from collecting, using or disclosing an individual's personal data unless the individual gives, or is deemed to have given, his consent for the collection, use or disclosure of his personal data. This requirement to obtain consent does not apply where collection, use or disclosure of an individual's personal data without consent is required or authorised under the PDPA or any other written law. This obligation to obtain the individual's consent is referred to in these Guidelines as the Consent Obligation. Sections 14 to 17 of the PDPA set out further provisions relating to the Consent Obligation. Please refer to the Advisory Guidelines on Key Concepts in the PDPA ("Key Concepts Guidelines") for more information on these provisions. 2.3 Section 14(2)(a) sets out one of the requirements organisations must comply with when obtaining consent under the Data Protection Provisions, as follows: (2) An organisation shall not – (a) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the	

		individual beyond what is reasonable1 to provide the product or service to that individual; ... 2.4 Section 14(3) provides that any consent given under the circumstances in section 14(2) is not validly given for the purposes of the PDPA. 3 Obtaining consent under the Do Not Call Provisions 3.1 An organisation that wishes to send a "specified message" (as defined in the PDPA)2 to a Singapore telephone number must comply with the Do Not Call Provisions. 3.2 In brief, a message (whether sent via a voice call, text message or fax message) is a "specified message" if the purpose of the message, or one of its purposes, is – (a) to advertise, promote or offer to supply or provide any of the following: i. goods or services3; ii. land or an interest in land; or iii. a business opportunity or an investment opportunity; or (b) to advertise or promote a supplier/provider (or a prospective supplier/provider) of the items listed in sub-paragraphs (a)(i) to (iii) above. 3.3 One significant obligation under the Do Not Call Provisions provides that an organisation will have to check the Do Not Call Registry before sending a specified message, unless the user or subscriber of the Singapore telephone number has given clear and unambiguous consent in evidential form or the organisation is exempted under the Personal Data Protection (Exemption from Section 43) Order (S 817/2013). Please refer to the Key Concepts Guidelines and the Advisory Guidelines on	

		the Do Not Call Provisions ("DNC Guidelines") for more information on the Do Not Call Provisions. 3.4 Section 46(1) sets out one of the requirements organisations must comply with when obtaining consent under the Do Not Call Provisions as follows: (1) A person shall not, as a condition for supplying goods, services, land, interest or opportunity, require a subscriber or user of a Singapore telephone number to give consent for the sending of a specified message to that Singapore telephone number or any other Singapore telephone number beyond what is reasonable to provide the goods, services, land, interest or opportunity to that subscriber or user, and any consent given in such circumstance is not validly given. 4 Comparison of sections 14(2) and 46(1) of the PDPA 4.1 For the purposes of the discussion in the subsequent paragraphs, we shall refer to "product or service" (used in the context of section 14(2)) and "goods or services" (used in the context of section 46(1)) collectively as "item". 4.2 Although sections 14(2)(a) and 46(1) relate to different parts of the PDPA and have slightly different requirements, they are similar in establishing the key principle that an organisation cannot, as a condition of providing a certain item, require an individual to give his consent for the purposes of the PDPA4beyond what is reasonable to provide the item. 5 Effect of sections 14(2)(a) and 46(1) of the PDPA 5.1 The effect of section 14(2)(a) (read with section 14(3)5) and section 46(1) is that	

		organisations cannot refuse to provide an individual an item because the individual does not consent for the purposes of the PDPA6, unless it is reasonable to require consent so as to provide the item. 5.2 In determining whether an organisation can require an individual to consent for the purposes of the PDPA7, the Commission will consider the relevant facts of the particular situation8 . Factors that may be considered in assessing whether it is reasonable to require consent would include: (a) the amount and type of personal data for which consent is required; (b) the purpose of the collection, use or disclosure of the personal data for which consent is required; (c) the nature of the item being provided, including whether there is any benefit tied to the item, for example, whether the item is being provided without monetary payment to the organisation. Please refer to paragraphs 8.1 to 8.8 of these Guidelines which illustrate this in greater detail; and (d) what a reasonable 9person would consider appropriate in the circumstances, including the personal data and purpose for which consent may be required in light of the nature of the item being provided. 7 Requiring consent for marketing purposes 7.1 If organisations wish to obtain consent for marketing purposes10, they should generally provide the individuals the option whether or not to give consent to the marketing purposes, and should not deny provision of the item to the	

		individuals simply because they do not give consent for the marketing purposes. 7.2 However, the Commission recognises that there are certain situations where organisations can require consent for marketing purposes. For example, organisations may provide offers, discounts or lucky draw opportunities to individuals that are conditional on the collection, use or disclosure of their personal data for specified purposes. The Commission will assess whether an organisation can require an individual's consent for marketing purposes based on the facts of the particular situation as described in paragraph 5.2, where relevant.	
29	Advisory Guidelines for Management Corporations		
30	Advisory Guidelines for the Education Sector		
31	Advisory Guidelines for the Social Service Sector		
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector		
34	Advisory Guidelines for the Healthcare Sector	The Consent, Purpose Limitation and Notification Obligations The PDPA requires organisations to, among other things, notify an individual of the purposes for the collection, use and disclosure of his personal data1 and obtain his consent, unless any relevant exception to consent2 applies.	

		Moreover, organisations shall only collect, use and disclose personal data that are relevant for the purposes, and for purposes that a reasonable person would consider appropriate in the circumstances. The following will highlight how consent may apply in common healthcare scenarios, how deemed consent applies as well as the exceptions to consent. Deemed consent Deemed consent by conduct: In situations where an individual (without actually giving consent) voluntarily provides his personal data to an organisation for an appropriate purpose, and it is reasonable that he would voluntarily provide the data, the individual's consent to the collection, use or disclosure of personal data is deemed to have been given by the individual's act of providing his personal data. Deemed consent by contractual necessity: Pursuant to Section 15(3), if an individual gives, or is deemed to have given, consent to the collection, use or disclosure of his personal data to one organisation ("A") for the purpose of a contractual transaction, the consent may cover sharing of his personal data by A with other organisations (and onward sharing by downstream organisations, as the case may be) so long as it is reasonably necessary for A to provide the personal data to the other organisations (likewise, for onward sharing by downstream organisations) to perform or conclude A's contractual obligations. Deemed consent by notification: Section 15A provides that if an individual does not take any	

		action to opt out of the collection, use or disclosure of his personal data for a purpose that he has been notified of, the individual is deemed to consent to the collection, use or disclosure of personal data by the organisation even for secondary use purposes that are different from the primary purposes for which it had originally collected the personal data for3. Nonetheless, the individual must have been notified that their personal data would be used for such secondary use purposes. The organisation must meet stipulated conditions by conducting an assessment to identify any adverse impact on the individuals arising from the proposed collection, use or disclosure of his personal data, and implement mitigating measures in relation to the adverse impacts identified. Please refer to the Advisory Guidelines on Key Concepts in the PDPA (Chapter 12) for more information on the stipulated conditions. Withdrawal of consent Section 16 of the PDPA provides that individuals may at any time withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose by an organisation. Please refer to the Advisory Guidelines on Key Concepts in the PDPA (Chapter 12) for the requirements that must be complied with by either the individual or the organisation in relation to the withdrawal of consent. However, the organisation can continue to use and disclose personal data in their possession if allowed under other legal bases.	

		Exceptions to the Consent Obligation Section 17 of the PDPA permits the collection, use and disclosure of personal data without consent (and, in the case of collection, from a source other than the individual) and enumerates the permitted purposes in the First and Second Schedules to the PDPA. These exceptions to the Consent Obligation do not affect rights or obligations arising under any other law. Hence, even if an exception applies under the PDPA, organisations are required to comply with their other legal obligations, for example, to protect confidential information or other contractual obligations.Legitimate interests exception The term "legitimate interests" refers to any lawful interests of an organisation or other person (including other organisations). Organisations may collect, use and disclose personal data without consent where the identified legitimate interests outweigh any adverse effect on the individual. The "legitimate interests" exception encompasses either of the following: a) The general "legitimate interests" exception (under paragraph 1 of Part 3 of the PDPA First Schedule) is a broad exception for any purposes that meet the definition of "legitimate interest". Organisations relying on this exception must assess and act upon any adverse effects on the individuals (i.e., whether to eliminate, reduce likelihood of or mitigate the adverse effects); or b) The specific "legitimate interests" exception is confined to purposes prescribed within paragraphs 2 to 10 of Part 3 of	

		the PDPA First Schedule such as for evaluative purposes, for any investigation or proceedings, or for recovery or payment of debt owed etc. The "legitimate interests" exception allows the collection, use or disclosure of personal data without consent for a wide range of circumstances and purposes. Organisations relying on this exception would need to comply with additional safeguards to ensure the interests of individuals are protected and can refer to paragraphs 12.56 to 12.70 of the Advisory Guidelines on Key Concepts in the PDPA for more information. Organisations cannot rely on the legitimate interests exception to send direct marketing messages. Business improvement exception Part 5 of the First Schedule and Division 2 under Part 2 of the Second Schedule ("business improvement exception") enable organisations to use, without consent, personal data that they had collected in accordance with the Data Protection Provisions, so long as the use of the personal data falls within the scope of any of the following purposes: a) Improving, enhancing or developing new goods or services; b) Improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services; c) Learning or understanding behaviour and preferences of individuals (including groups of individuals segmented by profile); or d) Identifying goods or services that may be suitable for	

		individuals (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals. To rely on the business improvement exception, organisations will need to ensure the following: a) The business improvement purpose cannot reasonably be achieved without using the personal data in an individually identifiable form; and b) The organisation's use of personal data for the business improvement purpose is one that a reasonable person would consider appropriate in the circumstances. The business improvement exception also applies to the sharing of personal data (i.e., collection and disclosure) between entities belonging to a group of companies, without consent, for the following business improvement purposes: a) Improving, enhancing or developing new goods or services; b) Improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services; c) Learning or understanding behaviour and preferences of existing or prospective customers4 (including groups of individuals segmented by profile); or d) Identifying goods or services that may be suitable for existing or prospective customers (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals. Organisations relying on this	

		exception to share personal data within a group of entities need to ensure several conditions are fulfilled first. Organisations cannot rely on the business improvement exception to send direct marketing messages. For more information, please refer to paragraphs 12.71 to 12.77 of the Advisory Guidelines on Key Concepts in the PDPA. Research exception The business improvement exception is intended to enable organisations to use personal data to improve their products, services, business operations and customer experience. On the other hand, the research exception enables organisations to conduct broader research and development that may not have any immediate application to their products, services, business operations or market. Commercial laboratories or institutes of higher learning that carry out research for the development of health products or medicine, and organisations that carry out market research are examples of organisations that can rely on the research exception. The research exception (Division 3 under Part 2 of the PDPA Second Schedule) provides that organisations may use personal data for a research purpose without consent, including historical and statistical research, subject to the following conditions: a) The research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form; b) There is a clear public benefit to using the personal data for the research purpose; c) The results of the research will not be used to make any	

		decision that affects the individual; and d) In the event the results of the research are published, the organisation must publish the results in the form that does not identify the individual5. Organisations may disclose personal data for a research purpose without consent, including historical and statistical research, by assessing the same set of conditions applicable to the research exception relating to use of personal data with an additional condition: a) It is impracticable for the organisation to seek the consent of the individual for the disclosure. When assessing whether it would be "impracticable" for the organisation to seek consent of the individual, the specific facts of the case have to be considered. For more information on the research exception, please refer to paragraphs 12.80 to 12.83 of the Advisory Guidelines on Key Concepts in the PDPA. The following examples mainly focus on the application of these bligations, including situations where consent may be deemed, or where exceptions to the Consent Obligation may apply. Where appropriate, brief references may be made to other obligations, but it is not the intent to apply every obligation in the PDPA within each example. Example: Collecting personal data from patients seeking medical care John visits Hospital ABC for the first time for a medical examination. The nurse informs John that he has to register and hands him a registration form to fill out.	

		John voluntarily fills out the form and provides his full name, address, NRIC number and mobile number. Consent from John can be deemed for certain purposes By voluntarily providing his personal data (including through presenting himself for medical examination), John may be deemed to have consented to the collection, use and disclosure of his personal data (including data derived from ensuing medical examinations and tests) by Hospital ABC for the purpose of his visit, including any medical care provided in relation to the visit. Depending on the actual circumstances, this could include: • any associated examinations or tests; • follow-up consultations in relation to the purpose of his visit to Hospital ABC; and • the convening of a case conference with other doctors within Hospital ABC solely for the purpose of discussing treatment options for John. There is likely to be deemed consent by conduct as the purposes for the collection, use and disclosure of John's personal data are objectively obvious and reasonably appropriate from the surrounding circumstances. As long as John actively provides his personal data to Hospital ABC or allows his personal data to be collected by Hospital ABC, deemed consent by conduct applies. Whether deemed consent would cover purposes beyond the provision of medical care to John Deemed consent by conduct does not cover purposes outside those for which the personal	

		data was provided. Generally, if Hospital ABC intends to use or disclose such personal data for purposes that are not related to provision of medical care, it is less likely to be covered by deemed consent by conduct and in such instances Hospital ABC should notify John of such purposes and obtain his consent. However, Hospital ABC may rely on deemed consent by notification to use or disclose existing data for secondary purposes that are different from the primary purposes for which it had been originally collected for, by conducting an assessment first to ensure several conditions are met and taking reasonable steps to ensure that John is notified of Hospital ABC's intention to collect, use or disclose his personal data and the purpose(s) of such collection, use or disclosure6. Deemed consent by notification cannot be relied on if John has opted out of the collection, use or disclosure of his personal data. For example, Hospital ABC may wish to use John's personal data for the marketing of health products that are unrelated to John's condition to John. It is unlikely that John would be deemed to have given his consent for this purpose, since such usage has no nexus to his visit to Hospital ABC or the provision of medical care related to his visit. Hospital ABC is unable to rely on deemed consent by notification where consent previously obtained from John is used for the secondary purpose of marketing health products by direct marketing messages that are unrelated to his condition. Therefore, Hospital ABC should	

		notify John of such purposes and actively obtain his express consent. Other considerations Consent cannot be required beyond what is reasonable to provide the service In deciding what personal data to collect from patients, Hospital ABC should note that section 14(2)(a) of the PDPA provides that an organisation providing a product or service to an individual must not, as a condition of providing the product or service, require the individual to consent to the collection, use or disclosure of his personal data beyond what is reasonable to provide the product or service. As good practice, Hospital ABC should not collect more personal data than is required for its business or legal purposes. It is also good practice for Hospital ABC to indicate which fields in the form that collect personal data are compulsory and which are optional. How the Retention Limitation Obligation applies Hospital ABC may retain John's personal data after John's visit is completed, if there is a legal or business purpose to do so. For example, Hospital ABC may retain John's personal data in accordance with Regulation 12 of the Private Hospitals and Medical Clinics ("PHMC") Regulations, the National Guidelines for Retention Periods of Medical Records under the PHMC Act, Regulation 37 of the Healthcare Services (General) Regulations and the Licence Conditions on the retention periods of patient health records under Healthcare Services Act (HCSA) (which, in brief, provides that licensed healthcare	

		institutions must maintain medical records for such periods as may be required). Obtaining consent from patients for medical students or doctors on an attachment programme to collect, use and disclose their personal data as part of providing medical care John visits Hospital ABC to seek medical care. As illustrated in the example above, John may be deemed to have consented to the collection, use and disclosure of his personal data by Hospital ABC for the purpose of his visit (including the medical care that is to be provided in relation to the purpose of his visit) by voluntarily providing his personal data (including through presenting himself for medical examination). The consent deemed to have been provided from John will cover all activities which Hospital ABC (including employees and volunteers) has to undertake for the purpose of John's visit. The employees and volunteers involved in John's care at Hospital ABC would not need to obtain separate consent from John to collect, use or disclose his personal data for the purpose of providing medical care to him. Depending on the actual circumstances, the employees and volunteers could include doctors or medical students providing medical care as part of a formal attachment programme with Hospital ABC. An 'employee' under the PDPA includes a volunteer working under an unpaid volunteer work relationship. Example: Disclosing personal data in referral cases During separate consultations with the following patients, Doctor Lee makes the	

		recommendations as follows: a) for Patient A to consult a specialist; b) for Patient B to visit a hospital for further medical tests; and c) for Patient C to consider long term care services at a nursing home. Patients A, B and C each agree (verbally) to the respective recommendations and Doctor Lee proceeds to make the necessary arrangements, for example, by contacting another doctor directly7. Since each patient agreed to the recommendation by the primary doctor, the patient would have consented to the doctor disclosing his personal data as required for the referral when contacting the proposed healthcare service provider directly. In cases where Doctor Lee provides the patient with the referral letter, and the patient takes the referral letter to the organisation he is being referred to, it is the patient who would be considered to have disclosed his personal data to that organisation. As good practice, Doctor Lee could consider documenting the verbal consent given, such as by making a note in the patient's file. Having written evidence supporting verbal consent would be useful in the event of a dispute. Before Doctor Lee discloses Patients A, B and C's personal data to these organisations, he should take reasonable steps to ensure that their personal data is accurate and complete, and in compliance with any prevailing healthcare requirements and licensing conditions such as the PHMC Act and HCSA. For the avoidance of doubt, Doctor Lee may disclose the	

		personal data pursuant to such consent regardless of whether or when Patients A, B and C arrive at the respective facility to which they have been referred. Example: Collecting personal data of other individuals from a patient for medical care During John's consultation, the doctor asks if John has had any family history of cancer, as it is relevant to providing medical care to John. John informs the doctor that his Aunt Kim has had stomach cancer. This may or may not be considered personal data of Aunt Kim, depending on whether Aunt Kim can be identified by the organisation that is collecting such data (through the doctor) from this data itself or when this data is combined with other likely accessible data or information. If Aunt Kim can be identified The doctor asks John for more details about Aunt Kim including her medical history, like her full name and the healthcare institution she sought treatment at, as the information is relevant to provide medical care to John. In this case, the doctor is likely to be collecting personal data about Aunt Kim. The organisation (through the doctor) may collect the personal data of Aunt Kim without her consent under an exception provided in paragraph 8(a) of Part 3 of the First Schedule to the PDPA8, as the personal data was provided to the organisation (through the doctor), by another individual (John), to enable the organisation to provide a service for the personal and domestic purposes of that other individual (medical care for John). If the organisation wishes to use or disclose Aunt Kim's personal data without her consent solely	

		for purposes consistent with the purpose of the collection, it may do so pursuant to paragraph 8(b) of Part 3 of the First Schedule to the PDPA9. The organisation is still obliged to comply with the other Data Protection Provisions in the PDPA, such as the obligation to protect Aunt Kim's personal data. If Aunt Kim cannot be identified The doctor does not ask John for more details about Aunt Kim, as he determines that it is not relevant to provide medical care to John. If the organisation that is collecting the data (through the doctor) makes an assessment that it cannot identify Aunt Kim from this data (or when combining this data with other likely accessible data or information), then the data is not personal data and the PDPA does not apply. The onus is on the organisation to make the assessment and determine whether the PDPA is applicable to the data collected. For more information on the assessment that the organisation can make to determine if Aunt Kim can be identified from the data, please refer to paragraphs 5.4 to 5.6 of the Advisory Guidelines on Key Concepts in the PDPA. Example: Collecting, using or disclosing personal data for purposes other than for the patient's visit or medical care Clinic/ Healthcare Institution ABC ("Health Organisation ABC") wishes to collect, use or disclose John's personal data when he visits the clinic for medical care and the following purposes: a) review of internal processes for quality assurance and other activities that are integral to the proper functioning of overall	

		business operations; and b) formulation of teaching material, e.g. as part of a case study, lecture slides or other types of teaching material used for teaching purposes. Generally, Health Organisation ABC should notify John of its intended purposes and obtain his consent for such purposes, unless any relevant exception applies. Health Organisation ABC is free to determine the appropriate means by which it notifies and obtains consent from John. In relation to the specific purposes above: a) For internal quality assurance and other activities that are integral to the proper functioning of overall business operations: Health Organisation ABC is unlikely to be required to specifically notify John of such internal corporate purposes that support the delivery of medical care to him and/or obtain consent for them10; and b) For formulation of teaching material: Health Organisation ABC should typically notify John of such purposes and obtain consent if the data cannot be anonymised. Consent from patients would not be required where the training or professional registration activities do not involve the collection, use or disclosure of their personal data. (E.g. where a trainee doctor records in his log-book or reports only information that does not contain personal data of patients, such as the number of hours he has spent performing a particular medical procedure or other information that does not identify any patient11.) Organisations should also note that the Data Protection	

		Provisions would not affect any regulatory requirements by or under the laws which govern professional training or registration requirements for doctors and other healthcare professionals. (E.g. under the Medical Registration Act, certain conditions may be mposed by the Singapore Medical Council in respect of the registration of provisionally registered doctors.) Cannot require consent for additional purposes unless reasonably required to provide medical care If these additional purposes are not reasonably required to provide John with the service of medical care, Health Organisation ABC cannot require John to consent to his personal data being collected, used or disclosed for these purposes as a condition of providing him the medical care service (section 14(2)(a) of the PDPA). Even though the healthcare institution may be required by contractual obligation12 to teach students or trainees and to formulate teaching materials, this contractual obligation cannot be a requirement for the provision of medical care to John. Other considerations As good practice, Health Organisation ABC should consider if it is able to achieve the same purposes without using personal data. For example, using anonymised datasets that do not relate to any identifiable individual. Health Organisation ABC will not need to obtain consent from individuals if the personal data in its possession is anonymised before use. Consent is also not required if Health Organisation ABC uses and discloses the anonymised	

		data13. If Health Organisation ABC intends to send a specified message to John's Singapore telephone number (e.g. to advertise a service provided by ABC), then the Do Not Call Provisions will apply (addressed in Part III below). Example: Collecting personal data of individuals to respond to an emergency John takes his father to Clinic ABC. His father has been suffering from a very high fever for a few days. During the doctor's examination, John's father suddenly collapses. Clinic ABC immediately calls an ambulance to transfer him to a hospital. This involves Clinic ABC disclosing John's father's personal data to the hospital and ambulance services. Clinic ABC and the hospital may collect, use and disclose John's father's personal data without consent to respond to an emergency that threatens his life or health. This is pursuant to the vital interests exception under paragraph 2 of Part 1 of the First Schedule to the PDPA14 . The hospital should also notify John's father, as soon as is practicable, of the collection, use or disclosure and the purpose for the collection, use or disclosure of his personal data. Example: Consent given for a purpose will cover activities undertaken for that purpose Before collecting, using or disclosing personal data, organisations must notify individuals of their purposes and obtain consent unless any exception in the PDPA applies. However, when specifying its purposes relating to personal data, an organisation is not required to specify every activity which it may undertake, but	

		rather its objectives or reasons for the collection, use or disclosure (as the case may be) of the personal data. Healthcare Institution XYZ has obtained John's consent for the collection, use and disclosure (to other healthcare institutions) of his personal data for the purpose of providing medical treatment to him. Healthcare Institution XYZ is not required to separately obtain John's consent to maintain his medical records on its database, or to disclose the relevant records to other healthcare institutions through the database, if such activities are undertaken for the purpose that John has consented to. Example: Consent obligation imposed on organisations, not on employees Doctor Mei Ling is the sole proprietor of Clinic ABC. Doctor Mei Ling: a) Employs Doctor Hussein as the second doctor at Clinic ABC. b) Engages Doctor Ravi as a locum doctor to stand in at the clinic when she is on holiday. Doctor Hussein is an employee of Clinic ABC. The PDPA provides that the Data Protection Provisions do not impose any obligations on any employee acting in the course of his or her employment with an organisation. Any act done or conduct engaged in by a person in the course of his employment will be treated as done or engaged in by his employer for purposes of the PDPA15. Hence, Clinic ABC will have to ensure compliance with the Consent Obligation in respect of the collection, use and disclosure of personal data by Doctor Hussein, unless any relevant exception applies. However, Doctor Hussein will be	

		held accountable if he egregiously mishandles the personal data in the possession of or under the control of Clinic ABC16 or if he was not acting in the course of his employment when collecting, using or disclosing personal data. The specific Data Protection Provisions relevant for the locum doctor Doctor Ravi will depend, among other things, on the arrangements between Doctor Ravi and Clinic ABC, such as whether Doctor Ravi is processing personal data for the purposes of Clinic ABC pursuant to a written contract or whether Doctor Ravi was engaged as an employee of Clinic ABC. If Doctor Ravi is not an employee of Clinic ABC, the exclusion for employees will not apply to him and he may thus be subject to the Data Protection Provisions. If, however, Clinic ABC engages Doctor Ravi as an employee, then Clinic ABC will have to ensure compliance with the Consent Obligation in respect of the collection, use and disclosure of personal data by Doctor Ravi, unless any relevant exception applies. Doctor Mei Ling should ensure that Clinic ABC's contractual arrangements with Dr Hussein and Dr Ravi are consistent with the Data Protection Provisions in the PDPA and any other applicable legislation. Example: Acquisition of medical practice by another organization Doctor Mei Ling has been the sole proprietor of Clinic ABC. She retires and transfers her business to Doctor Hussein. She wants to give him access to all of her patients' personal data. In this scenario, paragraph 1 of Part 4 of the First Schedule to the PDPA relating to business	

		asset transactions could apply, subject to the conditions stated. Doctor Hussein is allowed to collect, use or disclose personal data about Doctor Mei Ling's patients without consent, as a party to a business asset transaction (the business transfer) with Doctor Mei Ling, to the extent that personal data collected relates directly to the part of the organisation or its business assets with which the business asset transaction is concerned. Example: Using personal data for a research purpose without consent Health Organisation ABC wishes to conduct retrospective research studies using medical records of individuals collected many years ago from its various patient databases, including both its research and administrative databases. The purpose of this research is to gain a better understanding of the epidemiology of diseases and socio-demographic characteristics of past patients which would influence ABC's public health strategies. The research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form. The researcher's institutional review board (IRB) has also determined that this research is not regulated under the Human Biomedical Research Act (HBRA). Health Organisation ABC did not retain the contact information of those individuals and has no knowledge of whether these patients have passed away or have relocated to another country. Hence it would be impracticable for Health Organisation ABC to seek	

		consent from the individuals for the use. Health Organisation ABC has no intention of contacting these patients to ask them to participate in the research. In addition, the results of the research will not be used to make specific decisions affecting the individuals and the benefits to be derived from the research are clearly in the public interest. In this case, Health Organisation ABC is able to use personal data about these individuals without consent, pursuant to the research exception in Division 3 under Part 2 of the Second Schedule to the PDPA. Health Organisation ABC also wishes to publish the results of its research in its website and newsletter. The results must be represented in a form that does not identify the past patients. Health Organisation ABC may also wish take into account the opinion of its Institutional Review Board ("IRB"), or equivalent body, which provides ethics approval for research projects.	
35	Advisory Guidelines for the Telecommunication Sector		
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act	Duties and responsibilities of the tied agent in respect of the PDPA obligations and any applicable requirements of the life insurer The Consent, Purpose Limitation and Notification Obligation 1 – Consent Obligation in PDPA An organisation must obtain the consent of the individual before collecting, using or disclosing his personal data for a purpose. This requirement to obtain consent does not apply where collection, use or disclosure of an	

		individual's personal data without consent is required or authorised under the PDPA or any other written law. An organisation may not, as a condition of providing a product or service, require the individual to consent to the collection, use or disclosure of his personal data beyond what is reasonably required to provide that product or service. Organisations must allow individuals to withdraw any consent given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose by an organisation at any time. The individual must give reasonable notice of the withdrawal to the organisation. On receipt of the notice, the organisation must inform the individual of the consequences of withdrawing consent, and must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be. 2 – Purpose Limitation Obligation in PDPA An organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, have been notified to the individual concerned. 3 – Notification Obligation in PDPA An organisation must notify the individual of the purpose(s) for which it intends to collect, use or disclose the individual's personal data on or before such collection, use or disclosure of the personal data. 10. Where the tied agent collects, uses or discloses personal data on behalf of the life insurer for	

		the purposes of the life insurer (e.g. to conduct the business of the life insurer), he is required to adhere to all the following requirements in this section. Generally, the tied agent should ensure compliance with all the internal data protection policies and procedures of the life insurer he represents. 11. The collection of personal data can be through any means, and recorded on hard or soft copy. This includes but is not limited to collection of personal data through face-to-face survey and through the use of online forms. 12. The tied agent shall: a) only collect, use or disclose any personal data of an individual for the following purposes: i. soliciting business for the life insurer; or ii. servicing of any policies of the life insurer for which the tied agent is authorised to service; or iii. performing any activities authorised by the life insurer; b) only collect, use or disclose personal data when valid consent has been obtained, unless otherwise required or authorised under the PDPA or any other written law.The PDPA permits the collection, use and disclosure of personal data without consent in the circumstances provided in the Second Schedule (Collection of personal data without consent), Third Schedule (Use of personal data without consent) and Fourth Schedule (Disclosure of personal data without consent) to the PDPA respectively; c) inform the appointed person of the life insurer of any notice received from an individual to withdraw his consent for the collection, use or disclosure of	

		his personal data as soon as reasonably possible; and d) upon receipt of such notice of withdrawal the tied agent shall also cease to collect, use or disclose the personal data, as the case may be. 6 13. The tied agent shall inform the individual of the likely consequences of the withdrawal of consent, unless otherwise instructed by the insurer. How the Consent, Purpose Limitation and Notification Obligation applies to different stages of the personal data life cycle Stage A: Leads Generation or Prospecting 14. Stage A describes the phase where the tied agent is collecting, using or disclosing personal data for the purposes of generating leads, prospecting, or recruitment of agents. Collection of Personal Data through Referrals 15. The tied agent may collect personal data in situations where the personal data (typically the name and contact number of an individual) is obtained from a third party source (e.g. obtaining personal data from a referrer who is a friend of the individual being referred). 16. The tied agent collecting personal data from a third party source is required to notify the source of the purposes for which the tied agent will be collecting, using and disclosing the personal data 17. The tied agent should exercise the appropriate due diligence to check and ensure that the third party source can validly give consent for the collection, use and disclosure of personal data on behalf of the individual or that the source had obtained consent for disclosure	

		of the personal data. Due diligence includes but is not limited to checking with the third party referrer that the individual being referred has agreed to let the tied agent contact him. 18. If the tied agent intends to send a telemarketing message to a Singapore telephone number of the individual being referred, the tied agent must check the DNC Registry first, unless he has obtained clear and unambiguous consent in evidential form from the individual.7 Example: Mark, a tied agent, asks Sarah his client: "Can you give me a referral whom you think will be alright for me to call? Can I mention your name?" Jane provides her personal data to Sarah for disclosure to Sarah's life insurance agent to contact her about life insurance matters. Sarah decides to provide the personal data of her friend Jane to Mark. Before recording Jane's personal data, Mark asks Sarah a few questions to determine if Jane has agreed to the disclosure of her personal data for such purposes. After obtaining verbal confirmation from Sarah in the affirmative to those questions, Mark proceeded to collect Jane's personal data. Mark is likely to have exercised appropriate due diligence in this situation. As a best practice, when contacting Jane for the first time, Mark should inform Jane that her personal data was disclosed by Sarah and verify that Jane had provided consent to do so. For example, Mark could say: "Hello Jane. My name is Mark from Insurer ABC. Your friend Sarah gave me your name for the purpose of contacting you	

		about life insurance matters. Would it be alright to continue this conversation?" Please note, however, that if Jane's Singapore telephone number is registered on the DNC Registry, Mark will not be able to contact Jane merely based on the above, as there is no evidence of Jane's clear and unambiguous consent to the sending of a telemarketing message to her telephone number, whether in written or other form so as to be accessible for subsequent reference. 19. If required by the life insurer he represents, the tied agent shall, in accordance with those requirements, record the confirmation of the referrer. In some cases, the life insurer may require the referrer to provide written confirmation using a prescribed form provided by the life insurer. Collection of Personal Data through Road Show, House-to-House or Street Prospecting, and the Like 20. The tied agent may collect personal data directly from an individual during a road show, or in other circumstances in the process of solicitation. 21. When collecting such personal data from the individual, the tied agent shall clearly notify the individual of the purpose(s) for collecting, using or disclosing his personal data. 22. If the individual consents to those purposes, the tied agent shall, subject to the requirements of the life insurer he represents, record that consent has been provided by the individual. The tied agent may request the individual to provide written confirmation using a prescribed form provided by the life insurer.	

		Stage B: Fact-Finding and Insurance Application 23. In this stage, the tied agent may collect personal data from an individual for the purposes of factfinding and/or application for the insurance. Notifying an individual of the purposes for which his personal data will be collected, used or disclosed8 24. On or before collecting personal data from the individual, the tied agent shall clearly notify the individual of the purposes for the collection, use or disclosure of his personal data. 25. The tied agent shall use the prescribed form(s) approved by the life insurer he represents to collect the personal data. These form(s) will state the purposes for which the personal data is collected, used or disclosed. 26. The tied agent shall ensure that the applicant reflects his consent in the relevant form(s) provided by the life insurer. Stage C: Post-Policy Inception 27. Stage C describes the phase where the tied agent may be collecting, using or disclosing personal data in relation to an insurance policy contract that has been issued to an individual. Collection, use or disclosure of an individual's personal data for the purpose of servicing a policy 28. If valid consent has been obtained, the tied agent can collect, use or the individual's personal data for activities within the purpose of servicing a policy which the individual has purchased ("servicing a policy"). 29. As an illustrative example, the purpose of "servicing a policy" could include the following activities: • assisting the individual to make a claim under a policy for	

		insurance benefit • terminating a policy • facilitating fund switches • informing the life insurer of a change of address or telephone number(s) • sending reminders to the individual that a policy payment is due • conducting a reassessment of the individual's life insurance needs pursuant to Paragraph 34 in MAS Notice FAA-N16 and Guidelines FAA-G11 Paragraph 3.3.5 30. The tied agent shall use the prescribed form provided by the life insurer (if applicable) when conducting such activities. If required by the life insurer, the tied agent shall ensure that the individual reflects his consent to these activities in the relevant form(s).	

#	Regulation		
		necessary for compliance with a legal obligation	necessary in order to protect the vital interests
1	Personal Data Protection Act 2012	(b) the collection, use or disclosure (as the case may be) without the individual's consent is required or authorised under this Act or any other written law.	PART 1 VITAL INTERESTS OF INDIVIDUALS 1.—(1) Subject to sub-paragraph (2), the collection, use or disclosure (as the case may be) of personal data about an individual is necessary for any purpose which is clearly in the individual's interests, and — (a) consent for the collection, use or disclosure (as the case may be) cannot be obtained in a timely way; or (b) the individual would not reasonably be expected to withhold consent. (2) Where the organisation collects, uses or discloses (as the case may be) personal data about the individual under sub-paragraph (1), the organisation must, as soon as is practicable,

			notify the individual of the collection, use or disclosure (as the case may be) and the purpose for the collection, use or disclosure, as the case may be.
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare		

	Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment		
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act		
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		

24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions		
26	Advisory Guidelines on Application of PDPA to Election Activities	3 RIGHTS AND OBLIGATIONS ETC UNDER OTHER LAWS 3.1 Section 4(6) of the PDPA states that unless otherwise provided in the PDPA, nothing in Parts 3 to 6A of the PDPA shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening the PDPA, and the provisions of other written law shall prevail to the extent that any provision of Parts 3 to 6A is inconsistent with the provisions of that other written law. Other provisions in the PDPA which are not inconsistent with other written law will continue to apply. 3.2 Political parties and election candidates should ensure that they comply with relevant laws and regulatory requirements governing election activities ("relevant laws")7. For example, under the Parliamentary Elections Act 1954, political parties and election candidates8 may purchase a copy of the registers of electors and use the information in the registers only for communicating with electors. Political parties and election candidates may therefore collect, use or disclose such information, without obtaining consent under the PDPA, to the extent that such collection, use or disclosure is for the purpose of communicating with electors in accordance with the Parliamentary Elections Act	

		1954. 3.3 For the avoidance of doubt, whilst political parties and election candidates may collect, use or disclose personal data without consent where permitted under other relevant legislation, other Data Protection Provisions under the PDPA will still apply to the extent that they are not inconsistent with other legislation. Consent Obligation 4.2 A political party or election candidate must obtain the consent of the individual before collecting, using or disclosing his or her personal data for a purpose, unless the collection, use or disclosure without consent is required or authorised under the PDPA or other written law. This would include the personal data of employees (including election agents and volunteers) and potential voters. 4.3 A political party or election candidate that takes a photograph of an identifiable individual will be required to obtain consent, unless an exception applies. In particular, there is an exception for the collection, use and disclosure of personal data that is publicly available9. For example, when the individual appears at an event or location that is open to the public, taking a photograph of the individual10 would likely constitute collection of personal data that is publicly available for which consent is not required. Nevertheless, as a matter of good practice, political parties and election candidates should still provide signage or other forms of obvious notice to notify the public that photography is taking place and for what purpose(s). To be clear, other	

		Data Protection Provisions under the PDPA still apply to personal data that is publicly available, such as the Protection, Purpose Limitation, Access, Correction, and Accuracy Obligations. 4.4 A political party or election candidate may only collect, use or disclose personal data from a third party source, if the third party source can validly give consent on behalf of the individual for the collection, use or disclosure of his or her personal data; or the individual has provided consent to the disclosure of his or her personal data by the third party to the political party or election candidate for their intended purposes, unless an exception11 applies. As good practice, where a political party or election candidate has obtained the individual's personal data from a third-party source, that political party or election candidate should inform the individual, upon request, of how his or her personal data was obtained by the political party or election candidate. 4.5 The political party or election candidate must allow an individual to withdraw his or her consent12 for the collection, use or disclosure of his or her personal data for a purpose13. As good practice, political parties or election candidatesshould keep a list of individuals who have exercised their right to withdraw their consent for the collection, use or disclosure of his or her personal data. 4.6 Political parties and election candidates are reminded that the collection, use or disclosure of such personal data must be in accordance with the relevant laws governing election activities, and political parties	

		and election candidates also must not obtain, or attempt to obtain, consent by providing false or misleading information or using deceptive or misleading practices. 4.7 A political party or election candidate may continue to use the personal data of individuals that was collected before 2 July 2014 for the purposes for which it was collected, unless consent is withdrawn under the PDPA or the individual had otherwise indicated that he or she does not consent to such use. Fresh consent is required for the use of such personal data for new purposes. 4.8 A political party or election candidate is not required to obtain consent before collecting, using or disclosing any business contact information, or to comply with any other obligation in the Data Protection Provisions in relation to business contact information. Under the PDPA, business contact information refers to an individual's name, position name or title, business telephone number, business address, business electronic mail address, or business fax number and any other similar information about the individual, not provided by the individual solely for his or her personal purposes14.	
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers	3 Collection, use or disclosure of NRIC numbers (or copies of NRIC) 3.1 Organisations are generally not allowed to collect, use or disclose NRIC numbers (or copies of NRIC). They may do so only in the following specified circumstances: a) Collection, use or disclosure of NRIC numbers (or copies of NRIC) is required under the law (or an exception under the PDPA	

		applies); or b) Collection, use or disclosure of NRIC numbers (or copies of NRIC) is necessary to accurately establish or verify the identities of the individuals to a high degree of fidelity. Collection, use or disclosure of NRIC numbers (or copies of NRIC) is required under the law (or an exception under the PDPA applies) 3.2 Organisations may collect, use or disclose an individual's NRIC number (or copy of NRIC) without his or her consent if it is required under the law11. As good practice, organisations should still notify the individual of the purpose for the collection, use or disclosure, as the case may be. 3.3 The following are some examples of situations where the collection, use or disclosure of NRIC numbers (or copies of NRIC) is required under the law. 3.10 In addition, there could be situations where there is an applicable exception under the Second, Third or Fourth Schedule of the PDPA such that the consent of the individual to collect, use or disclose his or her NRIC number (or copy of NRIC) is not required. Nonetheless, organisations must still ensure that its conduct is reasonable in the circumstances. Necessary to accurately establish or verify the identity of the individual to a high degree of fidelity 3.12 Where an organisation finds it necessary to accurately establish or verify the identity of the individual to a high degree of fidelity, it may collect, use or disclose his or her NRIC number with notification and consent. 3.13 PDPC would generally consider it necessary to	

		accurately establish or verify the identity of individual to a high degree of fidelity in the following situations – a) Where the failure to accurately identify the individual to a high degree of fidelity may pose a significant safety or security risk. For example, visitor entry to preschools where ensuring the safety and security of young children is an overriding concern; or b) Where the inability to accurately identify an individual to a high degree of fidelity may pose a risk of significant impact or harm14 to an individual and/or the organisation (e.g. fraudulent claims). Such transactions typically relate to healthcare, financial or real estate matters, such as property transactions, insurance applications and claims, applications and disbursements of substantial financial aid, background credit checks with credit bureau, and medical check-ups and reports. 3.14 The above are illustrative and not intended to be exhaustive as to the types of situations that would be considered necessary to accurately establish or verify the identity of the individual to a high degree of fidelity. Organisations should assess whether their specific situation meets the above considerations before collecting the individual's NRIC number (or copy of NRIC). In collecting the NRIC number (or copy of NRIC), organisations should be able to provide justification15 on request of either the individual or the PDPC as to why the collection, use or disclosure of the NRIC number (or copy of NRIC) is necessary to	

		accurately establish or verify the identity of the individual to a high degree of fidelity. 3.15 Organisations should note that when they collect a copy of the NRIC, they are considered to have collected all the personal data on the NRIC, and will be subject to the Data Protection Provisions of the PDPA for that collection. Organisations should assess whether they are collecting excessive personal data contained in the copy of the NRIC for the intended purpose, and if they could adopt alternatives to the individual's NRIC number or copy of NRIC. 3.16 Where the collection of the NRIC number (or copy of NRIC) is necessary to accurately establish or verify the identity of the individual to a high degree of fidelity, it would generally be considered reasonable for the organisations to require the consent of the individual to collect, use or disclose his or her NRIC number for the stated purpose16.	
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		
29	Advisory Guidelines for Management Corporations		
30	Advisory Guidelines for the Education Sector		Exceptions to the Consent Obligation 2.19 The PDPA permits the collection, use and disclosure of personal data without consent (and in the case of collection, from a source other than the individual) in circumstances provided in the Second (collection of personal data without consent), Third (use of

			personal data without consent) and Fourth Schedules (disclosure of personal data without consent) to the PDPA respectively. Such exceptions include where the collection, use or disclosure of personal data is necessary for evaluative purposes9. However, these exceptions to the Consent Obligation do not affect rights or obligations by or under other law. For example, even if an exception applies under the PDPA, organisations are required to comply with legal obligations of confidentiality that they may have. 2.20 Examples: Exceptions to the Consent Obligation for evaluative purposes David applies for admission to School ABC, an educational institution. He lists School XYZ as the current educational institution he is enrolled in. School ABC requires David's performance records in School XYZ to evaluate his suitability of admission into School ABC and requests for a copy of such records from School XYZ. In this case, consent is not required for School ABC to collect and use such personal data necessary to evaluate David's eligibility for admission to School ABC. Similarly, consent is not required for School XYZ to disclose such personal data to School ABC for the evaluative purpose. 2.21 Peggy is one of School ABC's scholarship recipients. The scholarship is only available for students with excellent conduct, class participation and examination results. School ABC uses the teachers' assessment of Peggy's conduct in class to determine whether the scholarship should be continued in its annual review of

			scholarship holders. In this scenario, School ABC is not required to obtain consent from Peggy to use her personal data as this falls within the exception in the Third Schedule to the PDPA for evaluative purposes. 2.22 Example: Disclosure of personal data to a public agency for policy formulation or review At the end of each academic year, School ABC compiles and submits a list of names, ages, addresses and examination grades for each subject of the students enrolled with the school to a public agency. The public agency uses the data to understand the performance trends of the categories of students enrolled in schools like ABC for its annual policy review. In this case, School ABC is not required to obtain the consent of the students to disclose their personal data to the public agency as there is an exception in the Fourth Schedule to the PDPA for disclosure of personal data of current or former students of an education institution to a public agency for the purposes of policy formulation or review. 2.23 Example: Disclosure of personal data without consent in an emergency situation Following a physical education class, Alan suddenly develops dizzy spells and faints. Alan is admitted into a hospital nearby, and Alan's teacher, Sue, provides the medical staff with Alan's personal data such as his full name, blood type and allergies. Sue may disclose Alan's personal data without consent, as there is an applicable exception under the Fourth Schedule to the PDPA for the disclosure of Alan's personal data that is necessary to respond

			to an emergency that threatened his health.
31	Advisory Guidelines for the Social Service Sector		Exceptions for collection, use or disclosure of personal data without consent 3.20 The PDPA permits the collection, use and disclosure of personal data without consent (and in the case of collection, from a source other than the individual) in circumstances provided in the First (collection, use and disclosure of personal data without consent), Second (additional bases for collection, use and disclosure of of personal data without consent) Schedules to the PDPA. 3.21 Such exceptions include where the collection, use or disclosure of personal data is necessary for evaluative purposes (such as in relation to the grant of financial or social assistance, or the delivery of appropriate health services, under any scheme administered by a public agency) 9. However, these exceptions to the Consent Obligation do not affect rights or obligations by or under other laws. For example, even if an exception applies under the PDPA, organisations are required to comply with any legal obligations of confidentiality that they may have. 3.22 Example: Disclosure of personal data without consent in an emergency situation Maggie works at a day care centre for senior citizens. One day, an elderly client at the centre, Mr. Tan, falls ill after his meal and has to be admitted to the hospital. Maggie provides the hospital staff with Mr. Tan's personal data such as his full name, NRIC number, and medical allergies. Treatment Maggie may disclose Mr. Tan's personal data without consent,

			as there is an applicable exception under the paragraph 2 of Part 1 of the First Schedule to the PDPA which relates to the disclosure of an individual's personal data, without consent, that is necessary to respond to an emergency that threatened, among other things, his health. 3.23 Example: Exception to the Consent Obligation for evaluative purposes Don is an employee of SSA DEF that provides social and recreational activities and food rations to low-income households. He receives a call from Audrey, a social worker with SSA 123. Audrey enquires on the services that one of SSA DEF's clients, Mr. Ong, had been receiving, and to understand Mr. Ong's financial situation. Audrey explains to Don that Mr. Ong had approached SSA 123 recently to apply for their pilot social assistance scheme administered by a public agency10. Treatment In this case, consent is not required for SSA 123 to collect and use Mr. Ong's personal data if the collection or use is necessary for an evaluative purpose 11 (e.g. to determine Mr. Ong's suitability or eligibility for grant of social assistance under the scheme administered by the public agency). Similarly, consent is not required for SSA DEF to disclose Mr. Ong's personal data to SSA 123 if the disclosure is necessary for an evaluative purpose12. Both SSA 123 and SSA DEF should also ensure that they remain compliant with relevant sectoral laws and regulatory requirementssuch as data sharing agreements between SSA 123 and SSA DEF.

			Business improvement exception 3.24 The business improvement exception allows organisations to use, without consent, personal data they have collected for business improvement purposes, such as developing new goods or services and understanding individual behaviour and preferences. To rely on this exception, organisations must ensure that the purpose cannot be reasonably achieved without using the data in an individually identifiable form and that the use of the data is one that a reasonable person would consider appropriate in the circumstances13. 3.25 Subject to certain conditions being fulfilled, the business improvement exception also permits the sharing of personal data between entities belonging to a group of companies, without consent, for improving goods and services, developing new business methods or processes, understanding behaviour and preferences of customers, and identifying suitable goods and services for customers. 3.26 This exception cannot be used to send direct marketing messages to individuals, for which explicit consent must generally be obtained. For further information on the business improvement exception, please refer to paragraphs 12.71 – 12.77 of the Key Concepts Guidelines. 3.27 Example: Use of personal data to improve client services SSA ABC wants to use its clients' personal data (i.e. age, type of services requested)to derive insights on client demographics to better tailor the services it provides to its clients and improve its outreach to them. SSA ABC assesses that (a) this

			purpose cannot reasonably be achieved without the use of personal data in individually identifiable form; and (b) its use of personal data is considered appropriate to a reasonable person. Treatment SSA ABC may rely on the business improvement exception to use its clients' personal data without consent to understand them better and to enhance the services it provides them. However, if SSA ABC assesses that this purpose can reasonably be achieved without the use of personal data in individually identifiable form, it may not rely on the business improvement exception. Instead, SSA ABC may consider anonymising the data before using it for such a purpose. Anonymisation is the process of removing identifying information, such that the remaining data does not identify any particular individual. Personal data that has been anonymised is no longer considered personal data for the purposes of the PDPA.14 3.28 Example: Use of personal data to better understand donors SSA DEF wants to use its donors' personal data (i.e. frequency of donation) to derive insights about their profiles and contributions to improve its donor retention rate. SSA DEF assesses that (a) this purpose cannot reasonably be achieved without the use of personal data in individually identifiable form; and (b) its use of personal data is considered appropriate to a reasonable person. Treatment SSA DEF may rely on the business improvement exception to use its donors' personal data

			without consent to understand them better. Legitimate interests exception 3.29 In general, "legitimate interests" refer to any lawful interests of an organisation or person, including other organisations. Part 3 of the First Schedule to the PDPA outlines specific purposes that would generally be considered "legitimate interests," such as evaluation, investigation, or debt recovery. It also sets out a broad exception that can be relied on for other purposes that meet the definition of "legitimate interests." 3.30 Before relying on the legitimate interests exception, organisations must identify and articulate the legitimate interests, conduct an assessment to identify and mitigate any adverse effects on individuals, and disclose reliance on the exception. The Commission uses a commercially reasonable standard to assess the appropriateness of the mitigatory measures. Examples of reasonable measures include minimizing the amount of personal data collected, implementing access controls, deleting personal data immediately after use. Organisations should also provide the business contact information of a person who can address individuals' queries about their reliance on the exception. 3.31 This exception cannot be used to send direct marketing messages to individuals, for which explicit consent must generally be obtained. For further information on the "legitimate interests" exception, please refer to paragraphs 12.56

			– 12.70 of the Key Concepts Guidelines. 3.32 Example: Fraud detection and prevention of misuse of services SSA ABC intends to use personal data about its clients and their use of its services to detect fraud and prevent the misuse of its services, where one client attempts to receive the same services multiple times. SSA ABC conducts an assessment of legitimate interests, and assesses that the benefits of the use of personal data (e.g. preventing fraud or misuse of services) is in the legitimate interests of SSA ABC and outweigh any likely adverse effect to the individual client (e.g. potential enforcement actions by authorities). SSA ABC also states in its data protection policy on its website that it is relying on the legitimate interest exception to use personal data to detect fraud and prevent misuse of services. Treatment SSA ABC may rely on the legitimate interests exception to use personal data about its clients and their use of its services to detect fraud and prevent the misuse of services. 3.33 Example: Recording of residential facilities for safety and security of residents SSA ABC provides residential facilities for the shelter and care of some of its clients. It wants to monitor and record, via CCTV, some portions of the residential facilities for the safety and security of its residents. SSA ABC conducts an assessment of legitimate interests, and assesses that the benefits of the collection, use and disclosure of personal data through the recording of the residential facilities (e.g. detect if

			any residents have injured themselves, deter break-ins to the residential facilities) is in the legitimate interests of SSA ABC and outweigh any likely adverse effect to the individual. SSA ABC also states in its intake form for prospective residents that it is relying on the legitimate interests exception to collect, use, and disclose personal data for the safety and security of all its residents. Treatment SSA ABC may rely on the legitimate interests exception to collect, use, and disclose personal data through CCTV recordings of some portions of its residential facilities to protect the safety and security of its residents. As good practice, SSA ABC may wish to put up notices to inform individuals that the areas are under CCTV surveillance. To comply with the Protection Obligation of the PDPA, SSA ABC implements reasonable security arrangements to protect the CCTV surveillance footage, such as encrypting the footage in the database and restricting employee access to the footage on a need-to-know basis. 3.34 Example: Recording of counselling sessions to improve supervision and delivery of casework by social worker SSA DEF provides counselling services to its clients at its premises. It wants to record the counselling sessions, via CCTV, to improve the supervision and delivery of casework by the social worker or counsellor. SSA DEF conducts an assessment of legitimate interests, and assesses that the benefits of the collection, use and disclosure of personal data through the recording of the

			sessions (e.g. provide a more conducive environment and better counselling services for the clients) is in the legitimate interests of SSA DEF and outweigh any likely adverse effect to the individual client (e.g. minor discomfort of being watched). SSA DEF also states in its counselling session intake form that it is relying on the legitimate interests exception to collect, use, and disclose personal data to deter undesirable behaviour by counselling clients. Treatment SSA DEF may rely on the legitimate interests exception to collect, use, and disclose personal data through CCTV recordings of counselling sessions to improve supervision and performance of the social worker or counsellor. As good practice, SSA DEF may wish to put up notices to inform its clients that the counselling sessions are under CCTV surveillance. To comply with the Protection Obligation of the PDPA, SSA DEF implements reasonable security arrangements to protect the CCTV surveillance footage, such as encrypting the footage in the database and restricting employee access to the footage on a need-to-know basis. 3.35 Example: Recording of helpline calls on domestic abuse SSA 123 provides a helpline service to its clients. It wants to record the helpline calls regarding domestic abuse suffered by its clients. The purpose of the recording is to equip SSA 123 to better fulfil its responsibilities to such clients, such as providing the client with the necessary support and taking action on their behalf.

			SSA 123 conducts an assessment of legitimate interests, and assesses that the benefits of the collection, use and disclosure of personal data through the recording of the helpline calls is in the legitimate interests of SSA 123, and outweigh any likely adverse effect to the individual client. SSA 123 also states in its data protection policy on its website that it is relying on the legitimate interests exception to collect, use, and disclose personal data to provide better services to its clients. Treatment SSA 123 may rely on the legitimate interests exception to collect, use, and disclose personal data through the recording of helpline calls regarding domestic abuse suffered by its clients to better fulfil its responsibilities to such clients. 3.36 Example: Joint assessment for better coordination of social services Madam Koh, a client with multiple social and medical needs, approaches SSA ABC to apply for social service assistance. While interviewing Madam Koh during the application process, Peter, a social worker at SSA ABC, found out that Madam Koh has also been receiving social services from SSA XYZ. Peter believes there could be better coordination between the two SSAs in terms of providing social services to Madam Koh. Peter proceeds to call Paula from SSA XYZ (whose name was shared by Madam Koh as the social worker handling her case) to invite Paula to a case conference and to discuss possible options to render

			assistance to Madam Koh. The case conference is likely to involve the mutual disclosure of Madam Koh's personal data such as her medical history, family conditions, services that Madam Koh is currently receiving, or has received in the past, by both SSA ABC and SSA XYZ, as represented by Peter and Paula. SSA ABC and SSA XYZ conduct a joint assessment of legitimate interests, and assess that the benefits of the disclosure of Madam Koh's personal data (e.g. prevent overlapping services and ensure fair distribution of welfare resources for all clients) is in the legitimate interests of both SSA ABC and SSA XYZ, and outweigh any likely adverse effect to the individual (e.g. minor embarrassment to Madam Koh if data about her family condition is leaked). Both SSAs also include in their respective data protection policies on their websites that they are relying on the legitimate interests exception to disclose personal data for better coordination of social services and management of resources. Treatment SSA ABC and SSA XYZ may rely on the legitimate interests exception to disclose personal data of their clients to one another to ensure better coordination of social services and management of resources. 3.37 Example: Disclosing existing personal data to volunteers to conduct surveys SSA DEF provides caregivers to patients, to discuss medical procedures with them and provide support mentally to them. To garner feedback and improve their caregiving services, SSA DEF engages

			volunteers to visit the homes or the hospital wards of patients to conduct a face-to-face survey. The personal data of patients (e.g. names, medical conditions, home addresses and location of hospital wards) that were previously collected by SSA DEF for provision of care to the patients are provided to the volunteers to visit the homes/hospital wards of patients and conduct the face-to-face surveys. Treatment SSA DEF wishes to rely on deemed consent by notification. It conducts an assessment to identify any adverse effect and determines that there are no likely adverse effects on the patients in using their personal data for this new purpose. SSA DEF assesses those 14 days is a reasonable period for the patients to opt out. It also assesses that notifying the patients through a message sent by the caregivers using a communication channel (e.g. WhatsApp) that the patients are used to, that their personal data would be used to conduct face-to-face surveys for the stated purpose, and of the opt-out period is an appropriate and effective method of notification. In the message to the patients, SSA DEF notifies the patients that they may opt out of the surveys by replying to the message within 14 days from the date of the message. Patients who do not opt out within the 14-day opt-out period are deemed to have consented to the collection, use and disclosure of their personal data for this purpose. However, SSA DEF will allow and facilitate any withdrawal of consent from the patients after the 14-day opt-out

			period. Alternatively, SSA DEF may rely on the legitimate interests exception if it conducts an assessment and determines that the benefits of the collection and use of personal data (e.g. names, medical conditions, home addresses and location of hospital wards) for volunteers of SSA DEF to visit the homes/hospital wards to conduct face-to-face surveys with the patients is in the legitimate interests of SSA DEF and outweigh any adverse effect on the patients. SSA DEF also states in the caregiver application form that it is relying on the legitimate interests exception to collect and use personal data for the purpose of improving caregiving services through conducting of face-to-face surveys by volunteers. Obtaining consent from source(s) other than the individual 3.38 The Commission is aware that in some circumstances, an organisation may obtain personal data about an individual with the consent of the individual, but from a source other than an individual ("third party"). These may include: a) Where the third party source can validly give consent to the collection, use and disclosure of the individual's personal data; or b) Where the individual has consented, or is deemed to have consented to the disclosure of his or her personal data by the third party source. 3.39 SSAs may wish to consider how best to obtain consent from clients who are individuals that may not have the capacity to give consent for themselves, such as a client who is mentally unwell, or is a minor15. In this regard, the Data Protection Provisions do

			not affect any authority, right, obligation or limitation under other laws and SSAs should accordingly ensure compliance with other laws such as the Mental Capacity Act. 3.40 Examples: Consent for collection of personal data from third parties Adam, an only child who lives with his elderly parents, has not been able to find a job for a year. He learns about a financial assistance programme offered by SSA ABC and decides to apply for it. As part of its enrolment process, SSA ABC requires all applicants to provide the personal data of family members living in the same household, including their full names, and employment status. SSA ABC collects and uses these personal data to evaluate a client's suitability for its programme. Adam had not obtained either parent's consent before disclosing their personal data to SSA ABC. Treatment Before disclosing personal data of an individual, the consent of the individual should typically be obtained, unless an exception applies. In this case, SSA ABC can collect Adam's parents' personal data from Adam without his parents' consent, pursuant to Paragraph 8 of Part 3 of the First Schedule to the PDPA. This exception relates to a situation where personal data of an individual (i.e. Adam's parents) was provided to the organisation (i.e. SSA ABC) by another individual (i.e. Adam) to enable the organisation to provide a service for the personal or domestic purposes of that other individual (i.e. Adam).

			SSA ABC should also ensure that it remains compliant with relevant sectoral laws and regulatory requirements. 3.41 Madam Lim visits SSA ABC and chats with Robert, who is employed by SSA ABC as a social worker, to find out more about a new social assistance programme which it is launching next month. Robert assesses that Madam Lim does not meet the requirements to qualify for SSA ABC's programme, but intends to refer Madam Lim to a programme offered by SSA XYZ. Robert obtains Madam Lim's consent to disclose her personal data to SSA XYZ as part of the professional referral process. Treatment Before SSA XYZ collects Madam Lim's personal data from SSA ABC (through SSA ABC's employee Robert), SSA XYZ should exercise due diligence to check and ensure that SSA ABC had obtained consent from Madam Lim to disclose her personal data. In this scenario, SSA XYZ is obtaining Madam Lim's personal data from a third party source – SSA ABC. Organisations should adopt appropriate measures to verify that the third party source has obtained consent from the individual concerned. Depending on the circumstances, this may be met by obtaining the individual's consent in writing or in other evidential form through the third party, or obtaining and documenting in an appropriate form, verbal confirmation from the third party that the individual has given consent. In addition, SSA XYZ could, as good practice, verify with Madam Lim when contacting her for the

			first time that she had provided consent through SSA ABC for SSA XYZ to contact her. Please refer to Chapter 12 of the Key Concepts Guidelines for more information on considerations when collecting personal data from third party sources.
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector		
34	Advisory Guidelines for the Healthcare Sector		
35	Advisory Guidelines for the Telecommunication Sector		
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		

#	Regulation		
		necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	necessary for the purposes of the legitimate interests pursued by the controller or by a third party
1	Personal Data Protection Act 2012	PART 2 USE OF PERSONAL DATA Division 1 — Public interest 1. The use of personal data about an individual, if — (a) the personal data was	PART 3 LEGITIMATE INTERESTS 1.—(1) Subject to sub-paragraphs (2), (3) and (4) — (a) the collection, use or disclosure (as the case may be)

		disclosed by a public agency; and (b) the use of the personal data by the organisation is consistent with the purpose of the disclosure by the public agency.	of personal data about an individual is in the legitimate interests of the organisation or another person; and (b) the legitimate interests of the organisation or other person outweigh any adverse effect on the individual. (2) For the purposes of sub-paragraph (1), the organisation must — (a) conduct an assessment, before collecting, using or disclosing the personal data (as the case may be), to determine whether sub-paragraph (1) is satisfied; and (b) provide the individual with reasonable access to information about the organisation's collection, use or disclosure of personal data (as the case may be) in accordance with sub-paragraph (1). (3) The organisation must, in respect of the assessment mentioned in sub-paragraph (2)(a) — (a) identify any adverse effect that the proposed collection, use or disclosure (as the case may be) of personal data about an individual is likely to have on the individual; (b) identify and implement reasonable measures — (i) to eliminate the adverse effect; (ii) to reduce the likelihood that the adverse effect will occur; or (iii) to mitigate the adverse effect; and (c) comply with any other prescribed requirements. (4) Sub-paragraph (1) does not apply to the collection, use or disclosure of personal data about an individual for the purpose of sending to that individual or any other individual a message for an applicable purpose within the meaning

			given by section 37(6). 2. The collection, use or disclosure (as the case may be) of personal data about an individual is necessary for evaluative purposes. 3. The collection, use or disclosure (as the case may be) of personal data about an individual is necessary for any investigation or proceedings. 4. The collection, use or disclosure (as the case may be) of personal data about an individual is necessary for the organisation — (a) to recover a debt owed by the individual to the organisation; or (b) to pay to the individual a debt owed by the organisation. 5. The collection, use or disclosure (as the case may be) of personal data about an individual is necessary for the provision of legal services by the organisation to another person, or for the organisation to obtain legal services. 6.—(1) Subject to sub-paragraph (2), the collection, use or disclosure (as the case may be) of personal data about an individual — (a) is for the purpose of the preparation by a credit bureau of a credit report; or (b) relates to a credit report provided by a credit bureau to a member of the credit bureau in relation to a transaction between the member and the individual. (2) Sub-paragraph (1) does not apply to a credit bureau that, being required to obtain a licence under any other written law, does not hold such a licence. 7. The collection, use or disclosure (as the case may be) of personal data about an individual is to — (a) confer an interest or a benefit

			on the individual under a private trust or benefit plan; and (b) administer that trust or benefit plan, at the request of the settlor or the person establishing the benefit plan, as the case may be. 8. The personal data about an individual — (a) is provided to the organisation by another individual to enable the organisation to provide a service for the personal or domestic purposes of that other individual; and (b) is collected, used or disclosed (as the case may be) by the organisation solely for the purpose in sub-paragraph (a). 9. The personal data about an individual — (a) is included in a document produced in the course, and for the purposes, of the individual's employment, business or profession; and
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		Excluded purposes under section 15A(3) of Act 13. For the purposes of section 15A(3) of the Act, the prescribed purpose is the sending of a message to the individual for an applicable purpose specified in

			the Tenth Schedule to the Act. Assessment of effect of proposed collection, use or disclosure of personal data for purposes of section 15A of Act 14.—(1) This regulation applies where an organisation intends to collect, use or disclose personal data about an individual under section 15A(2) of the Act. (2) An assessment mentioned in section 15A(4)(a) of the Act to determine that a proposed collection, use or disclosure of personal data by an organisation is not likely to have an adverse effect on an individual must specify all of the following information: (a) the types and volume of personal data to be collected, used or disclosed, as the case may be; (b) the purpose or purposes for which the personal data will be collected, used or disclosed, as the case may be; (c) the method or methods by which the personal data will be collected, used or disclosed, as the case may be; (d) the mode by which the individual will be notified of the organisation's proposed collection, use or disclosure (as the case may be) of the individual's personal data; (e) the period within which, and the mode by which, the individual may notify the organisation that the individual does not consent to the organisation's proposed collection, use or disclosure (as the case may be) of the individual's personal data; (f) the rationale for the period and mode mentioned in sub-paragraph (e). (3) The organisation must retain a copy of its assessment mentioned in section 15A(4)(a) of the Act relating to the collection,

			use or disclosure of personal data about an individual throughout the period that the organisation collects, uses or discloses personal data about the individual under section 15A(2) of the Act. Assessment of effect of proposed collection, use or disclosure of personal data for purposes of Part 3 of First Schedule to Act 15.—(1) This regulation applies where an organisation intends to collect, use or disclose personal data about an individual under paragraph 1(1) of Part 3 of the First Schedule to the Act. (2) An assessment mentioned in paragraph 1(2)(a) of Part 3 of the First Schedule to the Act in respect of the intended collection, use or disclosure of personal data must — (a) specify — (i) the types and volume of personal data to be collected, used or disclosed, as the case may be; (ii) the purpose or purposes for which the personal data will be collected, used or disclosed, as the case may be; and (iii) the method or methods by which the personal data will be collected, used or disclosed, as the case may be; (b) identify any residual adverse effect on any individual after implementing any reasonable measures mentioned in paragraph 1(3)(b) of Part 3 of the First Schedule to the Act; (c) identify the legitimate interests that justify the collection, use or disclosure (as the case may be) by the organisation of personal data about the individual; (d) where the legitimate interests identified under sub-paragraph (c) relate to a person other than

			the organisation, identify that other person by name or description; and (e) set out the reasons for the organisation's conclusion that the legitimate interests identified under sub-paragraph (c) outweigh any adverse effect on the individual. (3) The organisation must retain a copy of the assessment it conducted in accordance with paragraph 1(2)(a) of Part 3 of the First Schedule to the Act relating to the collection, use or disclosure of personal data about an individual throughout the period that the organisation collects, uses or discloses personal data about the individual under paragraph 1(1) of Part 3 of the First Schedule to the Act.
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		

15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment		
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act		
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		

25	Advisory Guidelines on the Do Not Call Provisions		
26	Advisory Guidelines on Application of PDPA to Election Activities		
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		
29	Advisory Guidelines for Management Corporations		
30	Advisory Guidelines for the Education Sector		
31	Advisory Guidelines for the Social Service Sector		
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector		
34	Advisory Guidelines for the Healthcare Sector		
35	Advisory Guidelines for the		

	Telecommunication Sector		
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		

#	Regulation		
		opt-out	others
1	Personal Data Protection Act 2012		
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		

12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment		
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal		

	Data Protection Act		
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions		
26	Advisory Guidelines on Application of PDPA to Election Activities		
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		
29	Advisory Guidelines for Management Corporations		
30	Advisory Guidelines for the Education Sector		
31	Advisory Guidelines for the Social Service Sector		
32	Advisory Guidelines on In-vehicle		

	Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector		
34	Advisory Guidelines for the Healthcare Sector		
35	Advisory Guidelines for the Telecommunication Sector		
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		

Rights of the data subject

#	Regulation	Right to be informed	Right of access
1	Personal Data Protection Act 2012		Access to personal data 21.—(1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation must, as soon as reasonably possible, provide the individual with — (a) personal data about the individual that is in the possession or under the control of the organisation; and (b) information about the ways in which the personal data mentioned in paragraph (a) has been or may have been used or disclosed by the organisation within a year before the date of the request. (2) An organisation is not required to provide an individual with the individual's personal

			data or other information under subsection (1) in respect of the matters specified in the Fifth Schedule. (3) Subject to subsection (3A), an organisation must not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information (as the case may be) could reasonably be expected to — (a) threaten the safety or physical or mental health of an individual other than the individual who made the request; (b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request; (c) reveal personal data about another individual; (d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his or her identity; or (e) be contrary to the national interest. [40/2020] (3A) Subsection (3)(c) and (d) does not apply to any user activity data about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual. [40/2020] (4) An organisation must not inform any individual under subsection (1)(b) that the organisation has disclosed personal data about the individual to a prescribed law enforcement agency if the disclosure was made under this Act or any other written law without the individual's consent.

			[40/2020] (5) If an organisation is able to provide the individual with the individual's personal data and other information requested under subsection (1) without the personal data or other information excluded under subsections (2), (3) and (4), the organisation must provide the individual with access to the personal data and other information without the personal data or other information excluded under subsections (2), (3) and (4). (6) Where — (a) an individual makes a request under subsection (1) to an organisation on or after 1 February 2021; and (b) the organisation, by reason of subsection (2) or (3), does not provide an individual with the individual's personal data or other information requested under subsection (1), the organisation must, within the prescribed time and in accordance with the prescribed requirements, notify the individual of the rejection. [40/2020] (7) Where — (a) an individual makes a request under subsection (1) to an organisation on or after 1 February 2021; and (b) the organisation provides the individual, in accordance with subsection (5), with the individual's personal data or other information requested under subsection (1), the organisation must notify the individual of the exclusion, under subsection (2) or (3), of any of the personal data or other information so requested. [40/2020]

2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		How to make request 3.—(1) A request to an organisation must be made in writing and must include sufficient detail to enable the organisation, with a reasonable effort, to identify — (a) the applicant making the request; (b) in relation to a request under section 21(1) of the Act, the personal data and use and disclosure information requested by the applicant; and (c) in relation to a request under section 22(1) of the Act, the correction requested by the applicant. (2) A request must be sent to the organisation — (a) in accordance with section 48A of the Interpretation Act (Cap. 1); (b) by sending the request to the organisation's data protection officer in accordance with the business contact information provided under section 11(5) of the Act; or (c) in any other manner that is acceptable to the organisation. Duty to respond to request under section 21(1) of Act 4.—(1) Subject to section 21(2), (3), (3A) and (4) of the Act and regulations 6 and 7(3), an

			organisation must respond to each request made to it under section 21(1) of the Act on or after 1 February 2021 as accurately and completely as necessary and reasonably possible. (2) The organisation must provide an applicant access to the applicant's personal data requested under section 21(1) of the Act on or after 1 February 2021 — (a) by providing the applicant with a copy of the personal data and use and disclosure information in documentary form; (b) if sub-paragraph (a) is impracticable in any particular case, by allowing the applicant a reasonable opportunity to examine the personal data and use and disclosure information; or (c) in any other form requested by the applicant as is acceptable to the organisation. Notification of timeframe for response 5. Subject to the requirement to comply with section 21(1) of the Act as soon as reasonably possible or section 22(2) of the Act as soon as practicable (as the case may be), if the organisation is unable to comply with that requirement within 30 days after receiving a request made in accordance with regulation 3, the organisation must within that time inform the applicant in writing of the time by which it will respond to the request. Refusal to confirm or deny existence, use or disclosure of personal data 6. Subject to section 21(4) of the Act, an organisation, in a response to a request made to it under section 21(1) of the Act,

			may refuse to confirm or may deny any of the following: (a) the existence of personal data mentioned in paragraph 1(h) of the Fifth Schedule to the Act as in force before, on or after 1 February 2021; (b) the use or disclosure of personal data without consent under the following provisions for any investigation or proceedings, if the investigation or proceedings and related appeals have not been completed: (i) paragraph 3 of Part 3 of the First Schedule to the Act as in force on or after 1 February 2021; (ii) paragraph 1(e) of the Third Schedule to the Act or paragraph 1(f) of the Fourth Schedule to the Act (as the case may be) as in force before 1 February 2021. Fees 7.—(1) Subject to section 28 of the Act as in force immediately before 1 February 2021 or section 48H of the Act (as the case may be), an organisation may charge an applicant who makes a request to it under section 21(1) of the Act a reasonable fee for services provided to the applicant to enable the organisation to respond to the applicant's request. (2) An organisation must not charge a fee to respond to the applicant's request under section 21(1) of the Act unless the organisation has — (a) provided the applicant with a written estimate of the fee; and (b) if the organisation wishes to charge a fee that is higher than the written estimate provided under sub-paragraph (a), notified the applicant in writing of the higher fee. (3) An organisation does not

			have to respond to an applicant's request under section 21(1) of the Act unless the applicant agrees to pay the following fee: (a) where the organisation has notified the applicant of a higher fee under paragraph (2)(b) — (i) if the Commission — (A) has reviewed the higher fee under section 28(1) of the Act as in force immediately before 1 February 2021, the fee allowed by the Commission under section 28(2) of the Act as in force immediately before that date; or (B) has reviewed the higher fee under section 48H(1) of the Act, the fee allowed by the Commission under section 48H(2) of the Act; or (ii) if sub-paragraph (i) does not apply, the higher fee notified under paragraph (2)(b); (b) where sub-paragraph (a) does not apply and the organisation has provided the applicant with an estimated fee under paragraph (2)(a) — (i) if the Commission — (A) has reviewed the estimated fee under section 28(1) of the Act as in force immediately before 1 February 2021, the fee allowed by the Commission under section 28(2) of the Act as in force immediately before that date; or (B) has reviewed the estimated fee under section 48H(1) of the Act, the fee allowed by the Commission under section 48H(2) of the Act; or (ii) if sub-paragraph (i) does not apply, the estimated fee provided under paragraph (2)(a). (4) To avoid doubt, an organisation must not charge the applicant any fee to comply with its obligations under section 22(2) of the Act. Preservation of copies of personal data 8.—(1) For the purposes of

			section 22A(1) of the Act, the prescribed period for the preservation of a copy of the personal data that an organisation has refused to provide is the period beginning immediately after the date of the organisation's refusal and ending immediately after the relevant date. (2) In this regulation — "date of refusal", in relation to an organisation's refusal, means the date on which the organisation notifies an individual of the organisation's refusal; "date of withdrawal" — (a) in relation to an application made by a complainant under section 48H(1) of the Act in relation to an organisation's refusal, means the date on which the complainant withdraws the application or the Commission dismisses the application under the Personal Data Protection (Enforcement) Regulations 2021 (G.N. No. S 62/2021); (b) in relation to an application or appeal made by a complainant in relation to a decision or direction made by the Commission, means the date on which the complainant withdraws the application or appeal; or (c) in relation to an application or appeal made by an organisation in relation to a decision or direction made by the Commission, means the date of compliance by the organisation with the decision or direction; "organisation's refusal" means an organisation's refusal to provide, pursuant to an individual's request under section 21(1)(a) of the Act, the individual's personal data in the possession or under the control of the organisation; "relevant date", in relation to an

			organisation's refusal, means — (a) the 30th day after the date of refusal; or (b) where, on or before the day mentioned in paragraph (a) or while the personal data concerned in relation to the organisation's refusal is in the possession or under the control of the organisation on or after that date, the organisation has notice of any of the following applications or appeals — the latest of the following dates applicable to those applications or appeals: (i) an application to the Commission under section 48H(1)(a) of the Act to review the organisation's refusal — the date of withdrawal of the application or the 28th day after the Commission issues its decision or direction made under section 48H(2) of the Act in relation to the application; (ii) an application for reconsideration made to the Commission under section 48N(1) of the Act in relation to the organisation's refusal — the date of withdrawal of the application or the 28th day after the date of issue of the Commission's decision made under section 48N(6)(b) of the Act in relation to the application; (iii) an application under section 48N(5) of the Act to extend the prescribed period for an application for reconsideration in relation to the organisation's refusal — the date of withdrawal or refusal of the application or the date of expiry of the extended period allowed for the application, if any; (iv) an appeal under section 48Q(1) of the Act against the Commission's decision or direction made under section 48H(2) of the Act or decision

			made under section 48N(6)(b) of the Act (as the case may be) in relation to the organisation's refusal — the date of withdrawal of the appeal or the 28th day after the Appeal Committee hearing the appeal issues its direction or decision; (v) an appeal against, or with respect to, a direction or decision of the Appeal Committee mentioned in sub-paragraph (iv) under section 48R of the Act — the date of withdrawal of the appeal or the date the General Division of the High Court or Court of Appeal (as the case may be) determines the appeal. Exercise of rights under Act in respect of deceased individual 16.—(1) The persons specified in paragraph (2) may exercise all or any of the following rights in relation to section 24 of the Act or any provision of the Act relating to the disclosure of personal data, in respect of a deceased individual who has been dead for 10 years or fewer: (a) the right to give or withdraw any consent for the purposes of the Act; (b) the right to bring an action — (i) under section 32 of the Act as in force immediately before 1 February 2021 in respect of a contravention, before 1 February 2021, by an organisation of section 24 of the Act or other provision of the Act relating to the disclosure of personal data (as the case may be) as in force before that date; or (ii) under section 480 of the Act in respect of a contravention, on or after 1 February 2021, by an organisation or a person of section 24 of the Act or other provision of the Act relating to the disclosure of personal data (as the case may be) as in force

			on or after that date; (c) the right to bring a complaint under the Act. (2) The following persons are specified for the purposes of paragraph (1): (a) a person appointed under the deceased individual's will to exercise the right mentioned in paragraph (1) which is to be exercised or a personal representative of the deceased individual, unless the person or personal representative (as the case may be) has renounced the grant of such right; (b) if no person or personal representative mentioned in sub-paragraph (a) is able to exercise such right or power, the deceased individual's nearest relative determined in accordance with the First Schedule. (3) Subject to Part II of the Probate and Administration Act (Cap. 251) (if applicable), the renunciation of the grant of any right under paragraph (1) must be made expressly in writing. (4) Any notice or other communication to be given under the Act concerning any consent, action or complaint mentioned in paragraph (1) may be given to the person who may exercise the right related to that consent, action or complaint under that paragraph. (5) This regulation does not — (a) enable any person to exercise any right under paragraph (1) if that person is legally incapable of exercising such a right on that person's own behalf; or (b) affect the authority of any person under any other law to exercise any right mentioned in paragraph (1). (6) A person does not cease to be a personal representative for the purposes of this regulation

			merely because that person has completed the administration of the deceased individual's estate.
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's		

	Personal Data in the Digital Environment		
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act		The Access and Correction Obligations 15.1 Sections 21, 22 and 22A of the PDPA set out the rights of individuals to request for access to their personal data and for correction of their personal data that is in the possession or under the control of an organisation, and the corresponding obligations of the organisation to provide access to, and correction of, the individual's personal data. These obligations are collectively referred to in these Guidelines as the Access and Correction Obligations as they operate together to provide individuals with the ability to verify their personal data held by an organisation. 15.2 The Access and Correction Obligations relate to personal data in an organisation's possession as well as personal data that is under its control (which may not be in its possession). For example, if an organisation has transferred personal data to a data intermediary that is processing the personal data under the control of the organisation, the organisation's response to an access or correction request must take into account the personal data which is in the possession of the data intermediary. The PDPA does not directly impose the Access and

			Correction Obligations on a data intermediary in relation to personal data that it is processing only on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing28. A data intermediary may (but is not obligated under the PDPA to) forward the individual's access or correction request to the organisation that controls the personal data. The Commission understands that, in some cases, an organisation may wish to enter into a contract with its data intermediary for the data intermediary to assist with responding to access or correction requests on its behalf. In this connection, the Commission would remind organisations that engage the data intermediary, that they remain responsible for ensuring compliance with the Access and Correction Obligations under the PDPA. Please refer to the sections on data intermediaries and their obligations for more information. Obligation to provide access to personal data 15.3 Section 21(1) of the PDPA provides that, upon request by an individual, an organisation must provide the individual with the following as soon as reasonably possible: a) personal data about the individual that is in the possession or under the control of the organisation; and b) information about the ways in which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request. 15.4 Section 21(1) allows an individual to submit a request to

			an organisation for access to personal data about him that is in the possession or under the control of the organisation (an "access request"). Such a request may be for: a) some or all of the individual's personal data; and b) information about the ways the personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request. 15.5 An organisation's obligation in responding to an access request is to provide the individual access to the personal data requested by the individual which is in the organisation's possession or under its control, unless any relevant exception in section 21 or the Fifth Schedule to the PDPA applies. 15.6 To be clear, an organisation is not required to provide access to the documents (or systems) which do not comprise or contain the personal data in question, so long as the organisation provides the individual with the personal data that the individual requested and is entitled to have access to under section 21 of the PDPA. In the case of a document containing the personal data in question, the organisation should, where feasible, provide only the personal data (or relevantsections of the document containing the personal data) without providing access to the entire document in its original form. 15.7 An organisation does not need to provide access to information which is no longer within its possession or under its control when the access request is received. The organisation should generally inform the

			requesting individual that it no longer possesses the personal data and is thus unable to meet the individual's access request. Organisations are also not required to provide information on the source of the personal data. 15.8 In certain circumstances, the individual making the access request may ask for a copy of his personal data in documentary form. Organisations should provide the copy and have the option of charging the individual a reasonable fee for producing the copy (please see the section on "fees chargeable for access to personal data" for more details). If the requested personal data resides in a form that cannot practicably be provided to the individual in documentary form, whether as physical or electronic copies (for example, the data cannot be extracted from a special machine owned by the organisation), then the organisation may provide the individual a reasonable opportunity to examine the requested data in person. 15.9 Organisations should note that the obligation to provide access applies equally to personal data captured in unstructured forms, such as personal data embedded in emails. Organisations are generally required to implement processes to keep track of the collection, use, and disclosure of all personal data under their control, including unstructured data. Organisations should note that they are not required to provide access if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interest or if the request is otherwise

			frivolous or vexatious. Please see the sections on exceptions to the obligation to provide access to personal data for more details (including situations where an organisation must not provide access). 15.10 If the personal data requested by the individual can be retrieved by the individual himself (e.g. resides in online portals in which access has been granted by the organisation), the organisation may inform the individual how he may retrieve the data requested. Example: Organisation ABC receives a request from John seeking to know what personal data relating to him was disclosed in Organisation ABC's correspondence with Organisation DEF in a specified month within the last one year. Assuming that the request does not fall under any relevant exception (for example, it is not opinion data kept solely for an evaluative purpose), ABC is required to provide John with his personal data even if its correspondence with DEF had not been archived in a formalised system such as a database. To be clear, ABC's obligation is limited to providing John with the full set of his personal data that he requested which is in its possession or control, and it is not necessarily required to provide John with copies of the actual correspondence with DEF. 15.11 The PDPA does not expressly state that an access request be accompanied by a reason for making the request. However, an organisation should ask the applicant to be more specific as to what type of personal data he requires, the

			time and date the personal data was collected, to facilitate processing of the access request, or to determine whether the request falls within one of the prohibitions under section 21(3) of the PDPA or any exception in the Fifth Schedule29. When assessing an access request, the organisation should consider the purpose of the applicant's access request, so as to determine the appropriate manner and form in which access to the personal data should be provided. For instance, the organisation may determine that it will provide the individual a snapshot from a video recording, instead of a masked video clip, as the most cost effective and efficient way to allow an individual to show that he was present at a particular location at a specific date and time. If the individual is unable or unwilling to provide more details, the organisation should make an attempt to respond to the access request as accurately and completely as reasonably possible. 15.12 Before responding to an access request, organisations should exercise due diligence and adopt appropriate measures to verify an individual's identity. While the Commission does not prescribe the manner in which organisations are to obtain verification from the individual making an access request, organisations are encouraged to have documentary evidence to demonstrate that they are in compliance with the PDPA, and minimise any potential disputes. Organisations may implement policies setting out the standard operating procedures on conducting verification when processing access requests (e.g.

			this may include the questions that an employee handling the access request may ask the applicant in order to verify his identity)30. 15.13 In a situation where a third party is making an access request on behalf of an individual, organisations receiving the access request should ensure that the third party has the legal authority to validly act on behalf of the individual. 15.14 In some cases, there may be two or more individuals (e.g. husband and wife) making an access request at the same time for their respective personal data captured in the same set of records. The organisation may obtain consent31 from the respective individuals to disclose their personal data to each other, so that it may provide the individuals access to a common data set containing their personal data, without having to exclude the personal data of the other individuals32. If such consent cannot be obtained, an organisation receiving such requests may provide access to the personal data to the individuals separately, for example, by masking the personal data of the other individuals before providing the individual access to his own personal data (i.e. the individual will be provided access to only his own personal data). Information relating to ways which personal data has been used or disclosed 15.15 As stated in section 21(1) of the PDPA, if an individual requests for information relating to the use or disclosure of his personal data by the organisation, the organisation is required to provide information

			relating to how the personal data has been or may have been used or disclosed within the past year. In this regard, an organisation may develop a standard list of all possible third parties to whom personal data may have been disclosed by the organisation. In many cases, an organisation may provide this standard list as an alternative to providing the specific set of third parties to whom the personal data has been disclosed, as part of its response to access requests that ask for information relating to how the personal data has been or may have been disclosed within the past year. The organisation should also update the standard list regularly and ensure that the information is accurate before providing the list to the individual. Generally, in responding to a request for information on third parties to which personal data has been disclosed, the organisation should individually identify each possible third party (e.g. 'pharmaceutical company ABC'), instead of simply providing general categories of organisations (e.g. 'pharmaceutical companies') to which personal data has been disclosed. This would allow individuals to directly approach the third party organisation to which their personal data has been disclosed. 15.16 In specifying how the personal data has been or may have been used or disclosed within the past year, organisations may provide information on the purposes rather than the specific activities for which the personal data had been or may have been used or disclosed. For example, an organisation may have disclosed

			personal data to external auditors on multiple occasions in the year before the access request. In responding to an access request, the organisation may state that the personal data was disclosed for audit purposes rather than describing all the instances when the personal data was disclosed. 15.17 Generally, the organisation's actual response would depend on the specific request, and organisations are reminded that in meeting their responsibilities under the PDPA, they are to consider what a reasonable person would consider appropriate in the circumstances. Example: Sarah makes an access request to her spa, requesting for information relating to how her personal data has been used or disclosed. The request was made on 5 December 2015. The spa is only required to provide information on how her personal data has been used or disclosed within the past year – that is, the period from 6 December 2014 to the date of the request, 5 December 2015. Response time frame for an access request 15.18 Subject to the PDPA and the Personal Data Protection Regulations 202133, an organisation is required to comply with section 21(1) of the PDPA and must respond to an access request as soon as reasonably possible from the time the access request is received. If an organisation is unable to respond to an access request within 30days34 after receiving the request, the organisation shall inform the individual in writing within 30 days of the time by which it will

			be able to respond to the request. When not to accede to an access request 15.19 An organisation must respond to an access request by providing access to the personal data requested, or by informing the individual of a rejection of the access request where it has valid grounds not to provide access. 15.20 Organisations are not required to accede to a request if an exception35 from the access requirement applies. 15.21 Additionally, an organisation shall not inform any individual or organisation that it has disclosed personal data to a prescribed law enforcement agency if the disclosure is necessary for any investigation or proceedings and the personal data is disclosed to an authorised36 officer of the agency. In this regard, an organisation may refuse to confirm or deny the existence of personal data, or the use of personal data without consent for any investigation or proceedings, if the investigation or proceedings and related appeals have not been completed. It also does not have to respond to a request unless the applicant agrees to pay the fee for services provided to the applicant to enable the organisation to respond to the applicant's request. This is provided the organisation has provided the applicant a written estimate of the fee. Where applicable, the Commission may review the fee by confirming, reducing or disallowing the fee, or directing the organisation to make a refund to the applicant. 15.23 An organisation shall not

			accede to an access request if any of the grounds in section 21(3) are applicable, for instance, where the provision of the personal data or other information could reasonably be expected to threaten the safety or physical or mental health of an individual other than the requesting individual, or to cause immediate or grave harm to the safety or physical or mental health of the requesting individual. 15.24 If the organisation searches for the requested personal data but is unable to respond to the access request within the 30-day timeframe (e.g. technical processing of personal data residing in a specific format requires more time), the organisation must inform the applicant within the 30-day timeframe of the date when it will be able to respond to the request, and must still respond to the request as soon as reasonably possible. Fees chargeable to comply with the access obligation 15.25 An organisation may charge an individual a reasonable fee to process an access request by the individual37. The purpose of the fee is to allow organisations to recover the incremental costs of responding to the access request. This may include the time and costs incurred to search for the personal data requested. An example of such incremental costs is the cost of producing a physical copy of the personal data for the individual requesting it. As organisations are required to make the necessary arrangements to provide for standard types of access requests, costs incurred in capital purchases (e.g.

			purchasing new equipment in order to provide access to the requested personal data) should not be transferred to individuals. 15.26 The Commission is of the view that it would be difficult to prescribe a standard fee or range of fees at the outset to apply across all industries or all types of access requests. Organisations should exercise proper judgement in deriving the reasonable fee they charge based on their incremental costs of providing access. The Commission may, upon the application of an individual, review a fee charged by an organisation under section 48H of the PDPA (among other matters). In reviewing a fee, the Commission may consider the relevant circumstances, including the absolute amount of the fee, the incremental cost of providing access which may include the time and costs incurred to search for the personal data requested, and similar fees charged in the industry. 15.27 If an organisation wishes to charge an individual a fee to process an access request, the organisation must give the individual a written estimate of the fee38. If the organisation wishes to charge a fee higher than the original written estimate, it must inform the individual in writing of the increased fee. The organisation may refuse to process or provide access to the individual's personal data until the individual agrees to pay the relevant fee. Example: Company ZYX receives an access request from a customer to view his personal data stored in a format that is readable only by a special machine. The company

			owns two such machines but both are faulty. In order to respond to the customer's request in a timely manner, ZYX purchases another machine and transfers its cost to the customer as part of the access fee. Because of this, the access fee amounts to $50,000. This would not be considered a reasonable fee as ZYX is expected to have the general means to comply with its customers' access requests. Example: An individual requests from Company TUV a paper copy of his personal data. Company TUV charges a fee of $50 for the information printed out on 50 pages of paper, based on the incremental cost of producing the copy. The fee is reasonable as it reflects the incremental cost of providing the personal data. Exceptions to the obligation to provide access to personal data 15.28 The obligation in section 21(1) is subject to a number of exceptions in sections 21(2) to 21(4) including some mandatory exceptions relating to situations where an organisation must not provide access. These exceptions are listed below. 15.29 Section 21(2) of the PDPA provides that an organisation is not required to provide individuals with the personal data or other information specified in section 21(1) in respect of the matters specified in the Fifth Schedule to the PDPA. An organisation is not prohibited from providing information in respect of the matters specified in the Fifth Schedule and may do so if it decides to. 15.30 The exceptions specified in the Fifth Schedule include the

			following matters: a) opinion data kept solely for an evaluative purpose39; b) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results; c) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust; d) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; e) a document related to a prosecution if all proceedings related to the prosecution have not yet been completed; f) personal data which is subject to legal privilege; g) personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation; h) personal data collected, used or disclosed without consent for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed40; i) personal data collected by an arbitrator or mediator in the conduct or an arbitration or mediation for which he or she was appointed to act – i. under a collective agreement under the Industrial Relations Act 1960; ii. by agreement between the parties to the arbitration or mediation; iii. under any written law; or

			iv. by a court, arbitral institution or mediation centre; or j) any request — i. that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests (i.e. considering the number and frequency of requests received); ii. if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests; iii. for information that does not exist or cannot be found; iv. for information that is trivial; or v. that is otherwise frivolous or vexatious. Example: A shopping centre receives a request from an individual to view all CCTV footage of him recorded at the shopping centre over the past year. In this scenario, reviewing all CCTV footage from the past year to find records of the individual making the request would require considerable time and effort. To the extent that the burden of providing access would be unreasonable to the shopping centre and disproportionate to the individual's interests as the individual is making a general request for all CCTV footage, the shopping centre is unlikely to have to provide the requested personal data under the Access Obligation. Example: A shop in the shopping centre receives a request from an individual to view a photograph of him taken by the official photographer at a private event held recently by the shop that

			the individual was invited to. The individual provides the shop with sufficient information to determine when the event was held. The provision of access in this case would be reasonable and the shop should provide the photograph which the individual requested. Example: An individual sends an email providing feedback to Organisation XYZ. The form contains his personal data including his full name and contact number. A day later, he requests access to the personal data in the form while having full knowledge of the information he is requesting. Such a request is likely to be considered frivolous or vexatious, unless it can be shown otherwise. Example: An individual submits an access request every fortnight for the same set of personal data in Organisation ABC's possession. Such requests are likely to be considered to unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests. 15.31 In addition to the matters specified in the Fifth Schedule to the PDPA, section 21(3) specifies a number of situations in which an organisation must not provide the personal data or other information specified in section 21(1). 15.32 The situations specified in section 21(3) are where the provision of personal data or other information under section 21(1) could reasonably be expected to: a) threaten the safety or physical or mental health of an individual

			other than the individual who made the request; b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request; c) reveal personal data about another individual41; d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his or her identity; or e) be contrary to the national interest42. Providing personal data of an individual without the personal data of other individuals 15.33 Section 21(5) of the PDPA provides that if an organisation is able to provide the individual with his personal data and other information requested under section 21(1) without the personal data of other information excluded under sections 21(2), 21(3) and 21(4), the organisation must provide the individual access to the requested personal data and other information without the personal data or other information excluded. Organisations may request information about the purpose of the access request so that it can consider if it is able to provide the requested personal data without the personal data of the other individuals, such as by masking out the personal data of other individual(s) before providing the personal data requested by the individual. Example: Mary requested Travel Agency ABC to furnish formal documentation confirming the cancellation of her transit flight to process her insurance claims.

			As the letter from the airline also contains the personal data of 36 other passengers who signed up for the same tour package, e.g. name, nationality, date of birth and passport number, ABC assesses that it is possible to provide Mary access to her personal data without revealing the other individuals' personal data by redacting the personal data of the other passengers from the letter. Access that may reveal personal data about another individual 15.34 One of the prohibitions, section 21(3)(c), requires that an organisation must not provide access to the personal data or other information under section 21(1) where the provision of personal data or other information could reasonably be expected to reveal personal data about another individual. The prohibition does not apply to any user activity data43 about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual. Although organisations do not need to mask or remove personal data of these other individuals in user-activity or provided data, organisations should still consider if the other harmful situations in 21(3) may arise. In addition, the Commission is of the view that this prohibition does not apply in circumstances where: a) any of the exceptions relating to disclosure of personal data without consent listed under the First and Second Schedules to the PDPA apply to the extent that the organisation may disclose the personal data of the other individual without consent (e.g. if the personal data of the

			individual is publicly available or if the organisation can rely on the legitimate interests exception); b) as permitted or required by any other law and regulation (e.g. exercise of police investigatory powers, compliance with discovery directions in civil proceedings or regulations governing building maintenance and strata management); or c) the other individual has given consent to the disclosure of his personal data. Example: Betty applies to Shopping Centre ABC for access to CCTV footage of herself walking through the aisles of the shopping centre on a specific day and time. The CCTV footage contains images of other individuals. Since the images of the other shoppers are recorded in a public area, the data is considered publicly available. Shopping Centre ABC does not need to obtain consent of the other shoppers in the CCTV footage or mask their images before providing access to Betty. Example: John applies to Organisation DEF for records of his transactions and purchases made on DEF's platform. Some of the transactions and purchases made by John on DEF's platform contain personal data of a third-party (e.g. name of third-party whom John had sent an item to after purchasing that item on the platform). As the personal data of the third-party forms part of John's user activity data in this instance, Organisation DEF may provide John with access to the data without redacting the personal data of the third-party. Example:

			Jane applies to Condominium ABC for access to CCTV footage of herself at the Condominium's taxi drop off point where she had an altercation with a thirdparty. As the taxi drop off point is open to the public, ABC can rely on the publicly available data exception and need not mask the image of the thirdparty within the footage in providing Jane access to the requested footage. Example: Jack is a subsidiary proprietor/owner of a unit in Condominium XYZ. Jack applies to Condominium XYZ's management for access to CCTV footage of himself at the condominium's lift lobby as he believes he dropped his personal belongings there. There were other people with Jack at the lift lobby at that time and Jack wishes to approach them for assistance in recovering his personal belongings. Under Section 47 of the Building Maintenance and Strata Management Act (BMSMA), a subsidiary proprietor/owner of a condominium unit may make an access request for the CCTV footage without the need to redact/mask the footage. 44 As PDPA is considered a baseline law, other sectoral regulations,such as BMSMA, which permit the access to unredacted footage, will take precedence in this instance. Example: There is a children's party being held at the function room of Condo KLM where a CCTV is installed. Jessie and her daughter, who do not stay or own a unit in Condo KLM, are guests of the host of the party. Jessie loses her personal belongings at the party. She decides to go directly to Condo

			KLM's management to request for a copy of the CCTV footage to assist her in locating the belongings. KLM assesses that there is legitimate interest in providing Jessie with access to the footage, without masking the images of other individuals, to assist her in recovering her personal belongings. KLM also assesses that in doing so, there is no adverse effects to individuals present at the party. As such, KLM allows Jessie access to the requested footage. KLM designs an approval process for such requests and addresses risks of abuse by limiting Jessie's access to viewing of the relevant CCTV footage under supervision. Access request relating to disclosure to prescribed law enforcement agency 15.35 Section 21(4) of the PDPA contains an additional obligation of organisations in relation to the Access Obligation. That subsection provides that where an organisation has disclosed personal data to a prescribed law enforcement agency without the consent of the individual under the PDPA or any other written law, the organisation must not inform the individual that personal data has been disclosed. Access request relating to legal proceedings 15.36 Where personal data has been collected for the purpose of prosecution, investigation, civil proceedings and associated proceedings and appeals, paragraph 1(h) of the Fifth Schedule may apply to exempt such personal data from the access request. Organisations are thus not required to provide the

			requested information. Further, under paragraph 1(e) of the Fifth Schedule, access need not be provided in respect of a document related to a prosecution if all proceedings related to the prosecution have not been completed. 15.37 Where personal data has been collected prior to the commencement of prosecution and investigations but is nonetheless relevant to the proceedings, an individual should obtain access through criminal and civil discovery avenues rather than through the Access Obligation under the PDPA. The intent of the Access Obligation is to ensure that organisations remain accountable for the personal data of individualsin their possession or under their control, including ensuring the accuracy and proper use of the personal data. The Data Protection Provisions of the PDPA do not affect discovery obligations under law that parties to a legal dispute may have(e.g. pursuant to any order of court). For instance, if criminal disclosure of civil discovery regimes are applicable, section 4(6) of the PDPA applies, and any request for access to the personal data should be made pursuant to any other written laws providing for such disclosure or discovery applications. A possible advantage of obtaining access to personal data through the discovery process is that it allows the requestor to obtain un-redacted and complete documents, while and access request would grant the requestor only his personal data, with other content redacted.

			Rejecting an access request 15.38 Subj
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions		
26	Advisory Guidelines on Application of PDPA to Election Activities		Access and Correction Obligations 4.16 A political party or election candidate must, upon request, (a) provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year16; or (b) correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation.
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		
29	Advisory Guidelines for Management Corporations		Handling access and correction requests 3.7 Under the PDPA, MCSTs are required to provide access to or

			make a correction to the individual's personal data in the MCSTs' possession or under their control upon the individual's request, unless a relevant exception under sections 21 or 22 of the PDPA applies27. For example, MCSTs must provide access to an individual's personal data captured in close-circuit television camera ("CCTV") footage requested by the individual, unless an exception applies. To be clear, MCSTs may not limit the provision of access to personal data only to law enforcement or other relevant authorities, or for the purposes of investigations by such authorities. To this end, MCSTs must develop and implement policies and processes for handling access and correction requests to ensure compliance with the PDPA. 3.8 MCSTs must also respond to an access request (i.e. provide access to the personal data) as soon as reasonably possible from the time the access request is received. If a MCST is unable to respond to an access request within 30 days after receiving the request, the MCST must inform the individual in writing within 30 days of the time by which it will be able to respond to the request. MCSTs may charge a reasonable fee for providing the requested access that reflects the time and effort required to respond to the access request. 3.9 While the PDPA does not require that an access request be accompanied by a reason for making the request, as good practice, MCSTs could ask the applicant to be more specific as to what type of personal data is required, as well as the time and date the personal data was

			collected, to facilitate processing of the access request, or to determine whether the request falls within one of the prohibitions under section 21(3) of the PDPA or any exception in the Fifth or Sixth Schedule. MCSTs could also ask the applicant as to what form a CCTV footage extract could be provided in (e.g. screenshot or video footage), in order to fulfil the access request in the most cost efficient manner. 3.10 In situations where access and correction requests are handled by managing agents, MCSTs should establish clear policies and processes for the handling of access and correction requests by these managing agents to ensure compliance with the PDPA. 3.11 Please refer to Chapter 15 of the Advisory Guidelines on Key Concepts in the PDPA for further information relating to the Access and Correction Obligations, as well as the Guide on Responsible Use of Biometric Data in Security Applications for more information on best practices for the collection, use, and disclosure of biometric data responsibly. The section on CCTVs in the Selected Topics Advisory Guidelines also provides examples relating to access requests.
30	Advisory Guidelines for the Education Sector		3 The Access and Correction Obligation 3.1 Section 21(1) of the PDPA provides that, upon request by an individual, an organisation shall provide the individual with the following as soon as reasonably possible: a) personal data about the individual that is in their possession or under the control of the organisation; and b) information about the ways in

			which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request. 3.2 The Fifth Schedule to the PDPA contains exceptions to this obligation such as where the data is opinion data kept solely for an evaluative purpose; or the information is in respect of any examination conducted by an education institution, examination scripts and prior to the release of examination results, examination results. 3.3 Section 22(1) of the PDPA provides that an individual may submit a request for an organisation to correct an error or omission in the individual's personal data that is in the possession or under the control of the organisation ("a correction request"). Upon receipt of a correction request, the organisation is generally required to make the correction, subject to applicable exceptions10. 3.4 In particular, section 22(2) goes on to provide that unless the organisation is satisfied on reasonable grounds that the correction should not be made, it should: a) correct the personal data as soon as practicable; and b) send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within the year before the date the correction request was made, unless that other organisation does not need the corrected personal data for any legal or business purpose. 3.5 If an organisation is satisfied upon reasonable grounds that a correction should not be made (whether the organisation is

			responding to a correction request made directly by the individual or has been notified of a correction made by such an organisation), section 22(5) requires the organisation to annotate (that is, make a note to) the personal data in its possession or under its control indicating the correction that was requested but not made. As a good practice, the organisation may also wish to annotate the reasons why it has decided that the correction should not be made. 3.6 The obligation to correct personal data is subject to a number of exceptionsin Section 22 and the Sixth Schedule of the PDPA. One such exception relates to personal data which is opinion data kept solely for an evaluative purpose11. 3.7 The following examples illustrate the application of the Access and Correction Obligation. 3.8 Example: Access to student's records Jack intends to apply for a job with Company ABC after graduating from School DEF. To provide information to support his application, Jack makes an access request to School DEF for records of his co-curricular activities and a transcript of his examination results. School DEF is required to provide access to the information in accordance with section 21(1) of the PDPA, unless there is an applicable exception. 3.9 Example: Accessing results of language competency test Prior to enrolment into School ABC, all students are required to undergo a language competency test. Grace makes an access request after taking the test (but before the release of results) to School ABC to find out her test

			grade. In this case, School ABC is not required to accede to Grace's access request as there is an exception under the Fifth Schedule to the PDPA in relation to information that is in respect of any examination conducted by an education institution, examination scripts and prior to the release of examination results, examination results. 3.10 Example: Correction of residential address Peter finds out that a cheque refund mailed out by School ABC to him was mistakenly sent to his neighbour residing two storeys above him. Peter makes a correction request for School ABC to amend the residential address recorded in School ABC's system from 123, DEF Road, #04-02 to 123, DEF Road, #02-04. As there are no reasonable grounds for the correction not to be made, School ABC corrects the listing of Peter's residential address so as to be able to communicate with him by mail. 3.11 Example: Correction of a teacher's opinion Karen's mother, Mary, notices a teacher's remarks in Karen's annual assessment report that Karen tends to lose attention during certain classes, and that Karen needs to improve her handwriting. Mary makes a correction request to the school to omit these remarks from Karen's report. In this case, the school is not required to make corrections to the teacher's remarks to the extent that the remarks are regarded as an opinion.
31	Advisory Guidelines for the Social Service Sector		4 The Access and Correction Obligation 4.1 The Access and Correction Obligations (PDPA sections 21, 22 and 22A) state that an

			organisation must, upon request, (i) provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year; and (ii) correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation. For more information on the Access and Correction Obligations, do refer to Chapter 15 of the Advisory Guidelines on Key Concepts in the PDPA. 4.2 The following examples illustrate the application of the Access and Correction Obligations. 4.3 Example: Accessing personal data of one individual which was provided by another individual SSA ABC is launching a new social service scheme targeting the elderly. Madam Chua, a widow who lives in a one-room apartment, intends to apply for SSA ABC's new scheme. As part of the application process, Madam Chua is required to provide SSA ABC with the personal data of her family members or those in her support system in order for SSA ABC to assess her suitability. Madam Chua discloses the full names of her five children, and their marital status. In addition, Madam Chua discloses that one of her children, Alan is not her biological son and was adopted. She added that Alan was not aware that he was an adopted child. Alan learns about his mother's application for the social service scheme and makes an access request for the personal data

			SSA ABC has about him, and how it had been used by SSA ABC. Treatment Generally, SSA ABC should provide Alan access to his personal data which is in the possession or under the control of SSA ABC and information about the ways in which such personal data has been or may have been used or disclosed by SSA ABC over the past year. However, SSA ABC must consider if any prohibition under section 21 applies.16 For example, section 21(3) of the PDPA prohibits SSA ABC from providing Alan with his personal data or other information, as the case may be, if doing so could reasonably be expected to cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request. 17 In this regard, SSA ABC may reject Alan's access request as disclosure may cause harm to his mental health. SSA ABC may also wish to consider if any of the exceptions to the Access Obligation set out in the Fifth Schedule apply. SSA ABC should generally exercise due diligence and adopt appropriate measures to verify the identity of Alan before providing him with access to his personal data.
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		4 Complying with Access Obligation Are Leasing Companies, Hirers and Service Providers required to provide individuals access to their personal data captured in in-vehicle recordings? What if it contains personal data of other individuals? 4.1 Generally, Leasing Companies, Hirers and Service Providers who are subject to the Access Obligation are required to

			grant individuals access to the personal data in their possession or control and provide information about how such personal data has, or may have, been used or disclosed by the organisation in the past year15. However, such Leasing Companies, Hirers and Service Providers do not need to provide access to information which is no longer in their possession or control when the access request is received. Before responding to an access request, Leasing Companies, Hirers and Service Providers should exercise due diligence and adopt appropriate measures to verify the individual's identity. 4.2 In providing access, Leasing Companies, Hirers and Service Providers should ensure they do not reveal personal data about other individuals in the recording, for example by masking the other individuals' images and/or voices. However, if there is consent from the other individuals to disclose their personal data for the purpose of the access request16, the Leasing Company, Hirer and Service Provider need not mask their images and/or voices17 (unless other prohibitions apply). 4.3 Leasing Companies, Hirers and Service Providers may have scheduled periodic deletion of in-vehicle recordings (e.g. in-vehicle recordings are deleted every X days18). If so, as soon as reasonably possible after receiving an access request, Leasing Companies, Hirers and Service Providers are to identify the requested personal data and ensure that the personal data requested is preserved while the Leasing Companies, Hirers and Service Providers are processing the access request.

			However, Leasing Companies, Hirers and Service Providers should generally be mindful not to unnecessarily preserve personal data "just in case" to meet possible access requests, and should not retain personal data indefinitely when there is no business or legal purpose to do so. 4.4 If an individual requests for a copy of his/her personal data in the in-vehicle recording, the Leasing Company, Hirer and Service Provider should provide a copy, and may charge the individual a reasonable fee for producing the copy. If the invehicle recording resides in a form that cannot be provided to the individual, or if it is prohibitively costly to provide a copy of the recording, the Leasing Company, Hirer and Service Provider may provide the individual a reasonable opportunity to view the requested personal data in person, with appropriate masking of the images and/or voices of other individuals where necessary. 4.5 Leasing Companies, Hirers and Service Providers need not provide access to the individuals' personal data where an exception in the Fifth Schedule to the PDPA applies, for example, if the request is frivolous or vexatious, or if the burden or expense of providing access would be unreasonable to the Leasing Companies, Hirers and Service Providers or disproportionate to the individual's interest. When relying on any exception to not provide access, Leasing Companies, Hirers and Service Providers should be able to provide supporting evidence to justify their decision.

			4.6 If a Leasing Company, Hirer or Service Provider determines that it is appropriate under section 21 of the PDPA and Part II of the Personal Data Protection Regulations 2014 to not provide the requested personal data ("withheld personal data"), the Leasing Company, Hirer or Service Provider should keep the withheld personal data for a reasonable period – minimally 30 calendar days or longer after rejecting the access request – as the individual may seek a review of the Leasing Company's, Hirer's or Service Provider's decision. In the event the individual submits an application for review to the PDPC and the PDPC determines that it will take up the review application, as soon as the Leasing Company, Hirer or Service Provider receives a Notice of Review Application from the PDPC, the Leasing Company, Hirer or Service Provider should preserve the withheld personal data until the review by PDPC is concluded and any right of the individual to apply for reconsideration and appeal is exhausted. 4.7 Notwithstanding the foregoing, in the event it is determined by the PDPC or any appellate body that the Leasing Company, Hirer or Service Provider did not have appropriate grounds under the PDPA to refuse to provide access to the personal data in question and had therefore contravened the obligations under the PDPA, the Leasing Company, Hirer or Service Provider may face enforcement action under section 29 of the PDPA. 4.8 For more information relating to access requests, please refer to Chapter 15 of the Key Concepts Guidelines.

			4.9 Example: Request for all in-vehicle recordings of the individual A taxi operator VWX receives a request from an individual for all recordings of him captured by IVRDs in all VWX's taxis over the past year. The individual is unable to provide more specific information as to the taxis and the dates he had taken the taxis to help facilitate the processing of his access request. In this case, reviewing the in-vehicle recordings of its entire fleet of taxis over the past year to locate recordings of the individual would require considerable time and effort. VWX may rely on the exception to deny the access request if the burden or expense of providing the requested access would be unreasonable to VWX or disproportionate to the individual's interests.
33	Advisory Guidelines for the Real Estate Agency Sector		
34	Advisory Guidelines for the Healthcare Sector		The Access and Correction Obligations The Access and Correction Obligations (PDPA sections 21, 22 and 22A) state that an organisation must, upon request, (i) provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year; and (ii) correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation. For more information on the Access and Correction Obligations, do refer to Chapter 15 of the Advisory Guidelines on Key

			Concepts in the PDPA. The following examples illustrate the application of the Access and Correction Obligations. Example: Responding to requests to access personal data John makes an access request to Clinic ABC, requesting for access to his personal data and how it has been used and disclosed by the clinic, on 5th December 2022. Clinic ABC has to provide John with the complete set of personal data requested that is in its possession or under its control (e.g. including personal data contained in its files in storage), and inform him about the ways in which the personal data has been or may have been used or disclosed, subject to any relevant exceptions in the PDPA. The clinic may, in good faith, ask John to be more specific as to what personal data he requires, to facilitate processing of the access request, or to determine whether the request falls within one of the exceptions in the Fifth Schedule to the PDPA. Before responding to an access request, the clinic should exercise due diligence and adopt appropriate measures to verify John's identity. How the personal data should be provided The clinic is not necessarily obliged to provide John with copies of the original documents in which the requested personal data reside (e.g. registration forms or doctor's notes) although it may be the most convenient means to provide access. Where possible, the clinic may provide such personal data in a form other than the original form in which such personal data was recorded. Example 1

			John requests access to personal data that he had provided through a registration form. In addition to the registration form, the clinic had recorded the personal data in a patient record card, and in an electronic system. The clinic is required to provide John with all his personal data but is not required to provide a duplicate of the registration form, patient record card or electronic system. Example 2 John requests for the diagnosis of a condition that he had visited the clinic for, which had been recorded in handwritten notes of the doctor. The clinic is not obliged to provide a photocopy of the handwritten notes, although it should provide John with the information he requested in an appropriate form, such as through a medical report, unless a relevant exception applies. The goal is to provide John with an account of his personal data that is contained in the document and how it has been used or disclosed. Where this goal is more easily achieved through a redacted document provided to John, redaction can be considered. In certain circumstances, it may be impracticable to redact the handwritten notes and still provide a redacted document that is intelligible. The clinic has to take into consideration what is reasonable in the circumstances and whether the mode of providing access enables John to understand how his personal data had been used or disclosed. Providing information about how personal data has been used and disclosed In relation to how the personal data has been used and disclosed, the clinic has to

			provide John with information about the ways in which his personal data has been or may have been used or disclosed within a year before the date of request, i.e. for the period 6th December 2021 to 5th December 2022, unless any exception applies. The clinic may develop a standard list of parties to which personal data is routinely used and disclosed, and in many cases, may provide this standard list as the first response to access requests for information relating to how the personal data has been or may have been disclosed within the past year. The clinic should keep this list updated. Other matters relating to an access request The clinic may charge John a reasonable fee for the access request, and must respond to the access request as soon as reasonably possible. If the clinic is unable to respond to an access request within 30 days from the time the request is made, the clinic must inform John in writing within the 30-day time frame of when it will be able to respond to the request, which should be the soonest possible time it can provide access. Rejecting an access request If the clinic rejects John's access request based on an exception from the Access Obligation under the Fifth Schedule to the PDPA, the clinic shall provide a reply to John and inform him of the relevant reason(s) for refusing his request. In this case, the clinic is still required to preserve a complete and accurate copy of John's personal data for a period of at least 30 calendar days after rejecting the access request, as John may

			seek a review of the clinic's decision. More information on how an organisation should respond to an access request and what constitutes a 'reasonable fee' can be found in Chapter 15 of the Advisory Guidelines on Key Concepts in the PDPA. Example: Responding to requests for correction of personal data John makes the following requests to Clinic ABC: a) To correct his contact details in the clinic's records to reflect his new postal address. b) To correct the information about his smoking habits which the doctor recorded during a visit by him to the clinic. c) To correct a diagnosis about his medical condition. In relation to the scenarios above, a) It would be reasonable for Clinic ABC to correct John's contact details to ensure that they are accurate and current. b) The clinic may decide not to correct its record about John's smoking habits, if it is satisfied upon reasonable grounds that a correction need not be made. c) Where the diagnosis is a professional or expert opinion, section 22(6) of the PDPA provides that the clinic is not required to correct or otherwise alter it. If the clinic does not make the corrections requested, the clinic should annotate such personal data with the corrections that were requested but not made. Rights and obligations, etc under other laws Existing rights, etc under law and other written law Section 4(6)(a) of the PDPA states that unless otherwise provided in the PDPA, nothing in

			Parts 3 to 6 of the PDPA (the Data Protection Provisions in the PDPA) shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening the PDPA. Section 4(6)(b) states that the provisions of other written law shall prevail to the extent that any provision of Parts 3 to 6 is inconsistent with the provisions of that other written law. That is, the provisions of the other written law will apply in respect of the matter(s) which is inconsistent between those provisions and Parts 3 to 6 of the PDPA. Other provisions in the PDPA which are not inconsistent with the other written law will continue to apply. Accordingly, organisations should continue to comply with their obligations under other written laws such as the PHMC Act, HCSA, National Registry of Diseases Act, Infectious Diseases Act, and Advance Medical Directive Act. Section 13(b) of the PDPA provides that an organisation shall not, on or after the Data Protection Provisions come into effect, collect, use or disclose personal data about an individual without the consent of the individual unless the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under the PDPA or any other written law. Example: Requirement to comply with other written law Section 6(1) of the Infectious Diseases Act (Cap. 137) states that every medical practitioner who has reason to believe or

			suspect that any person attended or treated by him is suffering from an infectious disease or is a carrier of that disease shall notify the Director of Medical Services within the prescribed time and in such form or manner as the Director may require. As this is a requirement under written law, the medical practitioner is not required under the PDPA to obtain the consent of the individual in order to notify the Director in compliance with the Infectious Diseases Act. Use of personal data collected before the appointed day Section 19 of the PDPA provides that notwithstanding the other provisions of Part 4 of the PDPA (which relate to collection, use and disclosure of personal data), an organisation may use personal data collected before the appointed day (i.e. 2nd July 2014) for the purposes for which the personal data was collected, unless consent for such use is withdrawn or the individual has indicated to the organisation that he does not consent to the use of the personal data. Such 'use' could include disclosure that is necessarily part of the organisation's use of such personal data. The effect of section 19 is that organisations can continue to use personal data collected before the appointed day for the same purposes for which the personal data was collected without obtaining fresh consent, unless the individual has withdrawn consent (whether before on, or after the appointed day). For the avoidance of doubt, the Do Not Call Provisions will apply to the sending of specified messages to Singapore

			telephone numbers, even if the Singapore telephone numbers had been collected before the appointed day. Example: Using personal data collected before the appointed day Dental Clinic ABC collected John's personal data before 2nd July 2014 and has been sending him reminders by post to visit the dental clinic. Hitherto, John has not withdrawn consent, nor has he indicated that he does not consent to such use of his personal data. Dental Clinic ABC may continue to send such reminders to John until he indicates that he no longer wishes to receive them.
35	Advisory Guidelines for the Telecommunication Sector		
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		The Access and Correction Obligation in the PDPA 4 – Access and Correction Obligation in PDPA An organisation must, upon request: i. provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data has been or may have been used or disclosed during the past year; and ii. correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation. Upon receipt of a correction request, the organisation should consider whether the correction should be made. Unless the organisation is satisfied on reasonable grounds that a

			correction should not be made, the organisation shall correct the personal data as soon as practicable and send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose. If an organisation is satisfied upon reasonable grounds that a correction should not be made section 22(5) requires the organisation to annotate (that is, make a note to) the personal data in its possession or under its control indicating the correction that was requested but not made. Request for Access to Personal Data 31. A tied agent who receives a request for access to personal data shall ensure that the individual: i. fills in the prescribed form of the life insurer; or ii. submits the request in writing with sufficient information for the life insurer to process the request. 32. The tied agent shall, within the stated timeline prescribed by the life insurer, submit the following to the appointed person of the life insurer: i. whichever is applicable, the completed prescribed form or written request obtained from the individual; ii. (if applicable) any personal data of the individual which the tied agent has; or iii. (if applicable) any information which the tied agent has about the ways in which the personal data has been or may have been used or disclosed during the past year.

			33. If the tied agent intends to or has provided some or all of the personal data requested directly to the individual, the tied agent should: i. inform the life insurer that he intends to do so or has done so; and ii. inform the individual as to whether the life insurer would be providing other relevant personal data in response to the access request. 34. Upon receipt of an access request, the life insurer may contact the individual who submitted the access request directly to obtain any necessary information required for the life insurer to process the request. 35. Where the life insurer receives an access request for personal data or information, the life insurer may contact the individual directly to find out the identities of the tied agent(s) to whom the individual has provided personal data, and any other relevant information. 36. If necessary, the life insurer may request the personal data and information directly from the relevant tied agent(s) identified by the individual. The tied agent(s) shall, within the stated timeline prescribed by the life insurer, provide the life insurer with the requested personal data or information. 37. For the avoidance of doubt, if a tied agent receives an access request for personal data that is solely in his possession or under his control (and not in the possession of or under the control of the life insurer), the tied agent shall provide the personal data to the individual directly. 38. In addition, the tied agent shall adhere to the life insurer's standards on request for access

			to personal data. Request for Correction of Personal Data 39. A tied agent who receives a request for the correction of personal data shall ensure that the individual: i. fills in the prescribed form of the life insurer; or ii. submits the request in writing in with sufficient information for the life insurer to process the request. 40. Upon receipt of a request to correct personal data, the tied agent shall, within the stated timeline prescribed by the life insurer, submit the completed prescribed form or written request to the appointed person of the life insurer. 41. Unless satisfied on reasonable grounds that a correction need not be made, the tied agent shall make the requested correction to the personal data which is in the possession or under the control of the tied agent. 42. In addition, the tied agent shall adhere to the life insurer's standards on correction of personal data.

#	Regulation	Right to rectification	Right to erasure
1	Personal Data Protection Act 2012	Correction of personal data 22.—(1) An individual may request an organisation to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organisation. (2) Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation must — (a) correct the personal data as soon as practicable; and (b) subject to subsection (3), send	

		the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose. (3) An organisation (not being a credit bureau) may, if the individual consents, send the corrected personal data only to specific organisations to which the personal data was disclosed by the organisation within a year before the date the correction was made. (4) When an organisation is notified under subsection (2)(b) or (3) of a correction of personal data, the organisation must correct the personal data in its possession or under its control unless the organisation is satisfied on reasonable grounds that the correction should not be made. (5) If no correction is made under subsection (2)(a) or (4), the organisation must annotate the personal data in its possession or under its control with the correction that was requested but not made. (6) Nothing in this section requires an organisation to correct or otherwise alter an opinion, including a professional or an expert opinion. (7) An organisation is not required to comply with this section in respect of the matters specified in the Sixth Schedule.	
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		

5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		

17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment		
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act	The Access and Correction Obligations 15.1 Sections 21, 22 and 22A of the PDPA set out the rights of individuals to request for access to their personal data and for correction of their personal data that is in the possession or under the control of an organisation, and the corresponding obligations of the organisation to provide access to, and correction of, the individual's personal data. These obligations are collectively referred to in these Guidelines as the Access and Correction Obligations as they operate together to provide individuals with the ability to verify their personal data held by an organisation. 15.2 The Access and Correction Obligations relate to personal data in an organisation's possession as well as personal data that is under its control (which may not be in its possession). For example, if an organisation has transferred personal data to a data intermediary that is processing	

		the personal data under the control of the organisation, the organisation's response to an access or correction request must take into account the personal data which is in the possession of the data intermediary. The PDPA does not directly impose the Access and Correction Obligations on a data intermediary in relation to personal data that it is processing only on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing28. A data intermediary may (but is not obligated under the PDPA to) forward the individual's access or correction request to the organisation that controls the personal data. The Commission understands that, in some cases, an organisation may wish to enter into a contract with its data intermediary for the data intermediary to assist with responding to access or correction requests on its behalf. In this connection, the Commission would remind organisations that engage the data intermediary, that they remain responsible for ensuring compliance with the Access and Correction Obligations under the PDPA. Please refer to the sections on data intermediaries and their obligations for more information. Obligation to provide access to personal data 15.3 Section 21(1) of the PDPA provides that, upon request by an individual, an organisation must provide the individual with the following as soon as reasonably possible: a) personal data about the individual that is in the possession or under the	

		control of the organisation; and b) information about the ways in which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request. 15.4 Section 21(1) allows an individual to submit a request to an organisation for access to personal data about him that is in the possession or under the control of the organisation (an "access request"). Such a request may be for: a) some or all of the individual's personal data; and b) information about the ways the personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request. 15.5 An organisation's obligation in responding to an access request is to provide the individual access to the personal data requested by the individual which is in the organisation's possession or under its control, unless any relevant exception in section 21 or the Fifth Schedule to the PDPA applies. 15.6 To be clear, an organisation is not required to provide access to the documents (or systems) which do not comprise or contain the personal data in question, so long as the organisation provides the individual with the personal data that the individual requested and is entitled to have access to under section 21 of the PDPA. In the case of a document containing the personal data in question, the organisation should, where feasible, provide only the personal data (or relevantsections of the document containing the personal data) without providing	

		access to the entire document in its original form. 15.7 An organisation does not need to provide access to information which is no longer within its possession or under its control when the access request is received. The organisation should generally inform the requesting individual that it no longer possesses the personal data and is thus unable to meet the individual's access request. Organisations are also not required to provide information on the source of the personal data. 15.8 In certain circumstances, the individual making the access request may ask for a copy of his personal data in documentary form. Organisations should provide the copy and have the option of charging the individual a reasonable fee for producing the copy (please see the section on "fees chargeable for access to personal data" for more details). If the requested personal data resides in a form that cannot practicably be provided to the individual in documentary form, whether as physical or electronic copies (for example, the data cannot be extracted from a special machine owned by the organisation), then the organisation may provide the individual a reasonable opportunity to examine the requested data in person. 15.9 Organisations should note that the obligation to provide access applies equally to personal data captured in unstructured forms, such as personal data embedded in emails. Organisations are generally required to implement processes to keep track of the collection, use, and disclosure of all personal data under their	

		control, including unstructured data. Organisations should note that they are not required to provide access if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interest or if the request is otherwise frivolous or vexatious. Please see the sections on exceptions to the obligation to provide access to personal data for more details (including situations where an organisation must not provide access). 15.10 If the personal data requested by the individual can be retrieved by the individual himself (e.g. resides in online portals in which access has been granted by the organisation), the organisation may inform the individual how he may retrieve the data requested. Example: Organisation ABC receives a request from John seeking to know what personal data relating to him was disclosed in Organisation ABC's correspondence with Organisation DEF in a specified month within the last one year. Assuming that the request does not fall under any relevant exception (for example, it is not opinion data kept solely for an evaluative purpose), ABC is required to provide John with his personal data even if its correspondence with DEF had not been archived in a formalised system such as a database. To be clear, ABC's obligation is limited to providing John with the full set of his personal data that he requested which is in its possession or control, and it is not necessarily required to provide John with copies of the	

		actual correspondence with DEF. 15.11 The PDPA does not expressly state that an access request be accompanied by a reason for making the request. However, an organisation should ask the applicant to be more specific as to what type of personal data he requires, the time and date the personal data was collected, to facilitate processing of the access request, or to determine whether the request falls within one of the prohibitions under section 21(3) of the PDPA or any exception in the Fifth Schedule29. When assessing an access request, the organisation should consider the purpose of the applicant's access request, so as to determine the appropriate manner and form in which access to the personal data should be provided. For instance, the organisation may determine that it will provide the individual a snapshot from a video recording, instead of a masked video clip, as the most cost effective and efficient way to allow an individual to show that he was present at a particular location at a specific date and time. If the individual is unable or unwilling to provide more details, the organisation should make an attempt to respond to the access request as accurately and completely as reasonably possible. 15.12 Before responding to an access request, organisations should exercise due diligence and adopt appropriate measures to verify an individual's identity. While the Commission does not prescribe the manner in which organisations are to obtain verification from the individual making an access request, organisations are encouraged to	

		have documentary evidence to demonstrate that they are in compliance with the PDPA, and minimise any potential disputes. Organisations may implement policies setting out the standard operating procedures on conducting verification when processing access requests (e.g. this may include the questions that an employee handling the access request may ask the applicant in order to verify his identity)30. 15.13 In a situation where a third party is making an access request on behalf of an individual, organisations receiving the access request should ensure that the third party has the legal authority to validly act on behalf of the individual. 15.14 In some cases, there may be two or more individuals (e.g. husband and wife) making an access request at the same time for their respective personal data captured in the same set of records. The organisation may obtain consent31 from the respective individuals to disclose their personal data to each other, so that it may provide the individuals access to a common data set containing their personal data, without having to exclude the personal data of the other individuals32. If such consent cannot be obtained, an organisation receiving such requests may provide access to the personal data to the individuals separately, for example, by masking the personal data of the other individuals before providing the individual access to his own personal data (i.e. the individual will be provided access to only his own personal data). Information relating to ways	

		which personal data has been used or disclosed 15.15 As stated in section 21(1) of the PDPA, if an individual requests for information relating to the use or disclosure of his personal data by the organisation, the organisation is required to provide information relating to how the personal data has been or may have been used or disclosed within the past year. In this regard, an organisation may develop a standard list of all possible third parties to whom personal data may have been disclosed by the organisation. In many cases, an organisation may provide this standard list as an alternative to providing the specific set of third parties to whom the personal data has been disclosed, as part of its response to access requests that ask for information relating to how the personal data has been or may have been disclosed within the past year. The organisation should also update the standard list regularly and ensure that the information is accurate before providing the list to the individual. Generally, in responding to a request for information on third parties to which personal data has been disclosed, the organisation should individually identify each possible third party (e.g. 'pharmaceutical company ABC'), instead of simply providing general categories of organisations (e.g. 'pharmaceutical companies') to which personal data has been disclosed. This would allow individuals to directly approach the third party organisation to which their personal data has been disclosed. 15.16 In specifying how the personal data has been or may	

		have been used or disclosed within the past year, organisations may provide information on the purposes rather than the specific activities for which the personal data had been or may have been used or disclosed. For example, an organisation may have disclosed personal data to external auditors on multiple occasions in the year before the access request. In responding to an access request, the organisation may state that the personal data was disclosed for audit purposes rather than describing all the instances when the personal data was disclosed. 15.17 Generally, the organisation's actual response would depend on the specific request, and organisations are reminded that in meeting their responsibilities under the PDPA, they are to consider what a reasonable person would consider appropriate in the circumstances. Example: Sarah makes an access request to her spa, requesting for information relating to how her personal data has been used or disclosed. The request was made on 5 December 2015. The spa is only required to provide information on how her personal data has been used or disclosed within the past year – that is, the period from 6 December 2014 to the date of the request, 5 December 2015. Response time frame for an access request 15.18 Subject to the PDPA and the Personal Data Protection Regulations 202133, an organisation is required to comply with section 21(1) of the PDPA and must respond to an access request as soon as	

		reasonably possible from the time the access request is received. If an organisation is unable to respond to an access request within 30days34 after receiving the request, the organisation shall inform the individual in writing within 30 days of the time by which it will be able to respond to the request. When not to accede to an access request 15.19 An organisation must respond to an access request by providing access to the personal data requested, or by informing the individual of a rejection of the access request where it has valid grounds not to provide access. 15.20 Organisations are not required to accede to a request if an exception35 from the access requirement applies. 15.21 Additionally, an organisation shall not inform any individual or organisation that it has disclosed personal data to a prescribed law enforcement agency if the disclosure is necessary for any investigation or proceedings and the personal data is disclosed to an authorised36 officer of the agency. In this regard, an organisation may refuse to confirm or deny the existence of personal data, or the use of personal data without consent for any investigation or proceedings, if the investigation or proceedings and related appeals have not been completed. It also does not have to respond to a request unless the applicant agrees to pay the fee for services provided to the applicant to enable the organisation to respond to the applicant's request. This is provided the	

		organisation has provided the applicant a written estimate of the fee. Where applicable, the Commission may review the fee by confirming, reducing or disallowing the fee, or directing the organisation to make a refund to the applicant. 15.23 An organisation shall not accede to an access request if any of the grounds in section 21(3) are applicable, for instance, where the provision of the personal data or other information could reasonably be expected to threaten the safety or physical or mental health of an individual other than the requesting individual, or to cause immediate or grave harm to the safety or physical or mental health of the requesting individual. 15.24 If the organisation searches for the requested personal data but is unable to respond to the access request within the 30-day timeframe (e.g. technical processing of personal data residing in a specific format requires more time), the organisation must inform the applicant within the 30-day timeframe of the date when it will be able to respond to the request, and must still respond to the request as soon as reasonably possible. Fees chargeable to comply with the access obligation 15.25 An organisation may charge an individual a reasonable fee to process an access request by the individual37. The purpose of the fee is to allow organisations to recover the incremental costs of responding to the access request. This may include the time and costs incurred to search for the personal data requested. An example of such	

		incremental costs is the cost of producing a physical copy of the personal data for the individual requesting it. As organisations are required to make the necessary arrangements to provide for standard types of access requests, costs incurred in capital purchases (e.g. purchasing new equipment in order to provide access to the requested personal data) should not be transferred to individuals. 15.26 The Commission is of the view that it would be difficult to prescribe a standard fee or range of fees at the outset to apply across all industries or all types of access requests. Organisations should exercise proper judgement in deriving the reasonable fee they charge based on their incremental costs of providing access. The Commission may, upon the application of an individual, review a fee charged by an organisation under section 48H of the PDPA (among other matters). In reviewing a fee, the Commission may consider the relevant circumstances, including the absolute amount of the fee, the incremental cost of providing access which may include the time and costs incurred to search for the personal data requested, and similar fees charged in the industry. 15.27 If an organisation wishes to charge an individual a fee to process an access request, the organisation must give the individual a written estimate of the fee38. If the organisation wishes to charge a fee higher than the original written estimate, it must inform the individual in writing of the increased fee. The organisation may refuse to process or provide	

		access to the individual's personal data until the individual agrees to pay the relevant fee. Example: Company ZYX receives an access request from a customer to view his personal data stored in a format that is readable only by a special machine. The company owns two such machines but both are faulty. In order to respond to the customer's request in a timely manner, ZYX purchases another machine and transfers its cost to the customer as part of the access fee. Because of this, the access fee amounts to $50,000. This would not be considered a reasonable fee as ZYX is expected to have the general means to comply with its customers' access requests. Example: An individual requests from Company TUV a paper copy of his personal data. Company TUV charges a fee of $50 for the information printed out on 50 pages of paper, based on the incremental cost of producing the copy. The fee is reasonable as it reflects the incremental cost of providing the personal data. Exceptions to the obligation to provide access to personal data 15.28 The obligation in section 21(1) is subject to a number of exceptions in sections 21(2) to 21(4) including some mandatory exceptions relating to situations where an organisation must not provide access. These exceptions are listed below. 15.29 Section 21(2) of the PDPA provides that an organisation is not required to provide individuals with the personal data or other information specified in section 21(1) in respect of the matters specified	

		in the Fifth Schedule to the PDPA. An organisation is not prohibited from providing information in respect of the matters specified in the Fifth Schedule and may do so if it decides to. 15.30 The exceptions specified in the Fifth Schedule include the following matters: a) opinion data kept solely for an evaluative purpose39; b) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results; c) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust; d) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; e) a document related to a prosecution if all proceedings related to the prosecution have not yet been completed; f) personal data which is subject to legal privilege; g) personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation; h) personal data collected, used or disclosed without consent for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed40; i) personal data collected by an arbitrator or mediator in the conduct or an arbitration or mediation for which he or she	

		was appointed to act – i. under a collective agreement under the Industrial Relations Act 1960; ii. by agreement between the parties to the arbitration or mediation; iii. under any written law; or iv. by a court, arbitral institution or mediation centre; or j) any request — i. that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests (i.e. considering the number and frequency of requests received); ii. if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests; iii. for information that does not exist or cannot be found; iv. for information that is trivial; or v. that is otherwise frivolous or vexatious. Example: A shopping centre receives a request from an individual to view all CCTV footage of him recorded at the shopping centre over the past year. In this scenario, reviewing all CCTV footage from the past year to find records of the individual making the request would require considerable time and effort. To the extent that the burden of providing access would be unreasonable to the shopping centre and disproportionate to the individual's interests as the individual is making a general request for all CCTV footage, the shopping centre is unlikely to have to provide the requested personal data under the Access Obligation.	

		Example: A shop in the shopping centre receives a request from an individual to view a photograph of him taken by the official photographer at a private event held recently by the shop that the individual was invited to. The individual provides the shop with sufficient information to determine when the event was held. The provision of access in this case would be reasonable and the shop should provide the photograph which the individual requested. Example: An individual sends an email providing feedback to Organisation XYZ. The form contains his personal data including his full name and contact number. A day later, he requests access to the personal data in the form while having full knowledge of the information he is requesting. Such a request is likely to be considered frivolous or vexatious, unless it can be shown otherwise. Example: An individual submits an access request every fortnight for the same set of personal data in Organisation ABC's possession. Such requests are likely to be considered to unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests. 15.31 In addition to the matters specified in the Fifth Schedule to the PDPA, section 21(3) specifies a number of situations in which an organisation must not provide the personal data or other information specified in section 21(1). 15.32 The situations specified in section 21(3) are where the	

		provision of personal data or other information under section 21(1) could reasonably be expected to: a) threaten the safety or physical or mental health of an individual other than the individual who made the request; b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request; c) reveal personal data about another individual41; d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his or her identity; or e) be contrary to the national interest42. Providing personal data of an individual without the personal data of other individuals 15.33 Section 21(5) of the PDPA provides that if an organisation is able to provide the individual with his personal data and other information requested under section 21(1) without the personal data of other information excluded under sections 21(2), 21(3) and 21(4), the organisation must provide the individual access to the requested personal data and other information without the personal data or other information excluded. Organisations may request information about the purpose of the access request so that it can consider if it is able to provide the requested personal data without the personal data of the other individuals, such as by masking out the personal data of other individual(s) before providing the personal data requested by the individual.	

		Example: Mary requested Travel Agency ABC to furnish formal documentation confirming the cancellation of her transit flight to process her insurance claims. As the letter from the airline also contains the personal data of 36 other passengers who signed up for the same tour package, e.g. name, nationality, date of birth and passport number, ABC assesses that it is possible to provide Mary access to her personal data without revealing the other individuals' personal data by redacting the personal data of the other passengers from the letter. Access that may reveal personal data about another individual 15.34 One of the prohibitions, section 21(3)(c), requires that an organisation must not provide access to the personal data or other information under section 21(1) where the provision of personal data or other information could reasonably be expected to reveal personal data about another individual. The prohibition does not apply to any user activity data43 about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual. Although organisations do not need to mask or remove personal data of these other individuals in user-activity or provided data, organisations should still consider if the other harmful situations in 21(3) may arise. In addition, the Commission is of the view that this prohibition does not apply in circumstances where: a) any of the exceptions relating to disclosure of personal data without consent listed under the	

		First and Second Schedules to the PDPA apply to the extent that the organisation may disclose the personal data of the other individual without consent (e.g. if the personal data of the individual is publicly available or if the organisation can rely on the legitimate interests exception); b) as permitted or required by any other law and regulation (e.g. exercise of police investigatory powers, compliance with discovery directions in civil proceedings or regulations governing building maintenance and strata management); or c) the other individual has given consent to the disclosure of his personal data. Example: Betty applies to Shopping Centre ABC for access to CCTV footage of herself walking through the aisles of the shopping centre on a specific day and time. The CCTV footage contains images of other individuals.Since the images of the other shoppers are recorded in a public area, the data is considered publicly available. Shopping Centre ABC does not need to obtain consent of the other shoppers in the CCTV footage or mask their images before providing access to Betty. Example: John applies to Organisation DEF for records of his transactions and purchases made on DEF's platform. Some of the transactions and purchases made by John on DEF's platform contain personal data of a third-party (e.g. name of third-party whom John had sent an item to after purchasing that item on the platform). As the personal data of the third-party forms part of John's user activity data in this	

		instance, Organisation DEF may provide John with access to the data without redacting the personal data of the third-party. Example: Jane applies to Condominium ABC for access to CCTV footage of herself at the Condominium's taxi drop off point where she had an altercation with a thirdparty. As the taxi drop off point is open to the public, ABC can rely on the publicly available data exception and need not mask the image of the thirdparty within the footage in providing Jane access to the requested footage. Example: Jack is a subsidiary proprietor/owner of a unit in Condominium XYZ. Jack applies to Condominium XYZ's management for access to CCTV footage of himself at the condominium's lift lobby as he believes he dropped his personal belongings there. There were other people with Jack at the lift lobby at that time and Jack wishes to approach them for assistance in recovering his personal belongings. Under Section 47 of the Building Maintenance and Strata Management Act (BMSMA), a subsidiary proprietor/owner of a condominium unit may make an access request for the CCTV footage without the need to redact/mask the footage. 44 As PDPA is considered a baseline law, other sectoral regulations,such as BMSMA, which permit the access to unredacted footage, will take precedence in this instance. Example: There is a children's party being held at the function room of Condo KLM where a CCTV is installed. Jessie and her daughter, who do not stay or	

		own a unit in Condo KLM, are guests of the host of the party. Jessie loses her personal belongings at the party. She decides to go directly to Condo KLM's management to request for a copy of the CCTV footage to assist her in locating the belongings. KLM assesses that there is legitimate interest in providing Jessie with access to the footage, without masking the images of other individuals, to assist her in recovering her personal belongings. KLM also assesses that in doing so, there is no adverse effects to individuals present at the party. As such, KLM allows Jessie access to the requested footage. KLM designs an approval process for such requests and addresses risks of abuse by limiting Jessie's access to viewing of the relevant CCTV footage under supervision. Access request relating to disclosure to prescribed law enforcement agency 15.35 Section 21(4) of the PDPA contains an additional obligation of organisations in relation to the Access Obligation. That subsection provides that where an organisation has disclosed personal data to a prescribed law enforcement agency without the consent of the individual under the PDPA or any other written law, the organisation must not inform the individual that personal data has been disclosed.Access request relating to legal proceedings 15.36 Where personal data has been collected for the purpose of prosecution, investigation, civil proceedings and associated proceedings and appeals, paragraph 1(h) of the Fifth Schedule may apply to exempt such personal	

		data from the accessrequest. Organisations are thus not required to provide the requested information. Further, under paragraph 1(e) of the Fifth Schedule, access need not be provided in respect of a document related to a prosecution if all proceedings related to the prosecution have not been completed. 15.37 Where personal data has been collected prior to the commencement of prosecution and investigations but is nonetheless relevant to the proceedings, an individual should obtain access through criminal and civil discovery avenues rather than through the Access Obligation under the PDPA. The intent of the Access Obligationis to ensure that organisations remain accountable for the personal data of individualsin their possession or under their control, including ensuring the accuracy and proper use of the personal data. The Data Protection Provisions of the PDPA do not affect discovery obligations under law that parties to a legal dispute may have (e.g. pursuant to any order of court). For instance, if criminal disclosure of civil discovery regimes are applicable, section 4(6) of the PDPA applies, and any request for access to the personal data should be made pursuant to any other written laws providing for such disclosure or discovery applications. A possible advantage of obtaining access to personal data through the discovery process is that it allows the requestor to obtain un-redacted and complete documents, while and access	

		request would grant the requestor only his personal data, with other content redacted. Rejecting an access request 15.38 Subj	
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions		
26	Advisory Guidelines on Application of PDPA to Election Activities	Access and Correction Obligations 4.16 A political party or election candidate must, upon request, (a) provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year16; or (b) correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation.	
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		

29	Advisory Guidelines for Management Corporations	Handling access and correction requests 3.7 Under the PDPA, MCSTs are required to provide access to or make a correction to the individual's personal data in the MCSTs' possession or under their control upon the individual's request, unless a relevant exception under sections 21 or 22 of the PDPA applies27. For example, MCSTs must provide access to an individual's personal data captured in close-circuit television camera ("CCTV") footage requested by the individual, unless an exception applies. To be clear, MCSTs may not limit the provision of access to personal data only to law enforcement or other relevant authorities, or for the purposes of investigations by such authorities. To this end, MCSTs must develop and implement policies and processes for handling access and correction requests to ensure compliance with the PDPA. 3.8 MCSTs must also respond to an access request (i.e. provide access to the personal data) as soon as reasonably possible from the time the access request is received. If a MCST is unable to respond to an access request within 30 days after receiving the request, the MCST must inform the individual in writing within 30 days of the time by which it will be able to respond to the request. MCSTs may charge a reasonable fee for providing the requested access that reflects the time and effort required to respond to the access request. 3.9 While the PDPA does not require that an access request be accompanied by a reason for making the request, as good practice, MCSTs could ask the	

		applicant to be more specific as to what type of personal data is required, as well as the time and date the personal data was collected, to facilitate processing of the access request, or to determine whether the request falls within one of the prohibitions under section 21(3) of the PDPA or any exception in the Fifth or Sixth Schedule. MCSTs could also ask the applicant as to what form a CCTV footage extract could be provided in (e.g. screenshot or video footage), in order to fulfil the access request in the most cost efficient manner. 3.10 In situations where access and correction requests are handled by managing agents, MCSTs should establish clear policies and processes for the handling of access and correction requests by these managing agents to ensure compliance with the PDPA. 3.11 Please refer to Chapter 15 of the Advisory Guidelines on Key Concepts in the PDPA for further information relating to the Access and Correction Obligations, as well as the Guide on Responsible Use of Biometric Data in Security Applications for more information on best practices for the collection, use, and disclosure of biometric data responsibly. The section on CCTVs in the Selected Topics Advisory Guidelines also provides examples relating to access requests.	
30	Advisory Guidelines for the Education Sector	3 The Access and Correction Obligation 3.1 Section 21(1) of the PDPA provides that, upon request by an individual, an organisation shall provide the individual with the following as soon as reasonably possible: a) personal data about the	

		individual that is in their possession or under the control of the organisation; and b) information about the ways in which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request. 3.2 The Fifth Schedule to the PDPA contains exceptions to this obligation such as where the data is opinion data kept solely for an evaluative purpose; or the information is in respect of any examination conducted by an education institution, examination scripts and prior to the release of examination results, examination results. 3.3 Section 22(1) of the PDPA provides that an individual may submit a request for an organisation to correct an error or omission in the individual's personal data that is in the possession or under the control of the organisation ("a correction request"). Upon receipt of a correction request, the organisation is generally required to make the correction, subject to applicable exceptions10. 3.4 In particular, section 22(2) goes on to provide that unless the organisation is satisfied on reasonable grounds that the correction should not be made, it should: a) correct the personal data as soon as practicable; and b) send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within the year before the date the correction request was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.	

		3.5 If an organisation is satisfied upon reasonable grounds that a correction should not be made (whether the organisation is responding to a correction request made directly by the individual or has been notified of a correction made by such an organisation), section 22(5) requires the organisation to annotate (that is, make a note to) the personal data in its possession or under its control indicating the correction that was requested but not made. As a good practice, the organisation may also wish to annotate the reasons why it has decided that the correction should not be made. 3.6 The obligation to correct personal data is subject to a number of exceptionsin Section 22 and the Sixth Schedule of the PDPA. One such exception relates to personal data which is opinion data kept solely for an evaluative purpose11. 3.7 The following examples illustrate the application of the Access and Correction Obligation. 3.8 Example: Access to student's records Jack intends to apply for a job with Company ABC after graduating from School DEF. To provide information to support his application, Jack makes an access request to School DEF for records of his co-curricular activities and a transcript of his examination results. School DEF is required to provide access to the information in accordance with section 21(1) of the PDPA, unless there is an applicable exception. 3.9 Example: Accessing results of language competency test Prior to enrolment into School ABC, all students are required to	

		undergo a language competency test. Grace makes an access request after taking the test (but before the release of results) to School ABC to find out her test grade. In this case, School ABC is not required to accede to Grace's access request as there is an exception under the Fifth Schedule to the PDPA in relation to information that is in respect of any examination conducted by an education institution, examination scripts and prior to the release of examination results, examination results. 3.10 Example: Correction of residential address Peter finds out that a cheque refund mailed out by School ABC to him was mistakenly sent to his neighbour residing two storeys above him. Peter makes a correction request for School ABC to amend the residential address recorded in School ABC's system from 123, DEF Road, #04-02 to 123, DEF Road, #02-04. As there are no reasonable grounds for the correction not to be made, School ABC corrects the listing of Peter's residential address so as to be able to communicate with him by mail. 3.11 Example: Correction of a teacher's opinion Karen's mother, Mary, notices a teacher's remarks in Karen's annual assessment report that Karen tends to lose attention during certain classes, and that Karen needs to improve her handwriting. Mary makes a correction request to the school to omit these remarks from Karen's report. In this case, the school is not required to make corrections to the teacher's remarks to the extent that the remarks are regarded as an opinion.	

31	Advisory Guidelines for the Social Service Sector	4 The Access and Correction Obligation 4.1 The Access and Correction Obligations (PDPA sections 21, 22 and 22A) state that an organisation must, upon request, (i) provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year; and (ii) correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation. For more information on the Access and Correction Obligations, do refer to Chapter 15 of the Advisory Guidelines on Key Concepts in the PDPA. 4.2 The following examples illustrate the application of the Access and Correction Obligations. 4.3 Example: Accessing personal data of one individual which was provided by another individual SSA ABC is launching a new social service scheme targeting the elderly. Madam Chua, a widow who lives in a one-room apartment, intends to apply for SSA ABC's new scheme. As part of the application process, Madam Chua is required to provide SSA ABC with the personal data of her family members or those in her support system in order for SSA ABC to assess her suitability. Madam Chua discloses the full names of her five children, and their marital status. In addition, Madam Chua discloses that one of her children, Alan is not her biological son and was adopted. She added that Alan was not aware that he was an adopted child.	

		Alan learns about his mother's application for the social service scheme and makes an access request for the personal data SSA ABC has about him, and how it had been used by SSA ABC. Treatment Generally, SSA ABC should provide Alan access to his personal data which is in the possession or under the control of SSA ABC and information about the ways in which such personal data has been or may have been used or disclosed by SSA ABC over the past year. However, SSA ABC must consider if any prohibition under section 21 applies.16 For example, section 21(3) of the PDPA prohibits SSA ABC from providing Alan with his personal data or other information, as the case may be, if doing so could reasonably be expected to cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request. 17 In this regard, SSA ABC may reject Alan's access request as disclosure may cause harm to his mental health. SSA ABC may also wish to consider if any of the exceptions to the Access Obligation set out in the Fifth Schedule apply. SSA ABC should generally exercise due diligence and adopt appropriate measures to verify the identity of Alan before providing him with access to his personal data.	
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for		

	the Real Estate Agency Sector		
34	Advisory Guidelines for the Healthcare Sector	The Access and Correction Obligations The Access and Correction Obligations (PDPA sections 21, 22 and 22A) state that an organisation must, upon request, (i) provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year; and (ii) correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation. For more information on the Access and Correction Obligations, do refer to Chapter 15 of the Advisory Guidelines on Key Concepts in the PDPA. The following examples illustrate the application of the Access and Correction Obligations. Example: Responding to requests to access personal data John makes an access request to Clinic ABC, requesting for access to his personal data and how it has been used and disclosed by the clinic, on 5th December 2022. Clinic ABC has to provide John with the complete set of personal data requested that is in its possession or under its control (e.g. including personal data contained in its files in storage), and inform him about the ways in which the personal data has been or may have been used or disclosed, subject to any relevant exceptions in the PDPA. The clinic may, in good faith, ask John to be more specific as to what personal data he requires, to facilitate processing of the access request, or to determine	

		whether the request falls within one of the exceptions in the Fifth Schedule to the PDPA. Before responding to an access request, the clinic should exercise due diligence and adopt appropriate measures to verify John's identity. How the personal data should be provided The clinic is not necessarily obliged to provide John with copies of the original documents in which the requested personal data reside (e.g. registration forms or doctor's notes) although it may be the most convenient means to provide access. Where possible, the clinic may provide such personal data in a form other than the original form in which such personal data was recorded. Example 1 John requests access to personal data that he had provided through a registration form. In addition to the registration form, the clinic had recorded the personal data in a patient record card, and in an electronic system. The clinic is required to provide John with all his personal data but is not required to provide a duplicate of the registration form, patient record card or electronic system. Example 2 John requests for the diagnosis of a condition that he had visited the clinic for, which had been recorded in handwritten notes of the doctor. The clinic is not obliged to provide a photocopy of the handwritten notes, although it should provide John with the information he requested in an appropriate form, such as through a medical report, unless a relevant exception applies. The goal is to provide John with an account of his personal data that	

		is contained in the document and how it has been used or disclosed. Where this goal is more easily achieved through a redacted document provided to John, redaction can be considered. In certain circumstances, it may be impracticable to redact the handwritten notes and still provide a redacted document that is intelligible. The clinic has to take into consideration what is reasonable in the circumstances and whether the mode of providing access enables John to understand how his personal data had been used or disclosed. Providing information about how personal data has been used and disclosed In relation to how the personal data has been used and disclosed, the clinic has to provide John with information about the ways in which his personal data has been or may have been used or disclosed within a year before the date of request, i.e. for the period 6th December 2021 to 5th December 2022, unless any exception applies. The clinic may develop a standard list of parties to which personal data is routinely used and disclosed, and in many cases, may provide this standard list as the first response to access requests for information relating to how the personal data has been or may have been disclosed within the past year. The clinic should keep this list updated. Other matters relating to an access request The clinic may charge John a reasonable fee for the access request, and must respond to the access request as soon as reasonably possible. If the clinic is unable to respond to an access request within 30 days	

		from the time the request is made, the clinic must inform John in writing within the 30-day time frame of when it will be able to respond to the request, which should be the soonest possible time it can provide access. Rejecting an access request If the clinic rejects John's access request based on an exception from the Access Obligation under the Fifth Schedule to the PDPA, the clinic shall provide a reply to John and inform him of the relevant reason(s) for refusing his request. In this case, the clinic is still required to preserve a complete and accurate copy of John's personal data for a period of at least 30 calendar days after rejecting the access request, as John may seek a review of the clinic's decision. More information on how an organisation should respond to an access request and what constitutes a 'reasonable fee' can be found in Chapter 15 of the Advisory Guidelines on Key Concepts in the PDPA. Example: Responding to requests for correction of personal data John makes the following requests to Clinic ABC: a) To correct his contact details in the clinic's records to reflect his new postal address. b) To correct the information about his smoking habits which the doctor recorded during a visit by him to the clinic. c) To correct a diagnosis about his medical condition. In relation to the scenarios above, a) It would be reasonable for Clinic ABC to correct John's contact details to ensure that they are accurate and current.	

		b) The clinic may decide not to correct its record about John's smoking habits, if it is satisfied upon reasonable grounds that a correction need not be made. c) Where the diagnosis is a professional or expert opinion, section 22(6) of the PDPA provides that the clinic is not required to correct or otherwise alter it. If the clinic does not make the corrections requested, the clinic should annotate such personal data with the corrections that were requested but not made. Rights and obligations, etc under other laws Existing rights, etc under law and other written law Section 4(6)(a) of the PDPA states that unless otherwise provided in the PDPA, nothing in Parts 3 to 6 of the PDPA (the Data Protection Provisions in the PDPA) shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening the PDPA. Section 4(6)(b) states that the provisions of other written law shall prevail to the extent that any provision of Parts 3 to 6 is inconsistent with the provisions of that other written law. That is, the provisions of the other written law will apply in respect of the matter(s) which is inconsistent between those provisions and Parts 3 to 6 of the PDPA. Other provisions in the PDPA which are not inconsistent with the other written law will continue to apply. Accordingly, organisations should continue to comply with their obligations	

		under other written laws such as the PHMC Act, HCSA, National Registry of Diseases Act, Infectious Diseases Act, and Advance Medical Directive Act. Section 13(b) of the PDPA provides that an organisation shall not, on or after the Data Protection Provisions come into effect, collect, use or disclose personal data about an individual without the consent of the individual unless the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under the PDPA or any other written law. Example: Requirement to comply with other written law Section 6(1) of the Infectious Diseases Act (Cap. 137) states that every medical practitioner who has reason to believe or suspect that any person attended or treated by him is suffering from an infectious disease or is a carrier of that disease shall notify the Director of Medical Services within the prescribed time and in such form or manner as the Director may require. As this is a requirement under written law, the medical practitioner is not required under the PDPA to obtain the consent of the individual in order to notify the Director in compliance with the Infectious Diseases Act. Use of personal data collected before the appointed day Section 19 of the PDPA provides that notwithstanding the other provisions of Part 4 of the PDPA (which relate to collection, use and disclosure of personal data), an organisation may use personal data collected before the appointed day (i.e. 2nd July 2014) for the purposes for which the personal data was collected,	

		unless consent for such use is withdrawn or the individual has indicated to the organisation that he does not consent to the use of the personal data. Such 'use' could include disclosure that is necessarily part of the organisation's use of such personal data. The effect of section 19 is that organisations can continue to use personal data collected before the appointed day for the same purposes for which the personal data was collected without obtaining fresh consent, unless the individual has withdrawn consent (whether before on, or after the appointed day). For the avoidance of doubt, the Do Not Call Provisions will apply to the sending of specified messages to Singapore telephone numbers, even if the Singapore telephone numbers had been collected before the appointed day. Example: Using personal data collected before the appointed day Dental Clinic ABC collected John's personal data before 2nd July 2014 and has been sending him reminders by post to visit the dental clinic. Hitherto, John has not withdrawn consent, nor has he indicated that he does not consent to such use of his personal data. Dental Clinic ABC may continue to send such reminders to John until he indicates that he no longer wishes to receive them.	
35	Advisory Guidelines for the Telecommunication Sector		
36	Joint Technical Advisory on LockBit 3.0		

37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act	The Access and Correction Obligation in the PDPA 4 – Access and Correction Obligation in PDPA An organisation must, upon request: i. provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data has been or may have been used or disclosed during the past year; and ii. correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation. Upon receipt of a correction request, the organisation should consider whether the correction should be made. Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation shall correct the personal data as soon as practicable and send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose. If an organisation is satisfied upon reasonable grounds that a correction should not be made section 22(5) requires the organisation to annotate (that is, make a note to) the personal data in its possession or under its control indicating the correction that was requested but not made. Request for Access to Personal Data 31. A tied agent who receives a request for access to personal	

		data shall ensure that the individual: i. fills in the prescribed form of the life insurer; or ii. submits the request in writing with sufficient information for the life insurer to process the request. 32. The tied agent shall, within the stated timeline prescribed by the life insurer, submit the following to the appointed person of the life insurer: i. whichever is applicable, the completed prescribed form or written request obtained from the individual; ii. (if applicable) any personal data of the individual which the tied agent has; or iii. (if applicable) any information which the tied agent has about the ways in which the personal data has been or may have been used or disclosed during the past year. 33. If the tied agent intends to or has provided some or all of the personal data requested directly to the individual, the tied agent should: i. inform the life insurer that he intends to do so or has done so; and ii. inform the individual as to whether the life insurer would be providing other relevant personal data in response to the access request. 34. Upon receipt of an access request, the life insurer may contact the individual who submitted the access request directly to obtain any necessary information required for the life insurer to process the request. 35. Where the life insurer receives an access request for personal data or information, the life insurer may contact the individual directly to find out the identities of the tied agent(s) to	

		whom the individual has provided personal data, and any other relevant information. 36. If necessary, the life insurer may request the personal data and information directly from the relevant tied agent(s) identified by the individual. The tied agent(s) shall, within the stated timeline prescribed by the life insurer, provide the life insurer with the requested personal data or information. 37. For the avoidance of doubt, if a tied agent receives an access request for personal data that is solely in his possession or under his control (and not in the possession of or under the control of the life insurer), the tied agent shall provide the personal data to the individual directly. 38. In addition, the tied agent shall adhere to the life insurer's standards on request for access to personal data. Request for Correction of Personal Data 39. A tied agent who receives a request for the correction of personal data shall ensure that the individual: i. fills in the prescribed form of the life insurer; or ii. submits the request in writing in with sufficient information for the life insurer to process the request. 40. Upon receipt of a request to correct personal data, the tied agent shall, within the stated timeline prescribed by the life insurer, submit the completed prescribed form or written request to the appointed person of the life insurer. 41. Unless satisfied on reasonable grounds that a correction need not be made, the tied agent shall make the requested correction to the personal data which is in the	

		possession or under the control of the tied agent. 42. In addition, the tied agent shall adhere to the life insurer's standards on correction of personal data.	

#	Regulation	Right to restrict processing	Right to data portability
1	Personal Data Protection Act 2012		Preservation of copies of personal data 22A.—(1) Where — (a) an individual, on or after 1 February 2021, makes a request under section 21(1)(a) to an organisation to provide personal data about the individual that is in the possession or under the control of the organisation; and (b) the organisation refuses to provide that personal data, the organisation must preserve, for not less than the prescribed period, a copy of the personal data concerned. [40/2020] (2) The organisation must ensure that the copy of the personal data it preserves for the purposes of subsection (1) is a complete and accurate copy of the personal data concerned.
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		

8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for		

	Children's Personal Data in the Digital Environment		
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act		
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions		
26	Advisory Guidelines on Application of PDPA to Election Activities		
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for		

	Marketing Purposes		
29	Advisory Guidelines for Management Corporations		
30	Advisory Guidelines for the Education Sector		
31	Advisory Guidelines for the Social Service Sector		
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector		
34	Advisory Guidelines for the Healthcare Sector		
35	Advisory Guidelines for the Telecommunication Sector		
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		

#	Regulation	Right to object	Right not to be subject to a decision based solely on automated processing
1	Personal Data Protection Act 2012		

2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement		

	Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment		
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act		
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions		

26	Advisory Guidelines on Application of PDPA to Election Activities		
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		
29	Advisory Guidelines for Management Corporations		
30	Advisory Guidelines for the Education Sector		
31	Advisory Guidelines for the Social Service Sector		
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector		
34	Advisory Guidelines for the Healthcare Sector		
35	Advisory Guidelines for the Telecommunication Sector		

36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		

#	Regulation	Right to withdraw consent	others
1	Personal Data Protection Act 2012	Withdrawal of consent 16.—(1) On giving reasonable notice to the organisation, an individual may at any time withdraw any consent given, or deemed to have been given under this Act, in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose. (2) On receipt of the notice mentioned in subsection (1), the organisation concerned must inform the individual of the likely consequences of withdrawing his or her consent. (3) An organisation must not prohibit an individual from withdrawing his or her consent to the collection, use or disclosure of personal data about the individual, but this section does not affect any legal consequences arising from such withdrawal. (4) Subject to section 25, if an individual withdraws consent to the collection, use or disclosure of personal data about the individual by an organisation for any purpose, the organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data (as the case may be) unless	

		such collection, use or disclosure (as the case may be) without the individual's consent is required or authorised under this Act or other written law.	
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare		

	Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment		
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act		
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		

24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions		
26	Advisory Guidelines on Application of PDPA to Election Activities		
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		
29	Advisory Guidelines for Management Corporations		
30	Advisory Guidelines for the Education Sector		
31	Advisory Guidelines for the Social Service Sector		
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector	4 Rights and obligations, etc under other laws 4.1 Section 19 of the PDPA provides that notwithstanding the other provisions of Part IV of the PDPA (which contain some of the Data Protection Provisions), an organisation may use personal data collected before	

		the appointed day for the purposes for which the personal data was collected, unless consent for such use is withdrawn or the individual has indicated to the organisation that he does not consent to the use of the personal data. Such 'use' could include disclosure that is necessarily part of the organisation's use of such personal data. For avoidance of doubt, the Do Not Call Provisions will apply to the sending of specified messages to Singapore telephone numbers, even if the Singapore telephone numbers are collected before the appointed day. 4.2 Example: Existing use of personal data Estate agent ABC has been using the database of past and existing clients, collected before the appointed day (i.e. 2 July 2014), to send them flyers on new launches. ABC may continue to use such personal data for the reasonable purpose of sending clients flyers about new launches. For the avoidance of doubt, if ABC collects the personal data on or after the appointed day, ABC will have to comply with the relevant Data Protection Provisions, including obtaining the consent of its new clients to collect, use and disclose their personal data for the intended purposes. ABC wishes to call the clients in its database to market its new launches. While ABC may not need to obtain consent under the Data Protection Provisions to use the personal data of its clients in the database to call them for its new launches, the Do Not Call Provisions separately apply. ABC is required to either check and confirm that the Singapore	

		telephone number is not listed on the Do Not Call Registers within the prescribed period before making the marketing call. An exception is when ABC has obtained the clear and unambiguous consent of the subscriber or user of the Singapore telephone number in evidential form to the sending of the marketing message, or it is exempted from checking the registers for the sending of such message under the Personal Data Protection (Exemption from Section 43) Order (S.817/2013) ("Exemption Order"). ABC can rely on clear and unambiguous consent in evidential form that it has obtained before the appointed day to send the marketing message. 4.3 Section 4(6) of the PDPA states that unless otherwise provided in the PDPA, nothing in Parts III to VI of the PDPA shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening the PDPA, and the provisions of other written law shall prevail to the extent that any provision of Parts III to VI is inconsistent with the provisions of that other written law. 4.4 Section 13(b) of the PDPA provides that an organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual without the consent of the individual unless the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under the PDPA or any other written law.	

34	Advisory Guidelines for the Healthcare Sector		
35	Advisory Guidelines for the Telecommunication Sector		
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		

Extraterritorial application

#	Regulation	applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction	applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction
1	Personal Data Protection Act 2012		
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		

9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
20	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment		

21	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
22	Introduction to the Guidelines		
23	Advisory Guidelines on Key Concepts in the Personal Data Protection Act		
24	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
25	Advisory Guidelines on Enforcement of Data Protection Provisions		
26	Joint Advisory on ALTDOS		
27	Advisory Guidelines on the Do Not Call Provisions	PART VII: OTHER CLARIFICATIONS Locations of sender and recipient It should be noted that the locations of the sender and recipient when a specified message is sent and accessed affect whether the DNC Provisions apply. Section 38 of the PDPA provides that the DNC Provisions apply where: a) the sender of the specified message is in Singapore when the message is sent; or b) the recipient of the specified message is in Singapore when the message is accessed. Under section 38, the DNC Provisions do not apply if both the sender and the recipient are not in Singapore when the specified message is sent and accessed respectively. This may be the situation, for example, when the recipient is travelling in	

		another country and accesses a specified message sent by a sender in that country. However, the DNC Provisions would apply if the recipient is travelling in another country and the sender is in Singapore. The DNC Provisions also apply where one of the senders is located overseas while another is located in Singapore.	
28	Advisory Guidelines on Application of PDPA to Election Activities		
29	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
30	Advisory Guidelines on Requiring Consent for Marketing Purposes		
31	Advisory Guidelines for Management Corporations		
32	Advisory Guidelines for the Education Sector		
33	Advisory Guidelines for the Social Service Sector		
34	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
35	Advisory Guidelines for the Real Estate Agency Sector		

36	Advisory Guidelines for the Healthcare Sector		
37	Advisory Guidelines for the Telecommunication Sector		
38	Joint Technical Advisory on LockBit 3.0		
39	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		

#	Regulation		
		no express territorial scope, but would require some nexus to the jurisdiction	other
1	Personal Data Protection Act 2012		"organisation" includes any individual, company, association or body of persons, corporate or unincorporated, whether or not — (a) formed or recognised under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore; Application of Act 4.—(1) Parts 3, 4, 5, 6, 6A and 6B do not impose any obligation on — (a) any individual acting in a personal or domestic capacity; (b) any employee acting in the course of his or her employment with an organisation; (c) any public agency; or (d) any other organisations or personal data, or classes of organisations or personal data, prescribed for the purposes of this provision. [40/2020]

			(2) Parts 3, 4, 5, 6 (except sections 24 and 25), 6A (except sections 26C(3)(a) and 26E) and 6B do not impose any obligation on a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing. [40/2020] (3) An organisation has the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself. (4) This Act does not apply in respect of — (a) personal data about an individual that is contained in a record that has been in existence for at least 100 years; or (b) personal data about a deceased individual, except that the provisions relating to the disclosure of personal data and section 24 (protection of personal data) apply in respect of personal data about an individual who has been dead for 10 years or less. (5) Except where business contact information is expressly mentioned, Parts 3, 4, 5, 6 and 6A do not apply to business contact information. [40/2020] (6) Unless otherwise expressly provided in this Act — (a) nothing in Parts 3, 4, 5, 6, 6A and 6B affects any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation is not an excuse for contravening this Act; and

			(b) the provisions of other written law prevail to the extent that any provision of Parts 3, 4, 5, 6, 6A and 6B is inconsistent with the provisions of that other written law.
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare		

	Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
17	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
18	Personal Data Protection (Statutory Bodies) Notification 2013		
19	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment		
20	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
21	Introduction to the Guidelines		
22	Advisory Guidelines on Key Concepts in the Personal Data Protection Act		
23	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
24	Advisory Guidelines on Enforcement of Data Protection Provisions		

25	Joint Advisory on ALTDOS		
26	Advisory Guidelines on the Do Not Call Provisions		
27	Advisory Guidelines on Application of PDPA to Election Activities		
28	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
29	Advisory Guidelines on Requiring Consent for Marketing Purposes		
30	Advisory Guidelines for Management Corporations		
31	Advisory Guidelines for the Education Sector		
32	Advisory Guidelines for the Social Service Sector		
33	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
34	Advisory Guidelines for the Real Estate Agency Sector		
35	Advisory Guidelines for the Healthcare Sector		

36	Advisory Guidelines for the Telecommunication Sector		
37	Joint Technical Advisory on LockBit 3.0		
38	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		

#	Regulation	Representatives of controllers or processors not established in the country
1	Personal Data Protection Act 2012	
2	Public Sector (Governance) Act 2018	
3	Telecommunications Act 1999	
4	CRIMINAL PROCEDURE CODE 2010	
5	Cybersecurity Act 2018	
6	Workplace Safety and Health (Medical Examinations) Regulations 2011	
7	Banking Act 1970	
8	PERSONAL DATA PROTECTION REGULATIONS 2021	
9	Personal Data Protection (Appeal) Regulations 2021	
10	Personal Data Protection (Composition of Offences) Regulations 2021	

11	Personal Data Protection (Do Not Call Registry) Regulations 2013	
12	Personal Data Protection (Enforcement) Regulations 2021	
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021	
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015	
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014	
17	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020	
18	Personal Data Protection (Statutory Bodies) Notification 2013	
19	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment	
20	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems	
21	Introduction to the Guidelines	

22	Advisory Guidelines on Key Concepts in the Personal Data Protection Act	
23	Advisory Guidelines on the Personal Data Protection Act for Selected Topics	
24	Advisory Guidelines on Enforcement of Data Protection Provisions	
25	Joint Advisory on ALTDOS	
26	Advisory Guidelines on the Do Not Call Provisions	
27	Advisory Guidelines on Application of PDPA to Election Activities	
28	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers	
29	Advisory Guidelines on Requiring Consent for Marketing Purposes	
30	Advisory Guidelines for Management Corporations	
31	Advisory Guidelines for the Education Sector	
32	Advisory Guidelines for	

	the Social Service Sector	
33	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire	
34	Advisory Guidelines for the Real Estate Agency Sector	
35	Advisory Guidelines for the Healthcare Sector	
36	Advisory Guidelines for the Telecommunication Sector	
37	Joint Technical Advisory on LockBit 3.0	
38	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act	

Notification obligation

#	Regulation		
		Data breach notification to authorities	Data breach notification to affected individuals
1	Personal Data Protection Act 2012	Notifiable data breaches 26B.—(1) A data breach is a notifiable data breach if the data breach — (a) results in, or is likely to result in, significant harm to an affected individual; or (b) is, or is likely to be, of a	Notifiable data breaches 26B.—(1) A data breach is a notifiable data breach if the data breach — (a) results in, or is likely to result in, significant harm to an affected individual; or (b) is, or is likely to be, of a

		significant scale. [40/2020] (2) Without limiting subsection (1)(a), a data breach is deemed to result in significant harm to an individual — (a) if the data breach is in relation to any prescribed personal data or class of personal data relating to the individual; or (b) in other prescribed circumstances. [40/2020] (3) Without limiting subsection (1)(b), a data breach is deemed to be of a significant scale — (a) if the data breach affects not fewer than the prescribed number of affected individuals; or (b) in other prescribed circumstances. [40/2020] (4) Despite subsections (1), (2) and (3), a data breach that relates to the unauthorised access, collection, use, disclosure, copying or modification of personal data only within an organisation is deemed not to be a notifiable data breach. [40/2020] Duty to notify occurrence of notifiable data breach 26D.—(1) Where an organisation assesses, in accordance with section 26C, that a data breach is a notifiable data breach, the organisation must notify the Commission as soon as is practicable, but in any case no later than 3 calendar days after the day the organisation makes that assessment. [40/2020] (2) Subject to subsections (5), (6) and (7), on or after notifying the Commission under subsection (1), the organisation must also	significant scale. [40/2020] (2) Without limiting subsection (1)(a), a data breach is deemed to result in significant harm to an individual — (a) if the data breach is in relation to any prescribed personal data or class of personal data relating to the individual; or (b) in other prescribed circumstances. [40/2020] (3) Without limiting subsection (1)(b), a data breach is deemed to be of a significant scale — (a) if the data breach affects not fewer than the prescribed number of affected individuals; or (b) in other prescribed circumstances. [40/2020] (4) Despite subsections (1), (2) and (3), a data breach that relates to the unauthorised access, collection, use, disclosure, copying or modification of personal data only within an organisation is deemed not to be a notifiable data breach. [40/2020] Duty to notify occurrence of notifiable data breach 26D.—(1) Where an organisation assesses, in accordance with section 26C, that a data breach is a notifiable data breach, the organisation must notify the Commission as soon as is practicable, but in any case no later than 3 calendar days after the day the organisation makes that assessment. [40/2020] (2) Subject to subsections (5), (6) and (7), on or after notifying the Commission under subsection (1), the organisation must also

		notify each affected individual affected by a notifiable data breach mentioned in section 26B(1)(a) in any manner that is reasonable in the circumstances. [40/2020] (3) The notification under subsection (1) or (2) must contain, to the best of the knowledge and belief of the organisation at the time it notifies the Commission or affected individual (as the case may be),all the information that is prescribed for this purpose. [40/2020] (4) The notification under subsection (1) must be made in the form and submitted in the manner required by the Commission. [40/2020] (5) Subsection (2) does not apply to an organisation in relation to an affected individual if the organisation — (a) on or after assessing that the data breach is a notifiable data breach, takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or (b) had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual. [40/2020] (6) An organisation must not notify any affected individual in accordance with subsection (2) if — (a) a prescribed law enforcement agency so instructs; or (b) the Commission so directs.	notify each affected individual affected by a notifiable data breach mentioned in section 26B(1)(a) in any manner that is reasonable in the circumstances. [40/2020] (3) The notification under subsection (1) or (2) must contain, to the best of the knowledge and belief of the organisation at the time it notifies the Commission or affected individual (as the case may be), all the information that is prescribed for this purpose. [40/2020] (4) The notification under subsection (1) must be made in the form and submitted in the manner required by the Commission. [40/2020] (5) Subsection (2) does not apply to an organisation in relation to an affected individual if the organisation — (a) on or after assessing that the data breach is a notifiable data breach, takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or (b) had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual. [40/2020] (6) An organisation must not notify any affected individual in accordance with subsection (2) if — (a) a prescribed law enforcement agency so instructs; or (b) the Commission so directs. [40/2020]

		[40/2020] (7) The Commission may, on the written application of an organization, waive the requirement to notify an affected individual under subsection (2) subject to any conditions that the Commission thinks fit. [40/2020] (8) An organisation is not, by reason only of notifying the Commission under subsection (1) or an affected individual under subsection (2), to be regarded as being in breach of — (a) any duty or obligation under any written law or rule of law, or any contract, as to secrecy or other restriction on the disclosure of information; or (b) any rule of professional conduct applicable to the organisation. [40/2020] (9) Subsections (1) and (2) apply concurrently with any obligation of the organisation under any other written law to notify any other person (including any public agency) of the occurrence of a data breach, or to provide any information relating to a data breach.	(7) The Commission may, on the written application of an organisation, waive the requirement to notify an affected individual under subsection (2) subject to any conditions that the Commission thinks fit. [40/2020] (8) An organisation is not, by reason only of notifying the Commission under subsection (1) or an affected individual under subsection (2), to be regarded as being in breach of — (a) any duty or obligation under any written law or rule of law, or any contract, as to secrecy or other restriction on the disclosure of information; or (b) any rule of professional conduct applicable to the organisation. [40/2020] (9) Subsections (1) and (2) apply concurrently with any obligation of the organisation under any other written law to notify any other person (including any public agency) of the occurrence of a data breach, or to provide any information relating to a data breach.
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION		

	REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021	Data breach resulting in significant harm to individuals 3.—(1) For the purposes of section 26B(2) of the Act, a data breach is deemed to result in significant harm to an individual if the data breach relates to — (a) the individual's full name or alias or identification number, and any of the personal data or classes of personal data relating to the individual set out in Part 1 of the Schedule, subject to Part 2 of the Schedule; or (b) all of the following personal data relating to an individual's account with an organisation: (i) the individual's account identifier, such as an account name or number; (ii) any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account. (2) In paragraph (1)(b), "account identifier" includes a number assigned to any account the individual has with an organisation that is a bank or finance company. Data breach of significant scale	Data breach resulting in significant harm to individuals 3.—(1) For the purposes of section 26B(2) of the Act, a data breach is deemed to result in significant harm to an individual if the data breach relates to — (a) the individual's full name or alias or identification number, and any of the personal data or classes of personal data relating to the individual set out in Part 1 of the Schedule, subject to Part 2 of the Schedule; or (b) all of the following personal data relating to an individual's account with an organisation: (i) the individual's account identifier, such as an account name or number; (ii) any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account. (2) In paragraph (1)(b), "account identifier" includes a number assigned to any account the individual has with an organisation that is a bank or finance company. Data breach of significant scale

		4. For the purposes of section 26B(3)(a) of the Act, the prescribed number of affected individuals is 500. Notification to Commission 5.—(1) For the purposes of section 26D(3) of the Act, the notification by an organisation to the Commission of a notifiable data breach under section 26D(1) of the Act must include all of the following information: (a) the date on which and the circumstances in which the organisation first became aware that the data breach had occurred; (b) a chronological account of the steps taken by the organisation after the organisation became aware that the data breach had occurred, including the organisation's assessment under section 26C(2) or (3)(b) of the Act that the data breach is a notifiable data breach; (c) information on how the notifiable data breach occurred; (d) the number of affected individuals affected by the notifiable data breach; (e) the personal data or classes of personal data affected by the notifiable data breach; (f) the potential harm to the affected individuals as a result of the notifiable data breach; (g) information on any action by the organisation, whether taken before or to be taken after the organisation notifies the Commission of the occurrence of the notifiable data breach — (i) to eliminate or mitigate any potential harm to any affected individual as a result of the notifiable data breach; and (ii) to address or remedy any failure or shortcoming that the organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable	4. For the purposes of section 26B(3)(a) of the Act, the prescribed number of affected individuals is 500. Notification to Commission 5.—(1) For the purposes of section 26D(3) of the Act, the notification by an organisation to the Commission of a notifiable data breach under section 26D(1) of the Act must include all of the following information: (a) the date on which and the circumstances in which the organisation first became aware that the data breach had occurred; (b) a chronological account of the steps taken by the organisation after the organisation became aware that the data breach had occurred, including the organisation's assessment under section 26C(2) or (3)(b) of the Act that the data breach is a notifiable data breach; (c) information on how the notifiable data breach occurred; (d) the number of affected individuals affected by the notifiable data breach; (e) the personal data or classes of personal data affected by the notifiable data breach; (f) the potential harm to the affected individuals as a result of the notifiable data breach; (g) information on any action by the organisation, whether taken before or to be taken after the organisation notifies the Commission of the occurrence of the notifiable data breach — (i) to eliminate or mitigate any potential harm to any affected individual as a result of the notifiable data breach; and (ii) to address or remedy any failure or shortcoming that the organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable

		data breach; (h) information on the organisation's plan (if any) to inform, on or after notifying the Commission of the occurrence of the notifiable data breach, all or any affected individuals or the public that the notifiable data breach has occurred and how an affected individual may eliminate or mitigate any potential harm as a result of the notifiable data breach; (i) the business contact information of at least one authorised representative of the organisation. (2) If the organisation notifies the Commission of the notifiable data breach after the expiry of the period specified in section 26D(1) of the Act, the notification to the Commission must additionally specify the reasons for the late notification and include any supporting evidence. (3) Where, despite section 26D(2) of the Act, the organisation does not intend to notify any affected individual affected by a notifiable data breach mentioned in section 26B(1)(a) of the Act of the occurrence of that data breach, the notification to the Commission must additionally specify the grounds (whether under the Act or other written law) for not notifying the affected individual. (4) The notification by the organisation to the Commission must be in the form and manner specified on the Commission's website at www.pdpc.gov.sg. Notification to affected individuals 6. For the purposes of section 26D(3) of the Act, the notification by an organisation to an affected individual affected by a notifiable data breach under section 26D(2)	data breach; (h) information on the organisation's plan (if any) to inform, on or after notifying the Commission of the occurrence of the notifiable data breach, all or any affected individuals or the public that the notifiable data breach has occurred and how an affected individual may eliminate or mitigate any potential harm as a result of the notifiable data breach; (i) the business contact information of at least one authorised representative of the organisation. (2) If the organisation notifies the Commission of the notifiable data breach after the expiry of the period specified in section 26D(1) of the Act, the notification to the Commission must additionally specify the reasons for the late notification and include any supporting evidence. (3) Where, despite section 26D(2) of the Act, the organisation does not intend to notify any affected individual affected by a notifiable data breach mentioned in section 26B(1)(a) of the Act of the occurrence of that data breach, the notification to the Commission must additionally specify the grounds (whether under the Act or other written law) for not notifying the affected individual. (4) The notification by the organisation to the Commission must be in the form and manner specified on the Commission's website at www.pdpc.gov.sg. Notification to affected individuals 6. For the purposes of section 26D(3) of the Act, the notification by an organisation to an affected individual affected by a notifiable data breach under section 26D(2)

		of the Act must contain all of the following information: (a) the circumstances in which the organisation first became aware that the notifiable data breach had occurred; (b) the personal data or classes of personal data relating to the affected individual affected by the notifiable data breach; (c) the potential harm to the affected individual as a result of the notifiable data breach; (d) information on any action by the organisation, whether taken before or to be taken after the organisation notifies the affected individual — (i) to eliminate or mitigate any potential harm to the affected individual as a result of the notifiable data breach; and (ii) to address or remedy any failure or shortcoming that the organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach; (e) the steps that the affected individual may take to eliminate or mitigate any potential harm as a result of the notifiable data breach, including preventing the misuse of the affected individual's personal data affected by the notifiable data breach; (f) the business contact information of at least one authorised representative of the organisation.	of the Act must contain all of the following information: (a) the circumstances in which the organisation first became aware that the notifiable data breach had occurred; (b) the personal data or classes of personal data relating to the affected individual affected by the notifiable data breach; (c) the potential harm to the affected individual as a result of the notifiable data breach; (d) information on any action by the organisation, whether taken before or to be taken after the organisation notifies the affected individual — (i) to eliminate or mitigate any potential harm to the affected individual as a result of the notifiable data breach; and (ii) to address or remedy any failure or shortcoming that the organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach; (e) the steps that the affected individual may take to eliminate or mitigate any potential harm as a result of the notifiable data breach, including preventing the misuse of the affected individual's personal data affected by the notifiable data breach; (f) the business contact information of at least one authorised representative of the organisation.
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement		

	Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment	Data breach notification Part 6A of the PDPA sets out the requirements for organisations to assess whether a data breach is notifiable, and to notify the affected individuals and/or the PDPC where it is assessed to be notifiable12. In the case of a data breach resulting in significant harm to individuals who are children, the organisation remains obliged to inform the affected data subject, even though the data subject is a child. If an organisation proactively informs the child's parent or guardian of the data breach (if the organisation has the contact details of the parent / guardian), the child's parent or guardian would be able to take steps to mitigate the harm of the data breach. Where the organisation does not have the contact details of the child's parent or guardian, the organisation should ensure that the data breach notification to the child is in a language that is readily understandable by the child so that the child may understand the consequences of the data breach. The organisation should also consider advising the child to inform his / her parent or guardian about the data breach.	Data breach notification Part 6A of the PDPA sets out the requirements for organisations to assess whether a data breach is notifiable, and to notify the affected individuals and/or the PDPC where it is assessed to be notifiable12. In the case of a data breach resulting in significant harm to individuals who are children, the organisation remains obliged to inform the affected data subject, even though the data subject is a child. If an organisation proactively informs the child's parent or guardian of the data breach (if the organisation has the contact details of the parent / guardian), the child's parent or guardian would be able to take steps to mitigate the harm of the data breach. Where the organisation does not have the contact details of the child's parent or guardian, the organisation should ensure that the data breach notification to the child is in a language that is readily understandable by the child so that the child may understand the consequences of the data breach. The organisation should also consider advising the child to inform his / her parent or guardian about the data breach.

		Example: Unauthorised access of students' records The database administrator of an edtech company discovers an unauthorised access to its student records. The edtech company immediately assesses the data breach and determines that the data breach involves records of students' name and email address. The records of approximately 20 children are affected. As the data breach only involves students' name and email address, the data breach is deemed to be unlikely to result in significant harm to an individual and the organisation need not notify the affected students of the data breach. While the edtech company is not required to notify the affected individuals, the edtech company chooses to demonstrate accountability by notifying the affected children's parent (or legal guardian) of the data breach since the relevant contact details were collected during the registration process. If the edtech company has only the contact details of the child, the edtech company could advise the child, in language that is readily understandable by the child, to notify his / her parent (or guardian). Notifying allows the child's parent or guardian to take steps to mitigate the harm of the data breach, such as by monitoring the emails sent to their child's account for suspicious content.	Example: Unauthorised access of students' records The database administrator of an edtech company discovers an unauthorised access to its student records. The edtech company immediately assesses the data breach and determines that the data breach involves records of students' name and email address. The records of approximately 20 children are affected. As the data breach only involves students' name and email address, the data breach is deemed to be unlikely to result in significant harm to an individual and the organisation need not notify the affected students of the data breach. While the edtech company is not required to notify the affected individuals, the edtech company chooses to demonstrate accountability by notifying the affected children's parent (or legal guardian) of the data breach since the relevant contact details were collected during the registration process. If the edtech company has only the contact details of the child, the edtech company could advise the child, in language that is readily understandable by the child, to notify his / her parent (or guardian). Notifying allows the child's parent or guardian to take steps to mitigate the harm of the data breach, such as by monitoring the emails sent to their child's account for suspicious content.
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		

20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act		
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions		
26	Advisory Guidelines on Application of PDPA to Election Activities	Data Breach Notification Obligation 4.27 A political party or election candidate must assess whether a data breach is notifiable21 and notify the affected individuals and/or the PDPC where it is assessed to be notifiable. 4.28 Data intermediaries that process the personal data on behalf and for the purposes of a political party or election candidate are also required to notify that political party or election candidate of a data breach detected. The political party or election candidate that engaged the data intermediary remains responsible for assessing whether the data breach is notifiable, or to notify affected individuals and/or the PDPC within the required timelines22. 4.29 As good practice, political parties or election candidates should establish clear procedures for complying with	Data Breach Notification Obligation 4.27 A political party or election candidate must assess whether a data breach is notifiable21 and notify the affected individuals and/or the PDPC where it is assessed to be notifiable. 4.28 Data intermediaries that process the personal data on behalf and for the purposes of a political party or election candidate are also required to notify that political party or election candidate of a data breach detected. The political party or election candidate that engaged the data intermediary remains responsible for assessing whether the data breach is notifiable, or to notify affected individuals and/or the PDPC within the required timelines22. 4.29 As good practice, political parties or election candidates should establish clear procedures for complying with

		the Data Breach Notification Obligation when entering into service agreements or contractual arrangements with their data intermediaries.	the Data Breach Notification Obligation when entering into service agreements or contractual arrangements with their data intermediaries.
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		
29	Advisory Guidelines for Management Corporations		
30	Advisory Guidelines for the Education Sector		
31	Advisory Guidelines for the Social Service Sector	9 The Data Breach Notification Obligation 9.1 The Data Breach Notification Obligation (PDPA sections 26A to 26E) states that an organisation must assess whether a data breach is notifiable and notify the affected individuals and/or the Commission where it is assessed to be notifiable. For more information on the Data Breach Notification Obligation, do refer to Chapter 20 of the Advisory Guidelines on Key Concepts in the PDPA. 9.2 The following examples illustrate the application of the Data Breach Notification Obligation. 9.3 Example: Contractual requirements to report data breaches to funders SSA 123 is funded by multiple public agencies. The funding contracts require SSA 123 to	9 The Data Breach Notification Obligation 9.1 The Data Breach Notification Obligation (PDPA sections 26A to 26E) states that an organisation must assess whether a data breach is notifiable and notify the affected individuals and/or the Commission where it is assessed to be notifiable. For more information on the Data Breach Notification Obligation, do refer to Chapter 20 of the Advisory Guidelines on Key Concepts in the PDPA. 9.2 The following examples illustrate the application of the Data Breach Notification Obligation. 9.3 Example: Contractual requirements to report data breaches to funders SSA 123 is funded by multiple public agencies. The funding contracts require SSA 123 to

		immediately report to these public agencies in the event of a data breach that is assessed to result in significant harm to affected individuals or is of a significant scale. Treatment According to Section 4(6)(a) of the PDPA, the provisions of the PDPA will not affect other legal obligations of SSA 123, such as SSA 123's contractual obligations to its funders, i.e. other public agencies. However, the performance of a contractual obligation is not an excuse for SSA 123 to contravene the PDPA. Hence, in case of a data breach assessed to result in significant harm to affected individuals or is of a significant scale, SSA 123 must, in addition to its complying with its contractual obligations to its funders, comply with the Data Breach Notification Obligation by notifying the PDPC and/or the affected individuals where necessary. 9.4 Example: Data breaches of significant harm and of significant scale SSA ABC deals with cases of youth offenders. It discovered that one of its staff had misplaced a secure thumb drive containing the full names of 20 young persons and information that leads to the identification of them as having been the subject of investigations under the Children and Young Persons Act (CYPA) or had been arrested, on or after 1 July 2020, for an offence committed under any written law. Another social service agency, SSA DEF, administers bursary awards to high performing students from lower income households. The database administrator of SSA DEF discovers an unauthorized	immediately report to these public agencies in the event of a data breach that is assessed to result in significant harm to affected individuals or is of a significant scale. Treatment According to Section 4(6)(a) of the PDPA, the provisions of the PDPA will not affect other legal obligations of SSA 123, such as SSA 123's contractual obligations to its funders, i.e. other public agencies. However, the performance of a contractual obligation is not an excuse for SSA 123 to contravene the PDPA. Hence, in case of a data breach assessed to result in significant harm to affected individuals or is of a significant scale, SSA 123 must, in addition to its complying with its contractual obligations to its funders, comply with the Data Breach Notification Obligation by notifying the PDPC and/or the affected individuals where necessary. 9.4 Example: Data breaches of significant harm and of significant scale SSA ABC deals with cases of youth offenders. It discovered that one of its staff had misplaced a secure thumb drive containing the full names of 20 young persons and information that leads to the identification of them as having been the subject of investigations under the Children and Young Persons Act (CYPA) or had been arrested, on or after 1 July 2020, for an offence committed under any written law. Another social service agency, SSA DEF, administers bursary awards to high performing students from lower income households. The database administrator of SSA DEF

		access of the personal data of their bursary award candidates. The unauthorized access is found to involve the email addresses and first names of 600 candidates, but not any of their financial information (e.g. debit card number, parents' salary). Treatment Both SSA ABC and SSA DEF shall conduct an assessment of the data breach once they discover it, generally within 30 calendar days, to establish the facts of the data breach and determine whether it is notifiable. The data breach faced by SSA ABC would likely result in significant harm to affected individuals and SSA ABC should notify the PDPC no later than 3 calendar days 19 upon determining that the data breach is notifiable, and the affected individuals at the same time or after notifying the PDPC. The Personal Data Protection (Notification of Data Breaches) Regulations 2021 provides that a combination of an individual's full name and personal data of vulnerable individuals, such as those of youth offenders or potential youth offenders contained in the misplaced thumb drive, is deemed to result in significant harm to affected individuals if compromised in a data breach. The data breach faced by SSA DEF is of a significant scale as it affects the personal data of 500 or more individuals, even if the personal data compromised (i.e. email addresses and first names) do not fall under the prescribed classes of data deemed by the Personal Data Protection (Notification of Data Breaches) Regulations 2021 to cause significant harm. SSA DEF	discovers an unauthorized access of the personal data of their bursary award candidates. The unauthorized access is found to involve the email addresses and first names of 600 candidates, but not any of their financial information (e.g. debit card number, parents' salary). Treatment Both SSA ABC and SSA DEF shall conduct an assessment of the data breach once they discover it, generally within 30 calendar days, to establish the facts of the data breach and determine whether it is notifiable. The data breach faced by SSA ABC would likely result in significant harm to affected individuals and SSA ABC should notify the PDPC no later than 3 calendar days 19 upon determining that the data breach is notifiable, and the affected individuals at the same time or after notifying the PDPC. The Personal Data Protection (Notification of Data Breaches) Regulations 2021 provides that a combination of an individual's full name and personal data of vulnerable individuals, such as those of youth offenders or potential youth offenders contained in the misplaced thumb drive, is deemed to result in significant harm to affected individuals if compromised in a data breach. The data breach faced by SSA DEF is of a significant scale as it affects the personal data of 500 or more individuals, even if the personal data compromised (i.e. email addresses and first names) do not fall under the prescribed classes of data deemed by the Personal Data Protection (Notification of Data Breaches) Regulations 2021 to

		must notify the PDPC of the data breach no later than 3 calendar days upon determining that the data breach is notifiable, but is not required to notify affected individuals.	cause significant harm. SSA DEF must notify the PDPC of the data breach no later than 3 calendar days upon determining that the data breach is notifiable, but is not required to notify affected individuals.
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector		
34	Advisory Guidelines for the Healthcare Sector	The Data Breach Notification Obligation The Data Breach Notification Obligation (PDPA sections 26A to 26E) states that an organisation must assess whether a data breach is notifiable and notify the affected individuals and/or the Commission where it is assessed to be notifiable. For more information on the Data Breach Notification Obligation, do refer to Chapter 20 of the Advisory Guidelines on Key Concepts in the PDPA.	The Data Breach Notification Obligation The Data Breach Notification Obligation (PDPA sections 26A to 26E) states that an organisation must assess whether a data breach is notifiable and notify the affected individuals and/or the Commission where it is assessed to be notifiable. For more information on the Data Breach Notification Obligation, do refer to Chapter 20 of the Advisory Guidelines on Key Concepts in the PDPA.
35	Advisory Guidelines for the Telecommunication Sector		
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		

Obligations of Data Fiduciaries

#	Regulation	external	external

		Notification of data processing	registration of database
1	Personal Data Protection Act 2012	Notification of purpose 20.—(1) For the purposes of sections 14(1)(a) and 18(b), an organisation must inform the individual of — (a) the purposes for the collection, use or disclosure of the personal data (as the case may be) on or before collecting the personal data; (b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose; and (c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data. (2) An organisation, on or before collecting personal data about an individual from another organisation without the individual's consent, must provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act. (3) Subsection (1) does not apply if — (a) the individual is deemed to have consented to the collection, use or disclosure (as the case may be) under section 15 or 15A; or (b) the organisation collects, uses or discloses the personal data without the individual's consent in accordance with section 17. [40/2020] (4) Despite subsection (3), an	

		organisation must comply with subsection (5) on or before collecting, using or disclosing personal data about an individual for the purpose of or in relation to the organisation — (a) entering into an employment relationship with the individual or appointing the individual to any office; or (b) managing or terminating the employment relationship with or appointment of the individual. [40/2020] (5) For the purposes of subsection (4), the organisation must inform the individual of the following: (a) the purpose for which the organisation is collecting, using or disclosing (as the case may be) the personal data about the individual; (b) on request by the individual, the business contact information of a person who is able to answer the individual's questions about that collection, use or disclosure (as the case may be) on behalf of the organisation. Duty to conduct assessment of data breach 26C.—(1) This section applies to a data breach that occurs on or after 1 February 2021. [40/2020] (2) Subject to subsection (3), where an organisation has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach. [40/2020] (3) Where a data intermediary (other than a data intermediary mentioned in section 26E) has	

		reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation — (a) the data intermediary must, without undue delay, notify that other organisation of the occurrence of the data breach; and (b) that other organisation must, upon notification by the data intermediary, conduct an assessment of whether the data breach is a notifiable data breach. [40/2020] (4) The organisation must carry out the assessment mentioned in subsection (2) or (3)(b) in accordance with any prescribed requirements. [40/2020] Duty to notify occurrence of notifiable data breach 26D.—(1) Where an organisation assesses, in accordance with section 26C, that a data breach is a notifiable data breach, the organisation must notify the Commission as soon as is practicable, but in any case no later than 3 calendar days after the day the organisation makes that assessment. [40/2020] (2) Subject to subsections (5), (6) and (7), on or after notifying the Commission under subsection (1), the organisation must also notify each affected individual affected by a notifiable data breach mentioned in section 26B(1)(a) in any manner that is reasonable in the circumstances. [40/2020] (3) The notification under subsection (1) or (2) must contain, to the best of the	

		knowledge and belief of the organisation at the time it notifies the Commission or affected individual (as the case may be), all the information that is prescribed for this purpose. [40/2020] (4) The notification under subsection (1) must be made in the form and submitted in the manner required by the Commission. [40/2020] (5) Subsection (2) does not apply to an organisation in relation to an affected individual if the organisation — (a) on or after assessing that the data breach is a notifiable data breach, takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or (b) had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely tha	
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		

9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		Registration of telecommunications service providers 12.—(1) For the purpose of section 42 of the Act, every telecommunications service provider before submitting its first report under regulation 13 shall register and maintain such registration with the Commission (referred to in this Part as a registered telecommunications service provider) in such form and manner as the Commission may require. (2) A registered telecommunications service provider shall notify the Commission, in such form and manner as the Commission may require, of any change or inaccuracy in its particulars and any other information submitted to the Commission in connection with its registration. (3) The Commission may cancel the registration of a registered telecommunications service provider if the telecommunications service provider — (a) notifies the Commission in such form and manner as the Commission may require that it has ceased to be licensed under the Telecommunications Act (Cap. 323) to provide any telecommunication service to which Singapore telephone numbers are allocated; (b) being a person carrying on a business as a telecommunications service

			provider in Singapore, ceases to carry on that business and the registration of that business under the Business Registration Act (Cap. 32) is cancelled; or (c) being a company incorporated under the Companies Act (Cap. 50) or a limited liability partnership registered under the Limited Liability Partnerships Act (Cap. 163A), is wound up under the Companies Act or the Limited Liability Partnerships Act, as the case may be. Submission of report on terminated Singapore telephone numbers 13.—(1) Subject to regulation 14(2), a registered telecommunications service provider when submitting a report to the Commission under section 42(1) of the Act shall comply with the following requirements: (a) the report shall be submitted to the Commission through such electronic facility as may be specified by the Commission; (b) the report shall be made in the form provided at the specified website for such report; and (c) subject to paragraph (2), the report shall be submitted not later than the 15th day of each month, listing every Singapore telephone number terminated in the immediately preceding month. (2) In the case of any Singapore telephone number terminated during the period from 1st December 2013 to 31st January 2014 (both dates inclusive), the registered telecommunications service provider of the telephone service associated with the telephone number shall submit the report referred to in paragraph (1) not later than 15th

			February 2014. (3) In the event of unavailability of the electronic facility referred to in paragraph (1)(a), whether due to maintenance, malfunction, failure or any other cause, the report referred to in paragraph (1) shall be submitted in such other form and manner as the Commission may require. Prescribed fee 14.—(1) For the purposes of section 42(5) of the Act and subject to paragraph (2), the Commission shall pay to a registered telecommunications service provider that submits a report under regulation 13 containing the number of terminated Singapore telephone numbers specified in the first column of the Third Schedule shall be the fee specified opposite in the second column. (2) If a registered telecommunications service provider submits 2 or more reports in a month, the reports shall, for the purposes of determining the fee payable under paragraph (1), collectively be considered to be a single report.
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement		

	Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment	Communication with children The Commission recognises that children are unique individuals with varying developmental abilities. While there is no one-size-fits-all approach when communicating with individuals within this age bracket, organisations should consider the nature of their content and adopt age-appropriate language and media (e.g. infographics, video clips). When communicating with children, organisations must use language that is readily understandable by children so that children may understand the consequences of providing and withdrawing consent. This means that the notification of purpose and consent clauses, data protection policies, and terms and conditions, must be in language that is readily understandable by children4	
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal	The Notification Obligation As noted in the previous chapters on the Consent Obligation and the Purpose	

	Data Protection Act	Limitation Obligation, organisations must inform individuals of the purposes for which their personal data will be collected, used and disclosed in order to obtain their consent. The organisation's collection, use and disclosure is limited to the purposes for which notification has been made to the individuals concerned. Section 20 of the PDPA sets out the obligation of organisations to inform individuals of these purposes. In particular, section 20(1) requires an organisation to inform the individual of: a) the purposes for the collection, use and disclosure of his personal data, on or before collecting the personal data; or b) any purpose for use or disclosure of personal data which has not been informed under sub-paragraph (a), before such use or disclosure of personal data for that purpose. This obligation to inform individuals of the purposes for which their personal data will be collected, used and disclosed is referred to in these Guidelines as the Notification Obligation. The Notification Obligation does not apply in the circumstances specified in section 20(3). That is, organisations are not required to inform individuals of the purposes for which their personal data will be collected, used or disclosed if: a) the individual is deemed to have consented to the collection, use or disclosure of his or her personal data under section 15 or 15A of the PDPA; or b) the organisation is collecting, using or disclosing the personal data without the consent of the individual concerned in accordance with section 17 of the PDPA (that is, in the	

		circumstances specified in the First and Second Schedules to the PDPA). It is important for an organisation to identify the purposes for which it is collecting, using or disclosing personal data by establishing the appropriate policies and procedures. These would enable the organisation to identify what personal data it needs to collect, use and disclose for its business purposes and to ensure that the personal data collected is consistent with the purposes identified. It would also minimise the risk of collecting, using or disclosing personal data in contravention of the Data Protection Provisions. The following paragraphs consider three important issues relating to the Notification Obligation: a) when an organisation must inform the individual of its purposes; b) the manner and form in which the organisation should inform the individual of its purposes; and c) the information and details to be included when an organisation states its purposes. When an organisation must inform the individual of its purposes Under section 20 (1), (4) and (5) of the PDPA, an organisation must inform the individual of the purposes for which his personal data will be collected, used or disclosed on or before such collection, use or disclosure (as the case may be). For example, this may take place when an individual is entering into a contract with an organisation under which the organisation requires certain personal data from the individual.	

		In other situations, an organisation may need to inform the individual before entering into a contract with the individual. For example, an insurance advisor may need to obtain certain personal data from an individual before the insurance company enters into a contract of insurance with the individual. Where an organisation needs to collect, use and/or disclose personal data on a periodic basis, it must inform the individual before the first collection of the data. The manner and form in which an organisation should inform the individual of its purposes The PDPA does not specify a specific manner or form in which an organisation is to inform an individual of the purposes for which it is collecting, using or disclosing the individual's personal data. An organisation should determine the best way of doing so such that the individual is provided with the required information to understand the purposes for which his personal data is collected, used or disclosed. Relevant factors affecting an organisation's determination of the appropriate manner and form of notification to an individual of its purposes may include the following: a) the circumstances and manner in which it will be collecting the personal data; b) the amount of personal data to be collected; c) the frequency at which the personal data will be collected; and d) the channel through which the notification is provided (e.g. face-to-face or through a telephone conversation).	

		It is generally good practice for an organisation to state its purposes in a written form (which may be electronic form or other form of documentary evidence) so that the individual is clear about its purposes and both parties will be able to refer to a clearly documented statement of the organisation's purposes in the event of any dispute. For example, organisations may state their purposes in the service agreement between the organisation and the individual or in a separate data protection notice provided to the individual. The latter may be appropriate in situations where an organisation needs to obtain personal data from an individual either before, or independently of, any agreement with the individual. Providing notification through a Data Protection Policy The PDPA requires organisations to develop and implement policies and procedures that are necessary for the organisation to meet its obligations under the PDPA. In addition, organisations are required to make information available on such policies and procedures. Organisations may wish to develop a Data Protection Policy (also referred to as a Privacy Policy) to set out its policies and procedures for complying with the PDPA27. An organisation may choose to notify individuals of the purposes for which it collects, uses and discloses personal data through its Data Protection Policy. The Data Protection Policy may be provided to individuals as required, in the form of a physical document, on the organisation's website or some other manner. Organisations which choose to	

		provide notification to individuals through a Data Protection Policy should note the following: a) Where the policy is not made available to an individual as a physical document, the organisation should provide the individual with an opportunity to view its Data Protection Policy before collecting the individual's personal data. For example, when an individual signs up for services at an organisation's retail shop, the retailer could provide the individual with an extract of the most relevant portions of the Data Protection Policy in a physical document. b) If an organisation's Data Protection Policy sets out its purposes in very general terms (and perhaps for a wide variety of services), it may need to provide a more specific description of its purposes to a particular individual who will be providing his personal data in a particular situation (such as when subscribing for a particular service), to provide clarity to the individual on how his personal data would be collected, used or disclosed. For the avoidance of doubt, organisations are not required to make available to individuals information related to the organisation's internal corporate governance matters (e.g. expense policies or corporate rules) unrelated to the organisation's data protection policies and practices as part of their Data Protection Policy, so long as the Accountability Obligation is met. Please refer to Chapter 21 on "The Accountability Obligation" for more information on the requirement for organisations to	

		develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA and to make information about those data protection policies and practices available. Example: Sarah signs up for a membership at a gym. The application form contains an extract of the most relevant portions of the Data Protection Policy in a physical document. For example, it states that Sarah's address details will be used for sending her a gym membership card and other communications related to her gym membership. The sales representative of the gym informs her that the full Data Protection Policy is available on the gym's website and provides her with relevant information to locate it. In this case, the gym has informed Sarah of the purposes for which her personal data will be collected, used or disclosed. Information to be included when stating purposes An organisation should state its purposes at an appropriate level of detail for the individual to determine the reasons and manner in which the organisation will be collecting, using or disclosing his personal data. As explained earlier in the section on "Purposes", an organisation need not specify every activity it will undertake in relation to collecting, using or disclosing personal data when notifying individuals of its purposes. This includes activities that are directly related to the collection, use or disclosure of personal data or activities that are integral to the proper functioning of the overall	

		business operations related to the purpose. For example, if an organisation wishes to obtain consent to collect or use personal data for the purpose of providing a service to an individual, the organisation does not need to seek consent for: (a) every activity it will undertake to provide that service; and (b) internal corporate governance processes such as allowing auditors to access personal data as part of an audit. In considering how specific to be when stating its purposes, organisations may have regard to the following: a) whether the purpose is stated clearly and concisely; b) whether the purpose is required for the provision of products or services (as distinct from optional purposes); c) if the personal data will be disclosed to other organisations, how the organisations should be made known to the individuals; d) whether stating the purpose to a greater degree of specificity would be a help or hindrance to the individual understanding the purpose(s) for which his personal data would be collected, used, or disclosed; and e) what degree of specificity would be appropriate in light of the organisation's business processes. Example: An electronics store sells products online through its website. It informs individuals purchasing products through its website of the purposes for which it will be collecting, using and disclosing personal data, including that the contact details provided by the customers will be disclosed to other companies in the electronics store's corporate group and outsourced	

		marketing company for the purposes of marketing the products of the various companies in its corporate group from time to time. In this case, the electronics store would be considered to have stated a sufficiently specific purpose. In another case, the electronics store informs individuals purchasing products through its website that the personal data provided may be used and disclosed for valid business purposes. In this case, the electronics store would not be considered to have stated a sufficiently specific purpose. Good practice considerations relating to the Notification Obligation Informing the individual of the purposes for which his personal data will be collected, used or disclosed is an important aspect of obtaining consent for the purposes of the Data Protection Provisions. Hence organisations should endeavour to ensure that their notifications are clear, easily comprehensible, provide appropriate information and are easily accessible. In considering how to notify individuals of their purposes, organisations should consider: a) Drafting notices that are easy to understand and appropriate to the intended audience, providing headings or clear indication of where the individuals should look to determine the purposes for which their personal data would be collected, used or disclosed and avoiding legalistic language or terminology that would confuse or mislead individuals reading it; b) Using a 'layered notice' where appropriate, by providing the most important (e.g. summary of purposes) or basic information	

		(e.g. contact details of the organisation's DPO) more prominently (e.g. on the first page of an agreement) and more detailed information elsewhere (e.g. on the organisation's website). A layered approach is useful when individuals do not want to read all the information at the point of transaction, or when the medium of transaction is not suitable for conveying detailed information (e.g. telephone conversation); c) Considering if some purposes may be of special concern or be unexpected to the individual given the context of the transaction, and whether those purposes should be highlighted in an appropriate manner; d) Selecting the most appropriate channel(s) to provide the notification (e.g. in writing through a form, on a website, or orally in person); and e) Developing processes to regularly review the effectiveness of and relevance of the notification policies and practices. Example: A supermarket surveys a group of shoppers on its premises to find out ways to improve customer experience. It collects personal data such as the names and contact details of the shoppers through a survey form which it hands to shoppers. The first line of each survey form clearly and legibly states that "Your personal data will be used by the supermarket and its appointed survey company for analysis of survey responses to find out ways to improve customer experience at our supermarket, or to contact survey respondents for follow-up queries on the survey responses for such analysis.". The	

		supermarket would be considered to have provided appropriate notification in this scenario. An estate agent places a guest book at the reception counter in a show flat. Individuals who visit the show flat are asked to provide their name, address and income information in the guest book. The receptionist greets every individual who enters the show flat and explains verbally that his personal data is collected for the real estate agency's market research and product planning purposes, and that it would not be used to contact individuals after they leave the show flat. The real estate agency would be considered to have provided appropriate notification in this case. Use and disclosure of personal data for a different purpose from which it was collected The Data Protection Provisions recognise that there will be circumstances in which an organisation would like to use or disclose an individual's personal data for purposes which it has not yet informed the individual of or for which it has not yet obtained the individual's consent. Where an organisation wishes to use or disclose personal data for purposes which it has not yet informed the individual or for which it has not yet obtained the individual's consent, organisations need to inform individuals of those purposes and obtain consent (the "Notification" and "Consent Obligation"). In determining if personal data can be used or disclosed for a particular purpose without obtaining fresh consent, an organisation should determine:	

		a) whether the purpose is within the scope of the purposes for which the individual concerned had originally been informed, for example, if it would fall within the organisation's servicing of the existing business relationship with the individual; b) whether consent can be deemed to have been given by the individual in respect of use or disclosure for that purpose in accordance with Section 15 or 15A of the PDPA; and c) whether the purpose falls within the exceptions from consent in the First and Second Schedules to the PDPA. If the purpose does not fall within sub-paragraphs (a) to (c) above, then the organisation must obtain the individual's fresh consent for use and disclosure for the new purpose. Example: Sarah currently has a membership with a spa. Her spa wants to use her personal data for the purposes of sending her greeting cards and the spa's annual newsletter in the post while her spa membership is still active. These purposes would fall within sub-paragraph (a) above, as part of the organisation's servicing of the existing business relationship with the individual, for which consent would have been previously obtained. Sarah's spa wants to send her information about an affiliate company's hair salon promotions. The spa would need to obtain Sarah's consent before sending information promoting new services that Sarah has not signed up for, as that is unlikely to fall within sub-paragraphs (a) to (c) above. The Accountability Obligation82 21.1 In data protection, the	

		concept of accountability refers to how an organisation discharges its responsibility for personal data in its possession or which it has control over83. This may include situations where the organisation can determine the purposes for which the personal data is collected, used or disclosed, or the manner and means by which the data is processed. This general concept of accountability is in Part 3 of the PDPA on "General Rules with Respect to Protection of and Accountability for Personal Data" and premised on section 11(2) within Part 3 of the PDPA, which states, "An organisation is responsible for personal data in its possession or under its control.". 21.2 Accountability under the PDPA requires organisations to undertake measures in order to ensure that they meet their obligations under the PDPA and, importantly, demonstrate that they can do so when required. Some of these measures are specifically required under the PDPA. For example, designating one or more individuals to be responsible for ensuring the organisation's compliance with the PDPA, developing and implementing policies and practices that are necessary for the organisation to meet its obligations under the PDPA ("data protection policies and practices"), and making information about their data protection policies and practices available. Other measures as described at paragraph 21.15 are not mandatory but are good practices to help organisations in meeting their obligations under the PDPA. Appointing a Data Protection Officer	

		21.3 Section 11(3) of the PDPA requires an organisation to designate one or more individuals to be responsible for ensuring that the organisation complies with the PDPA. This individual is typically referred to as a DPO. Section 11(4) further provides that an individual so designated by an organisation may delegate the responsibility conferred by that designation to another individual. Section 11(6) clarifies that the designation of an individual by an organisation under section 11(3) does not relieve the organisation of any of its obligations under the PDPA. That is, legal responsibility for complying with the PDPA remains with the organisation and is not transferred to the designated individual(s). On the whole, these provisions require organisations to designate the appropriate individuals, who may in turn delegate certain responsibilities to other officers, so that collectively, they co-operate to ensure that the organisation complies with the PDPA. 21.4 An organisation's DPO plays an essential role in how the organisation meets its obligations under the PDPA. The responsibilities of the DPO often include working with senior management and the organisation's business units to develop and implement appropriate data protection policies and practices for the organisation. In addition, the DPO would undertake a wide range of activities, which may include producing (or guiding the production of) a personal data inventory, conducting data protection impact assessments, monitoring and reporting data	

		protection risks, providing internal training on data protection compliance, engaging with stakeholders on data protection matters and generally acting as the primary internal expert on data protection. Depending on the organisation's needs, the DPO may also work with (or have additional responsibilities relating to) the organisation's data governance and cybersecurity functions. The DPO can also play a role in supporting an organisation's innovation.21.5 Individual(s) designated by an organisation under section 11(3) should be: (a) sufficiently skilled and knowledgeable; and (b) amply empowered, to discharge their duties as a DPO, although they need not be an employee of the organisation. Organisations should ensure that individuals appointed as a DPO are trained and certified84. The individual(s) should ideally be a member of the organisation's senior management team or have a direct reporting line to the senior management to ensure the effective development and implementation of the organisation's data protection policies and practices. As part of corporate governance, the commitment and involvement of senior management is key to ensure that there is accountability and oversight over the management of personal data in the organisation. 21.6 The DPO (or someone working with him) may also be the primary contact point for the organisation's data protection matters. Section 11(5) of the PDPA requires an organisation to make available the business contact information of at least one individual designated by the	

		organisation under section 11(3), while section 20(1)(c) and 20(5)(b) require an organisation to make available the business contact information of a person who is able to answer questions on behalf of the organisation relating to the collection, use or disclosure of personal data.85 These individuals and persons may be the same individual or the organisation may have different persons undertaking such roles. 21.7 The business contact information of the relevant person may be provided on BizFile+for companies that are registered with ACRA, or provided in a readily accessible part of the organisation's official website86 such that it can be easily found. It should be readily accessible from Singapore, operational during Singapore business hours and in the case of telephone numbers, be Singapore telephone numbers. This is especially important if the relevant person is not physically based in Singapore. This would facilitate the organisation's ability to respond promptly to any complaint or query on its data protection policies and practices. Developing and implementing data protection policies and practices 21.8 Section 12 of the PDPA sets out four additional key requirements which form part of the Accountability Obligation. 21.9 Firstly, an organisation is required to develop and implement data protection policies and practices to meet its obligations under the PDPA87. Policies can be internal or external facing; and practices can include establishing governance structures and designing processes to	

		operationalise policies. Organisations should develop policies and practices by taking into account matters such as the types and amount of personal data it collects, and the purposes for such collection88 . This also entails ensuring that policies and practices are easily accessible to the intended reader. Furthermore, the organisation should put in place monitoring mechanisms and process controls to ensure the effective implementation of these policies and practices. 21.10 Secondly, an organisation must develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA89. This is to ensure that the organisation can effectively address individuals' complaints and concerns with its data protection policies and practices and aid in its overall compliance efforts. 21.11 Thirdly, an organisation is required to provide staff training and communicate to its staff information about its policies and practices90. Such communication efforts could be incorporated in organisations' training and awareness programmes and should include any additional information which may be necessary for the organisation's staff to effectively implement its data protection policies and practices. An effective training and awareness programme builds a staff culture that is sensitive and alert to data protection issues and concerns. 21.12 Finally, an organisation is required to make information available on request concerning its data protection policies and practices and its complaint	

		process91. This is to ensure that individuals are able to find the necessary information and, if necessary, have the means of raising any concerns or complaints to the organisation directly. 21.13 In general, an organisation's personal data protection policies and practices set the tone for the organisation's treatment of personal data, and provide clarity on the direction and manner in which an organisation manages personal data protection risks. These should be developed to address and suit specific business or organisational needs. Please refer to the Commission's website for resources on demonstrating organisational accountability. Other provisions related to the Accountability Obligation 21.14 The Data Protection Provisions also provide for specific circumstances where organisations have to be answerable to individuals and the Commission, and be prepared to address these parties in an accountable manner. For example: a) individuals may request for access to their personal data in the possession or under the control of an organisation, which enables them to find out which of their personal data may be held by an organisation and how it has been used; b) organisations have to notify the Commission and/or affected individuals when a data breach is likely to result in significant harm or is of a significant scale; c) organisations have to conduct risk assessments to identify and mitigate adverse effects for certain uses	

		of personal data such as for legitimate interests; d) individuals may submit a complaint to the Commission and the Commission may review or investigate an organisation's conduct and compliance with the PDPA92; e) the Commission may, if satisfied that an organisation has contravened the Data Protection Provisions, give directions to the organisation to ensure compliance including (amongst others) imposing a financial penalty of up to $1 million (or in due course, up to $1 million or 10% of the organisation's annual turnover in Singapore, whichever is higher); and f) individuals who suffer loss or damage directly as a result of a contravention of Parts 4, 5, 6 or 6A of the PDPA by an organisation may commence civil proceedings against the organisation93. Other measures relating to accountability 21.15 Although not expressly provided for in the PDPA, organisations may wish to consider demonstrating organisational accountability through measures such as conducting Data Protection Impact Assessments ("DPIA") in appropriate circumstances, adopting a Data Protection by Design ("DPbD") approach, or implementing a Data Protection Management Programme ("DPMP"), to ensure that their handling of personal data is in compliance with the PDPA94. Although failing to undertake such measures is not itself a breach of the PDPA, it could, in certain circumstances, result in the organisation failing to meet other obligations under the PDPA. For example, an	

		organisation that does not conduct a DPIA may not fully recognise risks to the personal data it is handling within its IT infrastructure. This, in turn, may result in the organisation failing to implement reasonable security measures to protect such data and hence committing a breach of section 24 of the PDPA. Example: In its effort to comply with the PDPA and demonstrate accountability, Organisation ABC undertakes a proactive and comprehensive approach by developing a DPMP. The DPMP incorporates data protection policies to provide transparency in the manner ABC handles personal data, processes as well as roles and responsibilities of the people in the organisation. As part of its corporate risk management framework, ABC also has in place a process to conduct DPIAs to identify, assess and address personal data protection risks. Having implemented robust personal data protection policies and practices, ABC decides to certify its data protection policies and practices under the Data Protection Trustmark ("DPTM") Certification to enhance consumer trust and provide greater assurance for its stakeholders.	
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		

25	Advisory Guidelines on the Do Not Call Provisions	Obligation on third-party checkers Under section 43A(1), a "checker" is a person who checks the DNC Register for a sender and provides the sender information on whether a Singapore telephone number is listed in the relevant register ("the applicable information"). A checker does not include an individual who is an employee of the sender, or an employee or a contractor of the checker. Under section 43A(2), the checker must: a) Ensure that the applicable information provided to the sender is accurate in accordance with the results from the DNC Registry; and b) When communicating the applicable information to the sender, provide him with the date the checker received the results from the DNC Registry, and the validity period of the applicable information. Requirement to provide clear and accurate information identifying the sender20 ("identification information") The policy intent of this requirement is that a recipient of a specified message is able to, using the identification information included in the message, find out who sent or authorised the sending of the message. Use of website address as identification information Persons may choose to use their website address as identification information if the recipient can identify the sender using the information provided within the text of the website address itself, or within the contents of the landing page which the website address leads	

		to. Using other names as identification information The Commission recognises that in certain circumstances, persons who send specified messages may wish to identify themselves using a name other than their own which is more closely related to the goods or services offered ("related names") or if the related name would be more familiar to the recipient. Examples of such related names could be the names of a person's brands, retail outlets, buildings or property developments. Persons should not attempt to obscure or conceal their identity by using related names as identification information. In the following examples, "XYZ" is a related name of "ABC company". Generic pronouns generally not considered to identify the sender Identification information must be provided in the form of a name or alias that is able to identify the sender. The sender would not be considered to have provided identification information if that information is provided solely in the form of generic pronouns, e.g. "me" or "us", informal nicknames, or fictitious names. Requirement to provide clear and accurate information about how the recipient can readily contact the sender21 ("contact information") Section 44(b) requires that the contact information must enable the recipient to "readily contact" the sender. The PDPA does not define the terms "readily" or "contact". These terms would apply as they are commonly understood in relation to the scenario where a recipient of a specified message would like to	

		communicate with the sender directly, in writing or otherwise. The Commission would consider this requirement to be met so long as the contact information enables the recipient to directly contact the sender in a reasonably convenient manner. The most straightforward way to provide contact information would be to provide an operational Singapore telephone number which can receive incoming calls or text messages, or a valid email address which can receive incoming emails. Persons should note that short codes and "No-Reply" email addresses would not be considered contact information, as they do not allow the recipient to readily contact the sender. As good practice, any contact information provided should be readily accessible from Singapore and operational during Singapore business hours. In considering whether the contact information provided enables the recipient to readily contact the sender, the Commission will take into account the actual outcome when the contact information is used. Persons may choose to display the identification or contact information outside of the body of message. A typical example would be displaying the contact information in the "From" field, usually located directly above the body of the message. Physical address by itself does not allow the recipient to 'readily contact' the sender As explained above, section 44(b) requires that the contact information must enable the recipient to readily contact the sender. Solely providing the address of a physical location does not enable	

		the recipient to directly contact the sender without expending more time and effort to either make a trip to the location or write a letter and send it by post to the sender. Therefore, the Commission would not consider the provision of a physical address by itself to fulfil the requirement to provide contact information that enables the recipient to readily contact the sender Providing contact information on a website Persons who wish to direct recipients to access a website containing their contact information should ensure that the information is easily located on the website. The most straightforward manner of doing so would be to locate the information on the anding page of the relevant website address, or on the "Contact Us" (or equivalent) page. When considering if a person had provided contact information on a website, the Commission will consider the relevant website in totality, taking into account all relevant factors. Such factors include but are not limited to: the overall process the recipient has to go through to access the information, where it is located and how it is presented. Combining contact information with information on how to unsubscribe from distribution lists Persons who provide an unsubscribe facility within their messages may choose to combine that information with the contact information, so long as recipients can use that information to communicate with the sender directly on matters unrelated to unsubscribing from	

		the distribution list. Requirement to provide identification and contact information within the message Persons should note that the identification and contact information must be included within the specified message. The following examples illustrate when the information would not be considered to be included within the message.	
26	Advisory Guidelines on Application of PDPA to Election Activities	Notification Obligation 4.12 A political party or election candidate must notify15 the individual of the purposes for which it intends to collect, use or disclose his or her personal data on or before such collection, use or disclosure of the personal data. 5 DO NOT CALL PROVISIONS 5.1 The Do Not Call Provisions ("DNC Provisions") under the PDPA generally apply to marketing messages sent to a Singapore telephone number. 5.2 A message, the sole purpose of which is for election campaigning, would not be covered by the DNC Provisions, provided it does not offer to supply, offer, advertise or promote a good or service, or include any of the other purposes listed in the definition of a 'specified message' under the PDPA24. In addition, the Eighth Schedule of the PDPA provides for messages that will not be considered 'specified messages' for the purpose of the DNC Provisions. 5.3 If a political party or election candidate intends to send a specified message to a Singapore telephone number, the political party or election candidate must comply with the DNC Provisions. For more	

		information, please refer to the Advisory Guidelines on the DNC Provisions.	
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		
29	Advisory Guidelines for Management Corporations	3 Common activities that involve the collection, use or disclosure of personal data Dissemination of notices containing personal data Voter List 3.1 Under the BMSMA, MCSTs are required to display a list of the names of the persons who are entitled to vote as well as the addresses of lots owned by these persons on the estate's notice board20, at least 48 hours before the general meeting. Given that the BMSMA requires the names of persons entitled to vote as well as the lots in respect of which each of these persons is entitled to vote to be displayed on the estate's notice board, consent for the disclosure of such information for such purposes is not required under the PDPA. If MCSTs wish to display additional information other than those specified in the BMSMA, MCSTs are required to obtain consent from the relevant individuals before displaying and disclosing such other personal data, unless an exception applies21. MCSTs must also ensure that the disclosure of such other personal data would not be considered excessive or	

		inappropriate. As good practice, MCSTs should take care to display the list of voters for a reasonable duration and not display it for a longer period than necessary (e.g. removing the list of eligible voters soon after the conclusion of the general meeting). 3.2 Example: Voter List In the lead up to an annual general meeting to vote for the MCST executive committee of estate DEF, the MCST displayed a list of eligible voters on estate DEF's notice board. The list included the names of voters and their email addresses. As the names of voters are required to be displayed on the estate's notice board pursuant to the BMSMA, consent for the disclosure of voters' names is not required. However, consent is needed from residents to disclose their email addresses for this purpose.	
30	Advisory Guidelines for the Education Sector	2 The Consent, Purpose Limitation and Notification Obligations 2.1 The Commission understands that an education institution5 may collect, use or disclose a student's personal data for purposes such as to provide the student with education services, to evaluate the student's suitability for a course, or to administer bursaries, scholarships and relevant financial assistance schemes to eligible students. The Commission recognises that the purposes for the collection, use or disclosure of personal data may differ across education institutions. Organisations should, therefore, notify and specify purposes at an appropriate level of detail that will allow an individual to	

		determine the reasons that the education institution is collecting, using or disclosing his/her personal data. Education institutions are encouraged to consider factors such as the specific facts of the case, business and operational needs, and to refer to the Advisory Guidelines on Key Concepts in the PDPA ("Key Concepts Guidelines") for more information on providing notification and on stating purposes. 2.2 The Data Protection Provisions in Parts III to VI of the PDPA set out the obligations that organisations are required to comply with if they undertake activities relating to the collection, use or disclosure of personal data6. Among other things, organisations are required to obtain valid consent from the individual for a limited purpose that has been notified to the individual for the collection, use and disclosure of personal data of the individual, unless exceptions apply7. Considerations in obtaining consent 2.3 The PDPC does not prescribe the manner in which consent should be obtained by an organisation under the Data Protection Provisions. An education institution may decide on the most suitable way to obtain consent in accordance with the PDPA, and may refer to the Key Concepts Guidelines for more information on considerations and good practices when obtaining consent from an individual. 2.4 In relation to the Consent Obligation, prior to collecting, using or disclosing personal data about an individual, an education institution should consider:	

		a) Whether the individual (or a person who has the legal authority to validly8 act on behalf of the individual) had been notified of the purposes for the collection, use or disclosure of his personal data and had given consent to such collection, use or disclosure; b) If consent had not actually been given, whether consent can be deemed to have been given by the individual (or a person who has the legal authority to validly act on behalf of the individual) for the collection, use or disclosure of his personal data for the purpose; and c) Whether the collection, use or disclosure without the consent of the individual is required or authorised under the PDPA or any other written law, and assess whether the circumstances fall within any of the exceptions from the Consent Obligation in the Second, Third or Fourth Schedules to the PDPA. 2.5 The Commission is aware that, depending on the nature of their education product or service and demographics of their students, some education institutions may collect, use and disclose the personal data of minors and would accordingly have to obtain consent under the PDPA. Please refer to the Advisory Guidelines on Selected Topics ("Selected Topics Guidelines") for more information relating to considerations when obtaining consent from minors. 2.6 Example: Disclosure of personal data for school buddy orientation programmes Ella is a student currently pursuing a course at School ABC. School ABC intends to pair Ella with an incoming international student under an orientation	

		programme which matches existing students with incoming students and their families, and wishes to disclose Ella's personal data (such as name, age, interests and contact details) to Ella's potential buddy. School ABC should obtain Ella's consent before disclosing her personal data for such a purpose. For avoidance of doubt, School ABC may notify Ella and seek her consent using various avenues and platforms. For example, when collecting Ella's personal data during the enrolment process, School ABC could include a notification in the enrolment forms that the personal data of enrolled students may be used and disclosed to third parties for school-related activities or programmes, such as "buddy systems" for new students, and consent can be obtained via the same forms. 2.7 Example: Disclosure of personal data of minors for school field trip A pre-school, ABC, is organising a field trip to the zoo for its students. Pre-school ABC needs to disclose the participants' personal data to the zoo for the purpose of arranging the field trip programme. Generally, Pre-school ABC should obtain consent from the parent or other legal guardians of each student, as a pre-school student would not have legal capacity to give consent. 2.8 Example: Disclosure of personal data to another parent Sue and John are friends whose daughters attend School ABC. One day, Sue is required to attend a meeting at the last minute and she is unable to pick up her daughter, Vera, at school.	

		Sue calls John to pick Vera up on her behalf and send her home. John arrives at the school, informs School ABC that he is picking up Vera as well, and asks School ABC for Vera's home address. In this situation, in the absence of other forms of verification, School ABC should ensure that consent is obtained for the disclosure of Vera's personal data (e.g. home address) for such a purpose. For example, School ABC could make a call to Sue to confirm her agreement to disclose Vera's address to John. 2.9 Example: Disclosure of students' personal data for marketing purposesSchool ABC would like to publish the names and photographs of its top students and renowned alumni in its marketing collateral. As the names and photographs of these individuals are considered personal data relating to them, School ABC should obtain consent from these individuals to use and disclose their personal data for the marketing purposes. 2.10 Example: Disclosure of starting salaries of alumni School ABC conducts a survey on the employability of its alumni. The survey is conducted primarily via email, and personal data of School ABC's alumni are obtained through the survey such as their full names, student registration numbers, field(s) of study, the sector they are currently employed in, and their starting salaries. In the survey, School ABC states that the purpose of the survey is for School ABC to manage career services for its existing students. Organisation DEF, targeting high net worth individuals for their investment services, asks School	

		ABC for a list of alumni who earn more than $X a month, their contact details and salary range in order to contact them to offer investment services. As this would be a different purpose from which the personal data was collected for, School ABC is required to obtain fresh consent from its alumni to disclose their personal data to Organisation DEF for their purposes. Organisation GHI produces a report each year on the starting salaries of fresh graduates in each industry sector and asks School ABC for the salary details of its recently-graduated alumni. As this would be a different purpose for which the personal data was collected, School ABC is required to obtain fresh consent from the alumni to disclose their personal data to Organisation GHI for their purposes. School ABC may also consider whether the data required could be anonymised, for example by removing personal identifiers, and aggregating data points so that unique individuals cannot be identified from the data. School ABC should also consider factors which may pose a challenge in keeping data anonymised. Please refer to the chapter in the Selected Topics Guidelines relating to Anonymisation for more information. When consent may be deemed 2.11 An individual is deemed to consent to the collection, use and disclosure of his personal data for a purpose if the individual voluntarily provides the personal data to the organisation for that purpose and it is reasonable that the individual would do so. 2.12 In a situation where an individual gives, or is deemed to have given, consent to the	

		disclosure of personal data about the individual by one organisation to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation. 2.13 Although organisations may rely on deemed consent instead of obtaining actual consent from the individual, it is good practice for an organisation to review its business processes to determine the situations where it should obtain actual consent instead of relying on deemed consent. 2.14 When it is unclear whether consent may be deemed, organisations should obtain consent from the individual to collect, use or disclose his personal data (as the case may be) for the relevant purposes in order to avoid any dispute over whether consent was given. 2.15 The following examples illustrate situations where the Consent Obligation applies. Please also refer to the Key Concepts Guidelines for more information on the Consent Obligation. 2.16 The following examples illustrate situations where consent may be deemed to have been given. 2.17 Example: Personal data collected for security purposes As part of its security measures, School ABC requires visitors to the school to sign up for a visitor pass at the security guard house. Visitors are requested to provide their full name, NRIC/passport number, contact number and state the purpose for their visit. School ABC is required to comply with the Data Protection	

		Provisions when collecting, using and disclosing personal data. An individual is deemed to have given consent to School ABC's collection of his/her personal data for security purposes if the individual provides his/her personal data voluntarily for the purpose. As good practice, to ensure that the individual is aware of the purpose, School ABC may place a prominent sign at the reception desk indicating that visitors' details will be collected for security purposes. 2.18 Example: Personal data provided as administrative contact Jack signs up his son, Mack, for a one-day swimming camp organised by School ABC. In the registration form, Jack writes down his own name and mobile phone number for School ABC to contact him for the purpose of his son's participation in the camp. As Jack had voluntarily provided his name and contact details, he is deemed to have consented to School ABC's collection, use or disclosure of his personal data for such purposes. Should School ABC wish to use or disclose Jack's personal data for another purpose (for which consent had not been given or deemed to have been given), the school will need to separately obtain consent from Jack for that other purpose, unless an exception applies. 5 Organisations and Data Intermediaries 5.1 In some situations, education institutions may engage data intermediaries to process personal data. The PDPA provides that a data intermediary12 that processes personal data on behalf of and	

		for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will only be subject to the Protection Obligation and Retention Limitation Obligation and not any of the other Data Protection Provisions. 5.2 A data intermediary remains responsible for complying with all Data Protection Provisions in respect of other activities that do not constitute processing of personal data on behalf of and for the purposes of another organisation that is pursuant to a contract evidenced or made in writing. 5.3 In any case, under section 4(3) of the PDPA, the organisation that engages the data intermediary would still have the same obligations under the PDPA in respect of personal data processed on its behalf as if the personal data were processed by the organisation itself. 5.4 Please refer to the Key Concepts Guidelines which provide further elaboration on when an organisation is considered a data intermediary and the obligations applicable to data intermediaries under the PDPA. 5.5 Example: Provision of transport services School ABC has a written contract with an external Vendor JKL for the provision of transport services to School ABC's students. Among other things, the contract between School ABC and Vendor JKL specifies that Vendor JKL will use personal data of School ABC's students provided by School ABC for the sole purpose of providing transport services on behalf of ABC to these students.	

		Tina is a student currently pursuing a course with ABC. Tina wishes to sign up for transport services provided by School ABC through Vendor JKL. Tina provides her personal data by completing the form prepared by School ABC, and ticks the box on the form to give School ABC consent to disclose her personal data to the Vendor JKL for the purpose of arranging the transport services. Vendor JKL will be considered a data intermediary processing Tina's personal data on behalf of and for the purposes of School ABC pursuant to a written contract in relation to the provision of transport services to Tina. In this instance, Vendor JKL will be subject only to the Protection Obligation and the Retention Limitation Obligation, while School ABC will have the same obligations under the PDPA in respect of Tina's personal data processed on its behalf by Vendor JKL, as if the personal data were processed by School ABC itself. 5.6 Example: Engaging a consultancy firm to conduct a survey School ABC has engaged the services of consultancy Firm DEF via a contractual agreement to conduct an email survey among its upcoming cohort of graduates. The purpose of the survey is to study student perceptions on job placement quality, and quality of training. School ABC will use the survey findings to refine its existing policies on job placement and training. According to the terms of the agreement with School ABC, School ABC will provide Firm DEF with a list of graduate	

		students containing their full names, student matriculation numbers, and field(s) of study. Firm DEF will categorise the graduates according to their fields of study and then contact them by email to conduct the survey. Following the completion of the email survey, Firm DEF is required to return the list containing the graduate students' personal data and all survey results to School ABC. In this case, Firm DEF will be considered a data intermediary of School ABC when processing students' personal data for the purpose of the email survey. Firm DEF will be subject only to the Protection Obligation and the Retention Limitation Obligation in relation to such processing, while School ABC will have the same obligations under the PDPA in respect of personal data processed on its behalf by Firm DEF, as if the personal data were processed by School ABC itself. 5.7 There are several obligations within the Data Protection Provisions which require organisations to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. Organisations are required to make the information about their data protection policies available. For more information, please refer to the Key Concepts Guidelines and the Selected Topics Guidelines. 6 Rights and obligations, etc under other laws 6.1 Section 4(6) of the PDPA states that unless otherwise provided in the PDPA, nothing in Parts III to VI of the PDPA shall affect any authority, right, privilege or immunity conferred,	

		or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening the PDPA, and the provisions of other written law shall prevail to the extent that any provision of Parts III to VI is inconsistent with the provisions of that other written law. 6.2 Section 13(b) of the PDPA provides that an organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual without the consent of the individual unless the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under the PDPA or any other written law. 6.3 There are several provisions under the Private Education Act and Regulations that empower the CPE to obtain information (including personal data) from registered PEIs. These provisions include, but are not limited to, the following: a) Section 57 of the Private Education Act provides that an inspector of the CPE may during an inspection of a registered PEI require any person to, amongst others, furnish any information which is within the power of the person to furnish relating to such matters as the inspector may specify. b) Section 62 of the Private Education Act provides that the CPE may issue a requisition to any person to furnish such particulars or supply such information relating to any matter to which the Act applies as may be specified in the requisition. c) Regulation 22 of the Private	

		Education Regulations provides that the managers of a registered PEI shall prepare and submit to the CPE, by the 31st day of December of each year, an annual report on the activities and affairs of the PEI in that year. This includes, but is not limited to, personal data on the managers, academic/examination board members, teachers as well as students of the registered PEI. 6.4 Section 19 of the PDPA provides that notwithstanding the other provisions of Part IV of the PDPA, an organisation may use personal data collected before the appointed day for the purposes for which the personal data was collected, unless consent for such use is withdrawn or the individual has indicated to the organisation that he does not consent to the use of the personal data. Such 'use' could include disclosure that is necessarily part of the organisation's use of such personal data. For avoidance of doubt, the Do Not Call Provisions will apply to the sending of specified messages to Singapore telephone numbers, even if the Singapore telephone numbers are collected before the appointed day. PART III: APPLICATION OF THE DO NOT CALL PROVISIONS TO SCENARIOS FACED IN THE EDUCATION SECTOR The following examples outline the application of the Do Not Call Provisions and the Personal Data Protection (Exemption from Section 43) Order (S.817/2013) ("Exemption Order"). They address particular aspects of the PDPA, and are not meant to exhaustively address every obligation in the PDPA that would	

		apply in that scenario. In particular, they do not illustrate the application of the Data Protection Provisions, which were addressed earlier in these Guidelines. 7 The Do Not Call Provisions 7.1 Messages with a purpose to offer to supply, advertise or promote goods or services, land or an interest in land, or a business or investment opportunity, or a supplier of such goods, services, land or opportunity are specified messages and the Do Not Call Provisions will apply to such messages. Messages which do not have any of the purposes listed above will not be considered specified messages. The Eighth Schedule to the PDPA sets out exclusions from the meaning of "specified message" that relate to, among others, any "business-to-business" marketing message, any message sent by a public agency under, or to promote, any programme carried out by any public agency, which is not for commercial purpose, any message the sole purpose of which is to conduct market research or market survey, and other types of information specified in the Eighth Schedule. 7.2 The Do Not Call Provisions apply to a specified message addressed to a Singapore telephone number if the sender of the specified message is present in Singapore when the specified message is sent or the recipient of the specified message is present in Singapore when the specified message is accessed. 7.3 One significant obligation under the Do Not Call Provisions is that the organisation sending the specified message will have	

		to check the Do Not Call Registers as described above, unless: a) the user or subscriber of the Singapore telephone number has given clear and unambiguous consent in written or other accessible form to the sending of the specified message to that number; or b) the organisation is exempted from complying with its obligation under the Exemption Order. 7.4 Under the Exemption Order, a sender that is sending a specified fax message or a specified text message to a Singapore telephone number related to the subject of an ongoing relationship between the sender and a recipient is exempted from the requirement to check the relevant Do Not Call Registers, if certain conditions are met. An "ongoing relationship" under the Exemption Order means a relationship which is on an ongoing basis, between a sender and a subscriber or user of a Singapore telephone number, arising from the carrying on or conduct of a business or activity (commercial or otherwise) by the sender. The Exemption Order does not apply to voice calls and a sender is still required to check the Do Not Call Register before making any telemarketing calls to promote related products or services. The Advisory Guidelines on the Do Not Call Provisions provide further elaboration. 7.5 In determining what constitutes an ongoing relationship, the Commission considers one-off interactions or transactions in themselves to be insufficient to be an ongoing relationship. For example, the	

		fact that an individual previously contacted the education institution to enquire about upcoming courses or programmes once, or attended an open house organised by the education institution once, by themselves, would be insufficient to establish an ongoing relationship between the individual and the sender. 7.6 Examples: Whether messages are specified messages13 School ABC is conducting an annual walkathon. (a) School ABC sends an SMS inviting students to attend the annual walkathon. To the extent that the walkathon does not offer to supply a good or service or have any of the other purposes listed in the definition of a specified message, School ABC would not be sending a specified message, therefore the Do Not Call Provisions would not apply. (b) In conjunction with "Healthy Week", School ABC calls to inform students about an upcoming seminar by a shoe retailer on choosing the right shoes for the walkathon. As the seminar involves promoting a supplier, School ABC is likely to be sending a specified message and the Do Not Call Provisions will apply. (c) School ABC calls all parents of students to be chaperones at the walkathon. Such messages will not be considered "specified messages" under the PDPA to the extent that they do not involve marketing of any good or service. Hence, the Do Not Call Provisions do not apply.(d) School ABC sends an SMS to thank all parents who volunteered in the	

		walkathon. School ABC is not sending a specified message and the Do Not Call Provisions do not apply. 7.7 In the upcoming school term, School ABC will be organising a school trip to Country XYZ as part of its efforts to enhance students' understanding of history and architecture. School ABC sends an SMS to students announcing the school trip, and possible travel insurance packages offered by various companies available to interested students. In this case, School ABC is considered to be sending a specified message as the SMS was also promoting travel insurance packages from different vendors to students. Hence, the Do Not Call Provisions will apply. 7.8 School DEF sends an SMS to students providing them administrative details of an upcoming examination, such as date, timing, venue and instructions for candidates to bring along their student matriculation card for verification purposes. School DEF is not sending a specified message, and the Do Not Call Provisions do not apply. 7.9 School ABC calls Albert to remind him of the deadline to settle his tuition fees. In this scenario, School ABC is not sending a specified message, and the Do Not Call Provisions do not apply. 7.10 School ABC sends an SMS to students announcing cancellation of outdoor classes due to inclement weather. School ABC is not sending a specified message, and the Do Not Call Provisions do not apply. 7.11 The following examples illustrate the application of the	

		Exemption Order. 7.12 Examples: Application of the Exemption Order School ABC will be introducing new language courses over the next year. (a) Jim previously enquired with School ABC on another course, and had no further interaction with School ABC thereafter. In this case, School ABC cannot rely on the Exemption Order to send a text or fax message marketing its new programmes to Jim as his enquiry was considered a one-off interaction. (b) Tracy, a former student of School ABC, has joined School ABC's alumni network, which receives regular email updates from School ABC on schoolrelated news including new courses and events open to alumni. School ABC may rely on the Exemption Order to send Tracy text or fax messages containing information about its new language courses. (c) Jason enrols his daughter, Jasmine, in a language course conducted by School ABC. In the enrolment form, Jason provides his name and Singapore telephone number as "parent contact information", which School ABC requires for the purposes of sending administrative updates about the course. In this case, the fact that Jason enrolled his daughter and provided his contact information, on its own, does not give rise to an ongoing relationship between him and School ABC. The on-going relationship is generally established between School ABC and Jasmine. School ABC should thus obtain clear and unambiguous consent, evidenced in written or any other form, from Jason if it wishes to send specified messages (e.g., such as	

		promoting the new language courses) to Jason's telephone number. If School ABC wishes to rely on any ongoing relationship to send specified messages under the Exemption Order to Jason, School ABC would need to consider if there are relevant factors that establish an ongoing relationship between itself and Jason.	
31	Advisory Guidelines for the Social Service Sector	3 The Consent, Purpose Limitation and Notification Obligations 3.1 The Commission understands that SSAs may collect, use or disclose a client's personal data including full name, NRIC number, contact details, financial and family situation, medical history, etc. for purposes such as evaluating the client's suitability for social services or administering social services to the clients. 3.2 The PDPA requires organisations to, among other things, notify an individual of the purposes for the collection, use and disclosure of his personal data2 and obtain his consent, unless any relevant exception to consent3 applies. Moreover, organisations shall only collect, use and disclose personal data that are relevant for the purposes, and for purposes that a reasonable person would consider appropriate in the circumstances. 3.3 Section 16 of the PDPA provides that individuals may at any time withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use or disclosure of their personal data for any	

		purpose by an organisation. Please refer to the Advisory Guidelines on Key Concepts in the PDPA (Chapter 12) for the requirements that must be complied with by either the individual or the organisation in relation to the withdrawal of consent. However, the organisation can continue to use and disclose personal data in their possession if allowed under other provisions. 3.4 The Commission is aware that, depending on the nature of their services and demographics of the client or beneficiary, some SSAs may collect, use or disclose the personal data of minors and would accordingly have to obtain consent under the PDPA. Please refer to the Advisory Guidelines on Selected Topics ("Selected Topics Guidelines") on "data activities relating to minors" for more information relating to persons who may exercise rights or powers under the PDPA, and considerations when obtaining consent from minors. 3.5 The following will highlight how consent may apply in common social service scenarios, how deemed consent applies as well as the exceptions to consent. 3.6 Examples: Using personal data SSA ABC arranges with Company XYZ such that the purpose and amount needed for donations to SSA ABC are listed on Company XYZ's public website. Company XYZ has a database of regular donors to whom it sends emails to solicit donations on a periodic basis.	

		The donors could choose to donate to SSA ABC by referring to the instructions on Company XYZ's website and provide their financial information to Company XYZ for processing of the transaction. Before proceeding, donors will indicate their consent to disclosing their personal data to SSA ABC when they donate through Company XYZ for purposes such as issuing tax deductible receipts to their email address. Treatment In processing the financial transaction from donors on its website, Company XYZ is considered to have collected, used and disclosed personal data. By receiving personal data of donors from Company XYZ, SSA ABC is considered to have collected and subsequently used the personal data. Accordingly, Company XYZ and SSA ABC will have to comply with the PDPA in respect of such collection, use and disclosure. 3.7 SSA DEF engages Company GHI for online on its upcoming programmes and events as sponsored social media posts. No individuals' personal data is given to Company GHI for generating the social media posts. The posts appear in the social media feed of users in a random manner. Treatment In this case, neither SSA DEF nor Company GHI would be considered to have collected or used the personal data of the users. Hence, both SSA DEF and Company GHI would not be subject to the Data Protection Provisions for this set of activities.	

		3.8 Example: Clients voluntarily giving their personal data for welfare services Seniors' activity centre ABC gives out free food items to senior citizens by leaving them at the door of the activity centre for self-collection by the senior citizens. There is a notice pasted at the door of the activity centre indicating that the seniors can leave their contact details if they are interested to be contacted for seniors' programmes, free or subsidized healthcare or financial support. To ensure that the personal data of the interested seniors are not shown to the public, interested seniors will fill in their names and contact details in a blank form placed at the door of the activity centre. They will drop the completed form inside a metal box that can only be accessed when the appropriate personnel from Seniors' activity centre ABC uses a key to open the lock on the box. On the form, there is a question clearly asking the seniors' consent for collection, use and disclosure of their personal data for the specific purpose and a checkbox beside the question for seniors to tick. Treatment If the senior citizen were to fill in their names and contact details in the blank form and indicated at the checkbox that they consent to the collection, use and disclosure of their personal data for the specified purpose, Seniors' activity centre ABC has obtained express consent from the interested seniors.	

		The consent is obtained in writing and provides the clearest indication that the individual has consented to the notified purposes of the collection, use or disclosure of their personal data. Seniors' activity centre ABC must ensure that the words on the notice and on the form are clear and noticeable, so that there is a higher certainty that the seniors would read and understand the purpose of the collection, use and disclosure of their personal data. By taking measures to ensure that the personal data left by interested seniors are not accessible to the public (e.g. using a metal box that can only be opened by authorised persons), Seniors' activity centre ABC has also complied with the Protection Obligation of the PDPA. 3.9 Example: Collection, use, and disclosure of personal data for client surveys SSA ABC intends to conduct a survey on the impact of its services on individual clients, which involves the collection and use of personal data (including clients' full names, contact details and income levels). SSA ABC intends to publish the results of the survey in a manner that identifies the individual clients4 in their annual report and on their website. Treatment SSA ABC must obtain consent from the individual clients to collect, use and disclose their personal data before conducting the survey, unless an exception applies.	

		If SSA ABC intends to use or disclose personal data that had previously been collected for other purposes for this survey, SSA ABC may wish to consider whether the exception for use or disclosure of personal data without consent for research in Division 35 of Part 2 of the Second Schedule or Division 26 of Part 3 of the Second Schedule respectively would apply. 3.10 Example: Disclosure of clients' personal data to a third party SSA ZYX receives an email request from a neighbourhood grassroots club for a list of SSA ZYX's needy clients and their addresses in order for the grassroots club to deliver some food rations to these clients. Treatment The Data Protection Provisions will generally apply to SSA ZYX's disclosure of its clients' personal data to the grassroots club. Among other things, consent would be required for such disclosure unless an exception applies, such as when the disclosure is necessary for any purpose which is clearly in the interests of the individual, if consent for its disclosure cannot be obtained in a timely way. Please refer to Chapter 12 of the Key Concepts Guidelines on the "Consent Obligation" for more information. Deemed consent 3.11 Deemed consent by conduct: In situations where an individual (without actually giving consent) voluntarily provides his personal data to an organisation for an appropriate purpose, and it is	

		reasonable that he would voluntarily provide the data, the individual's consent to the collection, use or disclosure of personal data is deemed to have been given by the individual's act of providing his personal data. 3.12 Example: Consent for photo-taking at a private function for clients SSA GHI hosts a private dinner function for families and engages a volunteer photographer to take photographs of attendees for its newsletter. SSA GHI does not explicitly ask the families for consent to take their photographs for the newsletter. However, in this context, consent is deemed to have been given when the individual voluntarily permits a photograph or video recording to be taken of him for SSA GHI's intended purpose, and it is reasonable that he would do so (e.g. the individual voluntarily stands in the frame of the photographer's camera without objection). The measures that SSA GHI may take to better ensure that the attendees are aware of the purpose for which their photographs are collected, used and disclosed, could include: a) Clearly stating in its invitation to families that photographs of attendees will be taken at the function for publication in its newsletter; and b) Putting up an obvious notice at the reception or entrance of the function room to inform attendees that photographs will be taken at the event for publication in its newsletter. After seeing the notice at the	

		reception, Mary informed the staff manning the reception that she does not want her photograph to be taken for publication in the newsletter. To facilitate Mary's refusal for her photograph to be taken, the reception staff gives her a lanyard of a different colour from the rest of the participants. This is so that the volunteer photographer can easily identify Mary, to avoid taking her photograph and publishing her photograph in SSA GHI's newsletter. Barry, who was initially deemed to have consented to his photograph being taken during the private function and published in SSA GHI's newsletter, subsequently withdraws his consent after the photograph has been published. SSA GHI is required under the PDPA to cease further publication of the photograph, unless such disclosure without Barry's consent is required or authorised under the PDPA or other written law, for example, if the photograph is already publicly available, or SSA GHI is able to effect the withdrawal of consent (e.g. by masking the image of the individual) before publishing or continuing to publish the photograph. 3.13 Deemed consent by contractual necessity: Pursuant to Section 15(3), if an individual gives, or is deemed to have given, consent to the collection, use or disclosure of his personal data to one organisation ("A") for the purpose of a contractual transaction, the consent may cover sharing of	

		his personal data by A with other organisations (and onward sharing by downstream organisations, as the case may be) so long as it is reasonably necessary for A to provide the personal data to the other organisations (likewise, for onward sharing by downstream organisations) to perform or conclude A's contractual obligations. 3.14 2.15 Example: Disclosing donors' data to downstream organisations involved in fulfilling transaction Mary donates $300 to SSA ABC which provides treatment and care to cancer patients. She provides her personal data (i.e. NRIC number, residential address, bank account details) through an online donation form on SSA ABC's website. The form clearly states that the purpose of collection, use and disclosure of donors' personal data is for SSA ABC to process the donation (e.g. through GIRO deduction from the bank) and for tax relief purposes. Treatment As Mary had consented to the collection, use and disclosure of her personal data for the notified purposes, deemed consent by contractual necessity would apply to all other parties involved in the GIRO and tax relief processing chain who collect, use or disclose Mary's personal data, where the collection, use or disclosure is reasonably necessary to fulfil the transaction between Mary and SSA ABC. The parties include, for example, Mary's bank, SSA ABC's bank, the online payment	

		gateway in which payment for the transaction is processed, the banks' processors and the tax authority. 3.15 Example: Disclosure of personal data to medical escorts for caregiving SSA DEF offers caregiving services to patients that need help to move around or have no caregiver to accompany them for their regular medical check-ups at the hospitals or clinics. In the provision of such caregiving services, SSA DEF engages medical escorts who accompany the patients to and from their homes and the hospitals or clinics for their medical check-ups, help to note down the doctor's prescriptions and help to schedule the next appointment. SSA DEF provides the patients' name, medical conditions and home addresses to the medical escorts for the purpose of fulfilling these caregiving services. In this case, as it is reasonably necessary for SSA DEF to provide the medical escorts with the personal data of patients for the medical escorts to fulfil the caregiving services for the patients, deemed consent by contractual necessity applies. 3.16 Deemed consent by notification: Section 15A provides that if an individual does not take any action to opt out of the collection, use or disclosure of his personal data for a purpose that he has been notified of, the individual is deemed to consent to the collection, use or disclosure of personal data by the organisation even for secondary use purposes that are different	

		from the primary purposes for which it had originally collected the personal data for7. 3.17 Nonetheless, the individual must have been notified that their personal data would be used for such secondary use purposes. The organisation must meet stipulated conditions by conducting an assessment to identify any adverse impact on the individuals arising from the proposed collection, use or disclosure of his personal data, and implement mitigating measures in relation to the adverse impacts identified. Please refer to the Advisory Guidelines on Key Concepts in the PDPA (Chapter 12) for more information on the stipulated conditions. 3.18 Example: Use of clients' personal data for publicity purposes Various medical institutions refer individuals to SSA ABC for the use of SSA ABC's facilities and services. SSA ABC accepts these individuals as its clients and receives their personal data from the medical institutions for the purpose of facilitating their use of its facilities and services. At the end of each year, SSA ABC engages in publicity to draw attention to its programmes and services, and it wants to use and disclose these clients' names in the publicity materials for that purpose. SSA ABC conducts an assessment to identify any adverse effect and determines that there are no likely adverse effects to the clients in using and disclosing their name	

		for this new purpose. It also assesses that emailing its clients on the intended sharing of their personal data for the stated purpose is an appropriate and effective method of notification, as it regularly sends such emails to them on its latest programmes. It also assesses that 10 days is a reasonable period for the clients to opt out. Treatment SSA ABC sends emails to its clients, notifying them of the intended use and disclosure of their name for the purpose and provides a contact number for any queries on the intended use and disclosure. In the email, SSA ABC stipulates that those who wish to opt out should reply to the email within 10 days from the date of the email, stating that they want to opt out. Clients who do not opt out within the 10-day opt-out period are deemed to have consented to the disclosure of their personal data for the purpose. Nonetheless, SSA ABC must allow and facilitate any withdrawal of consent after the 10-day opt-out period. 3.19 Example: Publishing photographs taken at a private event on social media SSA DEF will be conducting a private 1-day retreat for its clients, which include children below the age of 13, and its employees. It wishes to take photographs of the attendees and publish some of the photographs on its social media accounts to generate publicity about its programmes. SSA DEF conducts an	

		assessment to identify any adverse effect and determines that there are no likely adverse effects to the attendees in collecting, using and disclosing their personal data for this purpose. It also assesses that clearly stating in its email invitation to clients or their parents/guardians (for clients below the age of 13) and email notification to employees that photographs of attendees will be taken at the event for publication on its social media accounts is an appropriate and effective method of notification. SSA DEF also assesses that 14 days is a reasonable period to opt out. Treatment In its email invitations and notifications to clients and employees respectively, SSA DEF notifies them of the intended collection, use, and disclosure of their personal data for the purpose and provides a contact number for any queries. In the email, SSA DEF stipulates that those who wish to opt out of having their photographs taken at the event should reply to the email within 14 days from the date of the email, stating that they want to opt out. Clients and employees who do not opt out within the 14-day opt-out period are deemed to have consented to the collection, use and disclosure of their personal data for the purpose. Nonetheless, SSA DEF must allow and facilitate any withdrawal of consent after the 14-day opt-out period.8 11 Rights and obligations, etc	

		under other laws 11.1 Section 4(6) of the PDPA states that unless otherwise provided in the PDPA, nothing in Parts 3 to 6 of the PDPA shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening the PDPA, and the provisions of other written law shall prevail to the extent that any provision of Parts 3 to 6 is inconsistent with the provisions of that other written law. 11.2 Similarly, section 13(b) of the PDPA provides that an organisation shall not, on or after the appointed day (i.e., 2 July 2014), collect, use or disclose personal data about an individual without the consent of the individual unless the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under the PDPA or any other written law. 11.3 Section 19 of the PDPA provides that notwithstanding the other provisions of Part 4 of the PDPA, an organisation may use personal data collected before the appointed day (i.e., 2 July 2014) for the purposes for which the personal data was collected, unless consent for such use is withdrawn or the individual has indicated to the organisation that he does not consent to the use of the personal data. Such 'use' could include disclosure that is necessarily part of the organisation's use of such personal data. For avoidance of doubt, the Do Not Call Provisions	

		will apply to the sending of specified messages to Singapore telephone numbers, even if the Singapore telephone numbers are collected before the appointed day. PART III: APPLICATION OF THE DO NOT CALL PROVISIONS TO THE SOCIAL SERVICE SECTOR The following sections and examples set out the application of the Do Not Call Provisions to scenarios faced in the social service sector. They are not meant to exhaustively address every obligation in the PDPA that would apply in that scenario. In particular, they do not illustrate the application of the Data Protection Provisions, which were addressed earlier in these Guidelines. 12 The Do Not Call Provisions 12.1 Messages with a purpose to offer to supply, advertise or promote goods or services, land or an interest in land, or a business or investment opportunity, or a supplier of such goods, services, land or opportunity are specified messages and the Do Not Call Provisions will apply to such messages. Messages which do not contain any of such purposes would not be considered specified messages. 12.2 In addition, some types of messages, listed in the Eighth Schedule to the PDPA, are excluded from the definition of a specified message. Some examples include: a) "business-to-business" marketing messages; b) any message sent by a public agency under, or to promote, any programme carried out by any public agency,	

		which is not for a commercial purpose; c) any message the sole purpose of which is to facilitate, complete or confirm a transaction that the recipient of the message has previously agreed to enter into with the sender; d) any message that is sent while the sender is in an ongoing relationship with the recipient of the message; and the sole purpose of which relates to the subject matter of the ongoing relationship; or e) any message the sole purpose of which is to conduct market research or market survey. 12.3 The Do Not Call Provisions apply to a specified message (in the form of voice calls, text messages or faxes) addressed to a Singapore telephone number, if the sender of the specified message is present in Singapore when the specified message is sent, or the recipient of the specified message is present in Singapore when the specified message is accessed. Duty to check the Do Not Call Registers 12.4 One significant obligation under the Do Not Call Provisions is that the organisation sending the specified message will have to check the Do Not Call Registry (the "DNC Registry") established by the Commission under the PDPA to confirm that the number is not listed on the DNC Register, unless the user or subscriber of the Singapore telephone number has given clear and unambiguous consent in written or other accessible form.	

		12.5 The PDPA lists obligations for third-party checkers23 who check the DNC Registry for an organisation and provide to the organisation information on whether the Singapore telephone number is listed in the relevant DNC Register. The checker must make sure that information provided to the organisation is accurate and up-to-date in accordance with the provisions relating to the DNC Registry24, and to provide to the organisation the date of retrieval of this information and its validity period. 12.6 Examples: Whether messages are specified messages25 SSA ABC runs a caregiver support group for families taking care of the elderly and will be conducting a seminar to impart skills in caring for the elderly. a) SSA ABC sends an SMS to various individuals who are clients and volunteers to publicise the event. The message is likely to be a specified message to the extent that it is an offer to provide a service. b) SSA ABC calls SSA XYZ's office line to inform SSA XYZ about the seminar and ascertain whether SSA XYZ would like to promote the upcoming seminar to SSA XYZ's clients and volunteers. Such a call is not a specified message as under the Eighth Schedule, a message sent to an organisation (other than an individual acting in a personal or domestic capacity) for any business purposes of the receiving organisation is excluded from the meaning of	

		specified message. c) Should SSA XYZ market SSA ABC's seminar to individuals listed in SSA XYZ's own database of clients and volunteers by sending messages to their telephone numbers, SSA XYZ will be sending a specified message to those individuals. d) SSA ABC sends an SMS to its clients and volunteers, who had signed up for the seminar, informing of a postponement in the seminar. SSA ABC is not sending a specified message to the extent that the message does not offer to supply a good or service or have any of the other purposes listed in the definition of a specified message. 12.7 SSA XYZ is organising an annual charity fund-raiser. e) SSA XYZ sends an SMS to its donors and volunteers to donate money during the annual fund-raiser. To the extent that the SMS does not offer to supply a good or service or have any of the other purposes listed in the definition of a specified message, such a message would not be a specified message. f) SSA XYZ sends an SMS to its clients, donors and volunteers informing that it has partnered Company ABC to sell ABC's limited-edition products at the annual fund-raiser. In this case, as SSA XYZ is offering to supply or promoting Company ABC's products, it is considered to be sending a specified message. g) SSA XYZ calls its donors and	

		volunteers to thank them for the donations/assistance rendered at the charity fund-raiser. SSA XYZ is not sending a specified message as the message does not offer to supply a good or service or have any of the other purposes listed in the definition of a specified message. 12.8 Example: Obtaining clear and unambiguous consent for future volunteering opportunities John volunteers at SSA GHI where volunteers accompany elderly clients for an outdoor walk at the nature park. When John signed up for this volunteering activity in a form, he checked a box to indicate that he consents to receiving specified messages by SMS for future volunteering opportunities with SSA GHI, even after the outdoor walk with elderly clients. John would be considered to have provided clear and unambiguous consent for SSA GHI to send text messages for future volunteering opportunities. Therefore, SSA GHI may send such messages to John without checking the DNC Registry. Dictionary Attacks and Address-Harvesting Software 12.9 Section 48B of the PDPA provides that organisations must not send, cause to be sent, or authorise the sending of messages to recipient telephone numbers that are obtained by dictionary attack or address-harvesting. Dictionary attack is the method by which the telephone number is obtained using automated means that generate	

		possible telephone numbers by combining numbers into numerous permutations, whereas address-harvesting is a software specifically designed or marketed for use for searching the Internet for telephone numbers and the telephone numbers are collected, compiled, captured or otherwise harvested.	
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire	Purpose Limitation and Notification Obligations for in-vehicle recordings? 3.1 Leasing Companies, Hirers and Service Providers who are subject to the Consent, Purpose Limitation and Notification Obligations are required to notify individuals of the purposes and obtain their consent9 for collecting, using and disclosing their personal data if they record personal data of individuals through IVRDs, unless any exception applies. For example, consent need not be obtained for the collection, use or disclosure of personal data that is publicly available. For more information on the publicly available exception, please refer to paragraph 3.18 of this document. 3.2 Leasing Companies, Hirers and Service Providersshould also ensure that they collect, use or disclose personal data only for purposes that are reasonable. Reasonableness of a purpose would depend on whether a reasonable person would consider it appropriate in the circumstances10. How should notification be provided so as to obtain consent? 3.3 Leasing Companies, Hirers and Service Providers who are	

		subject to the Consent, Purpose Limitation and Notification Obligations must notify individuals of the purposes for collecting, using and disclosing the individuals' personal data in order to obtain consent under the PDPA. 3.4 The PDPC notes that there are various means of notifying an individual of the purposes for collection, use and disclosure of his personal data. For example, Leasing Companies, Hirers and Service Providers may wish to place a prominent notice at an appropriate location on the window of the passenger door such that individuals boarding the vehicle are made aware, before they board the vehicle, that IVRDs are deployed in the vehicle for a particular purpose. Within the vehicle, notices setting out the purpose of the recording could also be placed at prominent locations and a recorded message may be played in the vehicle before the start of the journey to inform individuals that IVRDs are in operation. The PDPA does not prescribe the manner of notification11 and the persons responsible for complying with the Notification Obligation should assess the most appropriate manner of notifying the individual of the purposes. 3.5 The PDPA also does not prescribe the content of such notifications. Generally, the notification should indicate that IVRDs are operating within the vehicle, and specify the purposesfor the collection, use and disclosure of the personal data. For example,	

		the notice could state that "in-vehicle video and/or audio recording is in operation for security and safety purposes". If there are other purposes for the collection, use and disclosure of personal data, these should be stated as well. 3.6 Example: Complying with the Consent, Purpose Limitation and Notification Obligations of the PDPA Taxi operator JKL places a prominent outward-facing notice indicating that IVRDs are in use in its taxis on the window of its taxis' passenger doors. Within the taxis, another notice is placed on the dashboard and the back of the head rests facing the passenger seats, which states clearly that the collection, use and disclosure of invehicle video recordings are for the purposes of ensuring the safety and security of the taxi driver and the passengers. A passenger sees the notices when boarding the taxi, and continues to take the taxi service. In this case, JKL would be considered to have obtained consent for the collection, use and disclosure of the passenger's personal data for those purposes12 . JKL would also be in compliance with the Purpose Limitation Obligation under the PDPA if the collected personal data was subsequently used or disclosed for the purposes as specified in the notice. 3.7 Example: Leasing Company complying with the Consent, Purpose Limitation and Notification Obligations of the PDPA	

		Leasing Company MNO provides limousine rental services. MNO has in place policies regarding the IVRDs it installs in its limousines, which stipulate that recordings will only be collected, used or disclosed for the purposes of ensuring the safety and security of the limousine driver and the passengers, as well as for the processing of insurance claims. MNO is contracted by an overseas-based company XYZ to provide limousine services in Singapore for XYZ's client, John. XYZ provides John with a form prepared by MNO that sets out the purposes for MNO's collection, use and disclosure of personal data, in particular personal data captured by in-vehicle recordings, and requires each prospective passenger to sign the form if he consents. XYZ provides MNO with a signed copy of the form that evidence John's consent. In this case, MNO would be considered to be in compliance with the Consent Obligation. 3.8 Example: Hirer complying with the Consent, Purpose Limitation and Notification Obligations of the PDPA Andy is a sole proprietor who provides transport services. He leases a limousine from Leasing Company PQR which has an IVRD installed. It is clearly stated in the leasing contract that the memory card for IVRDs is not provided and IVRDs are installed for use at the lessees' discretion and not for PQR's purposes. In addition, the contract provides that the	

		lessee is responsible for complying with all the Data Protection Provisions in respect of the collection, use and disclosure of the personal data recorded in the in-vehicle recordings, and as any recording is not on behalf of the PQR, the lessee must not represent or do anything that may imply that it is collecting, using, disclosing or processing personal data on behalf of PQR. Andy wishes to collect, use and disclose in-vehicle recordings for safety and security purposes, but he does not intend to place IVRD notices within the limousine. In this case, Andy could consider using other methods to notify his prospective passengers of the purposes for the collection, use or disclosure of their personal data, for example, in his email to a prospective passenger together with other terms of his transport services (e.g. costs) and requesting that consent be given (with confirmation of the booking) by replying to his email. 3.9 Further information on the Consent, Purpose Limitation and Notification Obligations can be found in Chapters 12, 13 and 14 of the Key Concepts Guidelines respectively. Can Leasing Companies, Hirers and Service Providers require individuals to consent to the in-vehicle recording to use their transport services? 3.10 The PDPA provides that an organisation shall not as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of the individual's personal data beyond what is	

		reasonable to provide the product or service to that individual. 3.11 Nonetheless, the PDPC recognises that there are certain situations where consent may be required for the provision of transport services. For example, it may be reasonable for Leasing Companies, Hirers and Service Providersto require those who wish to use their transport services to consent to the collection, use or disclosure of their personal data through in-vehicle recording to ensure the safety and security of the drivers, or to deter fare evasion. 3.12 Example: Passenger does not consent to the in-vehicle recording A taxi operator STU has in place policies on the use of IVRDs in its taxis, which stipulate that the IVRDs installed by STU in its taxis must remain in operation in the course of providing the taxi service for the purposes of ensuring the safety and security of the taxi driver and passengers. STU places prominent outward-facing notices on the windows of its taxis' passenger doors indicating that IVRDs are in use in its taxis. Before entering the taxi, the passenger sees the notices and is notified that invehicle video recordings are collected, used and disclosed for the safety and security purposes of the taxi driver and passengers. A passenger informs the taxi driver, before the start of the journey, that he does not consent to the collection, use and disclosure of his personal data in	

		the in-vehicle recording. As the collection, use or disclosure of personal data for the stipulated purpose is reasonable to provide the taxi service, consent of passengers can be required for the in-vehicle recording in order to provide the service. In this case, the taxi driver may inform the passenger of STU's requirement on the use of IVRD for the stipulated purposes, and allow the passenger to decide whether to use the taxi service. Can individuals withdraw consent for the use or disclosure of their personal data in the in-vehicle recording after using the transport service? 3.13 Leasing Companies, Hirers and Service Providers who are subject to the Consent, Purpose Limitation and Notification Obligations must allow individuals to withdraw any consent given under the PDPA, and put in place policies and practices to facilitate such withdrawal of consent. Leasing Companies, Hirers and Service Providers are advised to make their consent withdrawal policies easily accessible to individuals, and to include ways on how consent can be withdrawn. 3.14 If an individual withdraws consent for the use or disclosure of his personal data in the in-vehicle recording after using the transport service, the Leasing Company, Hirer and Service Provider must cease (and cause its data intermediaries and agents to cease13) using or disclosing the personal data in the in-vehicle recording, unless the	

		use or disclosure of the personal data without consent is required or authorised under the PDPA or any other written law. For example, the Leasing Company, Hirer and Service Provider may rely on exceptions provided in the Third and Fourth Schedules to the PDPA to use and disclose the passenger's personal data from the in-vehicle recording without consent where the use and disclosure are necessary for any investigation or proceedings. Leasing Companies, Hirers and Service Providers need not delete or destroy such personal data upon withdrawal of consent, and may retain the in-vehicle recording if there are any legal or business purposes to retain it. 3.15 Example: Withdrawal of consent after using the hired transport service John, a passenger, when boarding the taxi, consents to the taxi operator's collection of his personal data through in-vehicle recordings and to the use and disclosure of such personal data for safety and security purposes. At the end of the taxi journey, John withdraws his consent for the use and disclosure of his personal data in the invehicle recording and requests for its deletion. The taxi operator must cease, and cause its data intermediaries (which may be the taxi driver) to cease the use and disclosure of John's personal data in the in-vehicle recording, unless otherwise authorised or required under any written law. However, they need not delete the	

		recording upon withdrawal of consent, and may retain it if there are any legal or business purposes to retain it. 3.16 Example: Withdrawal of consent in the event of an investigation Ben, a passenger, when boarding the taxi, consents to the collection of his personal data through the taxi operator's in-vehicle recordings and to the use and disclosure of such personal data for safety and security purposes.During the journey, an incident takes place between Ben and the taxi driver. The taxi driver makes a police report for an alleged physical assault by Ben. Ben writes in to the taxi operator to withdraw consent for the use and disclosure of his personal data in the taxi's in-vehicle recording. The taxi operator may rely on exceptions provided in the Third and Fourth Schedules to the PDPA, to use and disclose the passenger's personal data in the in-vehicle recording without consent where it is necessary for any investigation or proceedings. In addition, the taxi operator need not delete the recording, and may retain it if there are any legal or business purposes to retain it. 3.17 For more information on withdrawal of consent, please refer to Chapter 12 of the Key Concepts Guidelines. How does the exception for "publicly available" personal data apply to in-vehicle recordings? 3.18 The PDPA does not require organisations to obtain the consent of individuals to collect personal data that is publicly available14. This	

		includes personal data that is observed by reasonably expected means at a location or event at which the individual appears and that is open to the public. The PDPC recognises that personal data of individuals appearing in public may be captured by outward-facing video cameras installed in hired transport services. Where such outward-facing cameras capture the images of individuals appearing in a public location outside the vehicle, the exception for "publicly available data" is likely to apply, and Leasing Companies, Hirers and Service Providers who are subject to the Consent, Purpose Limitation and Notification Obligations will not be required to notify and obtain consent from the individuals for the recording. 3.19 However, the exception for "publicly available data" does not apply where IVRDs capture images and/or voices of individuals inside the vehicle when it is hired. This is because the interior cabin of the vehicle would be considered a private space when it is hired. In such cases, Leasing Companies, Hirers and Service Providers must provide appropriate notification and obtain consent of the individuals before collecting, using or disclosing their personal data. 3.20 For more information on the exception for publicly available data, please refer to Chapter 12 of the Key Concepts Guidelines.	
33	Advisory Guidelines for the Real Estate Agency Sector	PART III: APPLICATION OF THE DO NOT CALL PROVISIONS TO SCENARIOS FACED IN THE REAL ESTATE AGENCY SECTOR The following examples outline the application of the Do Not Call	

		Provisions and the Exemption Order. They address particular aspects of the PDPA, and are not meant to exhaustively address every obligation in the PDPA that would apply in that scenario. In particular, they do not illustrate the application of the Data Protection Provisions, which were addressed earlier in these Guidelines. 5 The Do Not Call Provisions 5.1 Messages which purposes are to offer to supply, advertise, or promote goods or services, land or an interest in land, or a business or investment opportunity, or a supplier of such goods, services, land or opportunity are specified messages and the Do Not Call Provisions will apply to such messages. Messages offering to supply, advertise or promote property, or a supplier of property, would typically be considered specified messages. Messages which do not have any of the purposes listed above will not be considered specified messages. In addition, the Eighth Schedule to the PDPA sets out exclusions from the meaning of "specified message" that relate to, among others, any message sent by an individual acting in a personal or domestic capacity, any message the sole purpose of which is to conduct market research or market survey, any "business-to-business" marketing message and other types of information specified in the Eighth Schedule. 5.2 The Do Not Call Provisions apply to a specified message addressed to a Singapore telephone number if the sender of the specified message is present in Singapore when the specified message is sent or the	

		recipient of the specified message is present in Singapore when the specified message is accessed. 5.3 One significant obligation under the Do Not Call Provisions is that the organisation sending the specified message will have to check the Do Not Call Registers as described above, unless: a) the user or subscriber of the Singapore telephone number has given clear and unambiguous consent in written or other accessible form to the sending of the specified message to that number; or b) the organisation is exempted from complying with its obligation under the Exemption Order 5.4 Under the Exemption Order, a sender that is sending a specified fax message or a specified text message to a Singapore telephone number related to the subject of an ongoing relationship between the sender and a recipient is exempted from the requirement to check the relevant Do Not Call Registers, if certain conditions are met. An "ongoing relationship" under the Exemption Order means a relationship which is on an ongoing basis, between a sender and a subscriber or user of a Singapore telephone number, arising from the carrying on or conduct of a business or activity (commercial or otherwise) by the sender. The Commission's Advisory Guidelines on the Do Not Call Provisions provide further elaboration. 5.5 In determining what constitutes an ongoing relationship, the Commission considers one-off interactions or transactions in themselves to be	

		insufficient to be an ongoing relationship. For example, the fact that an individual previously contacted the sender to enquire about a particular property on sale, the fact that the individual previously engaged the sender to market a property for the individual, or the fact that the individual left his telephone number at a showroom, in themselves, would be insufficient to establish an ongoing relationship between the individual and the sender. 5.6 Examples: whether messages are specified messages Jack is a salesperson with estate agent ABC. Susan is interested to sell her apartment and engages Jack as her salesperson to market her apartment. (a) Jack receives an offer for the apartment and calls Susan to discuss the offer. Jack is not sending a specified message to Susan and the Do Not Call Provisions do not apply to the sending of the message. (b) Jack calls estate agent XYZ, who has been sourcing for suitable properties for a prospective buyer, to market Susan's apartment. Jack is sending a message to XYZ for the purposes of XYZ's business, i.e., a "business-to-business" marketing call, which is excluded from the meaning of "specified message". The Do Not Call Provisions do not apply to the sending of the message. (c) Jack buys a database of telephone numbers from a third party and calls a telephone number listed to ask if the individual would be interested to buy the property. Jack is sending a specified message to the recipient and the Do Not Call	

		Provisions apply. (d) Jack recalls his old contact list and calls Tom, who enquired about another property that Jack was marketing previously, to ask if he would be interested to buy the property. Jack is sending a specified message to Tom and the Do Not Call Provisions apply. 5.7 Jack is a salesperson with estate agent ABC. Susan is interested to buy an apartment and engages Jack to source for a suitable apartment for her. Jack manages to successfully find an apartment for Susan. Two years later, the property market appreciates and Jack calls Susan to ask if she would be interested to sell her apartment with him as her agent. Jack is sending a specified message to Susan (as he is offering his agency services to Susan) and the Do Not Call Provisions apply. 5.8 Jack is a salesperson with estate agent ABC stationed at the showroom of a new launch development "NewLaunch". Mark visits the showroom. (a) Jack walks Mark through the showroom and discusses a possible purchase of a NewLaunch unit with Mark. Mark tells Jack that he is not prepared to make a decision that day and would like to consider the purchase. Mark leaves his number with Jack and asks Jack to call him the next day for his final decision. Jack calls Mark the next day to find out his decision. As Jack is responding to Mark's request to call him about the decision on the purchase and not to make an offer or promote another good or service, Jack is not sending a specified message to Mark, and the Do Not Call Provisions do not apply.	

		(b) After Jack introduces the features of NewLaunch, Mark requests that Jack holds a unit for him and informs that he would return by close of business the next day with a cheque for the option amount. Jack calls Mark later to confirm if Mark will be heading back with the cheque. Jack will not be sending a specified message to Mark (as he is calling to confirm if Mark will be providing the down payment) and the Do Not Call Provisions will not apply. (c) Jack has no interaction with Mark at the showroom, but obtains Mark's contact details from the guestbook at the showroom. Jack calls Mark the next day to ask whether he would be interested to purchase a unit at NewLaunch. Jack will be sending a specified message to Mark and the Do Not Call Provisions apply. (d) Jack obtains Mark's contact details (either from Mark directly or from the guestbook) and calls Mark to market other properties that Jack or ABC is marketing. Jack will be sending a specified message to Mark and the Do Not Call Provisions apply. 5.9 Sarah advertises her apartment for sale in a newspaper. (a) Jack, a salesperson with estate agent ABC, contacts Sarah regarding her advertisement to offer his services to sell Sarah's apartment. In this case, Jack is considered to be sending a specified message as his offer of service would fall within the definition of a specified message. (b) One of estate agent GHI's salespersons, Tom, calls Sarah to enquire for more information about her apartment on behalf of a potential buyer. To the extent that Tom is not promoting,	

		marketing or offering any goods or services or any other activity that falls within the definition of a specified message, Tom would not be sending a specified message.15 5.10 Estate agent ABC sends an SMS to one of its salespersons, Sarah, informing her of details of an upcoming property launch and its proposed commission structure. To the extent that the SMS is for Sarah's business purposes, estate agent ABC will not be sending a specified message and the Do Not Call Provisions will not apply. 5.11 Example: Use of different contact details relating to the same individual but collected on different occasions Over the past few months, Sarah has been visiting various showflats of property developments marketed by estate agent ABC to source for a suitable home. At each showflat, Sarah provides either her home or mobile number in ABC's guestbook for ABC to contact her to follow-up on the developments. Sarah also gives clear and unambiguous consent in writing to the sending of specified messages regarding any and all property developments marketed by ABC to any and all of her telephone number(s) that she has provided to ABC. ABC would like to contact Sarah to inform her about a limited-period special discount offered to buyers of units in either of two upcoming properties, "NewLaunch" and "GreatLaunch". In this case, based on the scope of consent, ABC may contact Sarah using either her home or mobile number. 5.12 The following examples illustrate the application of the	

		Exemption Order. 5.13 Examples: When the Exemption Order may or may not apply based on whether there is an ongoing relationship (a) Sarah sends a message to enquire about a property marketed by a salesperson, Jack. Jack responds to the enquiry with more details about the property. In this case, while Jack can respond to Sarah's query, he cannot rely on the Exemption Order to subsequently send specified messages to Sarah's telephone number as her enquiry is a one-off interaction. (b) Sarah signs an option to purchase a property from Henry, which is marketed by a salesperson, Jack. Jack cannot rely on the Exemption Order to send specified messages to Sarah's telephone number as the option does not establish an ongoing relationship between Sarah and Jack. (c) Sarah previously engaged a salesperson, Jack, to sell her property. As part of maintaining his clientele base, Jack sends regular email updates to Sarah even though she neither requested for them nor responded to them. Jack cannot rely on the Exemption Order to send specified messages to Sarah's telephone number as the sale of Sarah's property is a one-off transaction and unilateral action on the part of Jack does not cause an ongoing relationship between Jack and Sarah to be formed. (d) Sarah signs up to be estate agent ABC's VIP member. VIP members receive regular updates on property market developments in Singapore and	

		analyses of the property market from estate agent ABC. When signing up, Sarah selects the types of properties she would like to be updated on based on a list of criteria (e.g. price, size, location, number of bedrooms) selected by her. This constitutes an ongoing relationship between ABC and Sarah. Estate agent ABC may rely on the Exemption Order to send text or fax messages containing updates about newly listed properties within the specified criteria to Sarah's telephone number (subject to other conditions in the Exemption Order being met 5.14 The following examples illustrate what the Commission would consider in assessing whether clear and unambiguous consent in evidential form has been given. 5.15 Examples: Obtaining clear and unambiguous consent in evidential form Jack is a salesperson with estate agent ABC marketing a property. The following situations, on their own, are not likely to constitute clear and unambiguous consent in evidential form from the subscriber to receive telemarketing calls from Jack: (a) 'Unverified claims' by third party: Jack buys a database of telephone numbers from a third party. The third party makes unverified claims that consent has been obtained from the subscribers of the telephone numbers to receive telemarketing calls; (b) Publicly available information: Jack obtained the telephone number from a publicly available source like a telephone directory or a publicly available social network profile; (c) Failure to opt out: There is a	

		sign at a showroom that states "ABC or its salespersons may contact you for marketing and promotions"; (d) Prior business relationship: Jack was previously in touch with Tom to source for or sell a property for Tom. 5.16 The following situations are likely to constitute clear and unambiguous consent in evidential form from the subscriber to receive telemarketing calls, if evidence is retained to demonstrate that the individual has indeed given such consent: (a) The guestbook at a showroom clearly indicates for every individual to "tick here if you wish to be contacted by phone or SMS for this development and other new launches by ABC Development Pte Ltd"; (b) Tom contacts Jack to enquire about a property. Jack sends an email to Tom with details of the property, in which Jack also asks if Tom would be agreeable to Jack calling him to provide information about other properties on the market. Tom replies "Yes" via email. 5.17 For avoidance of doubt, as noted in the Advisory Guidelines on the Do Not Call Provisions, a message sent to a Singapore telephone number where the purpose, or one of the purposes, is to obtain clear and unambiguous consent for the sending of specified messages, would be considered a specified message.	
34	Advisory Guidelines for the Healthcare Sector	PART III: APPLICATION OF THE DO NOT CALL PROVISIONS TO SCENARIOS FACED IN THE HEALTHCARE SECTOR The following sections and examples set out the application of the Do Not Call Provisions to	

		scenarios faced in the healthcare sector. They are not meant to exhaustively address every obligation in the PDPA that would apply in that scenario. In particular, they do not illustrate the application of the Data Protection Provisions, which were addressed earlier in these Guidelines. The Do Not Call Provisions Messages with a purpose to offer to supply, advertise or promote goods or services, land or an interest in land, or a business or investment opportunity, or a supplier of such goods, services, land or opportunity are specified messages17 and the Do Not Call Provisions will apply to such messages. Messages which do not contain any of such purposes would not be considered specified messages. In addition, some types of messages, listed in the Eighth Schedule to the PDPA, are excluded from the definition of a specified message. Some examples include: a) "business-to-business" marketing messages; b) any message sent by a public agency under, or to promote, any programme carried out by any public agency, which is not for a commercial purpose; c) any message the sole purpose of which is to facilitate, complete or confirm a transaction that the recipient of the message has previously agreed to enter into with the sender; d) any message that is sent while the sender is in an ongoing relationship with the recipient of the message; and the sole purpose of which relates to the subject matter of the ongoing relationship; or	

		e) any message the sole purpose of which is to conduct market research or market survey. The Do Not Call Provisions apply to a specified message addressed to a Singapore telephone number if the sender of the specified message is present in Singapore when the specified message is sent, or the recipient of the specified message is present in Singapore when the specified message is accessed Example: Messages that are not specified messages Example 1 Clinic ABC calls John at his Singapore telephone number on different occasions solely for one of the following purposes: a) To confirm that he has completed the full course of his medication. b) To check that his fever has subsided. c) To make an appointment to review the results from the previous check-up. These messages are unlikely to be considered specified messages. Example 2 James visits Dental Clinic DEF for the first time for a dental treatment. At the end of the visit, James makes an appointment with Dental Clinic DEF for his next visit. A week before the appointment date, Dental Clinic DEF sends James a text message at his Singapore telephone number solely to remind him of his appointment. Such a reminder sent by Dental Clinic DEF solely for the purpose of reminding James of his appointment would unlikely be considered a specified message.	

		One significant obligation under the Do Not Call Provisions is that the organisation sending the specified message will have to check with the Do Not Call (DNC) Registry, unless the user or subscriber of the Singapore telephone number has given clear and unambiguous consent in written or other accessible form to the sending of the specified message to that number. The PDPA lists obligations for third-party checkers18 who check the DNC Registry for an organisation and provide to the organisation information on whether the Singapore telephone number is listed in the relevant DNC Register. The checker must make sure that information provided to the organisation is accurate and up-to-date in accordance with the provisions relating to the DNC Registry19, and to provide to the organisation the date of retrieval of this information and its validity period. Example: Obtaining clear and unambiguous consent Example 1 Clinic ABC sends out a letter to inform all its former patients about a new healthcare supplement. The letter says that unless they reply to opt out, they would be considered to have provided consent for Clinic ABC to call them to market the supplement. Peter does not reply to opt out. The failure to opt out by Peter is in itself unlikely to constitute clear and unambiguous consent for Clinic ABC to call him for purposes of marketing the supplement. Clinic ABC must check the DNC Register and receive confirmation that Peter's	

		number is not listed before calling him to market the supplement. If Clinic ABC had engaged by contract a third-party checker that helps to check the DNC Registry, the third-party checker is responsible for checking that the information on whether Peter's number is listed is accurate and up-to-date. Example 2 Jason visits Dental Clinic DEF for the first time for a dental treatment. When providing his personal data to Dental Clinic DEF in the patient registration form, Jason checks a box to indicate that he consents to receiving reminder text messages from Dental Clinic DEF for subsequent dental visits. Jason would be considered to have provided clear and unambiguous consent for Dental Clinic DEF to send reminder text messages for his next dental visits. In addition, the sole purpose of Dental Clinic DEF sending the reminder text messages is to facilitate the transaction that Jason has previously agreed to. Therefore, Dental Clinic DEF may send such messages to Jason without checking the Do Not Call Registry. 6.8 Example: Messages where the sender is in an ongoing relationship with the recipient Clinic ABC regularly calls or sends text messages to its patients with chronic conditions at their Singapore telephone numbers to inform them about new drugs or medical procedures which the doctor considers could be effective treatment for their condition. Whether Clinic ABC has to first check the Do Not Call	

		Registers to ensure that the Singapore telephone numbers are not listed would depend largely on whether the new drug or procedure relates to a medical condition for which Clinic ABC is providing ongoing treatment to the relevant recipients. Example 1 John is undergoing treatment on an ongoing basis at Clinic ABC for his chronic asthma. Clinic ABC sends a text message to John to inform him about a new drug which could be effective treatment for his asthma. In this scenario, Clinic ABC's message can be excluded from the meaning of "specified message" in the Eighth Schedule to the PDPA and is not subject to the DNC provisions. Example 2 Clinic ABC calls Sarah to inform her about a new drug which could be an effective treatment for asthma. Sarah has never sought treatment at Clinic ABC for asthma or asthma-related conditions, and does not have an ongoing relationship with Clinic ABC. In this scenario, Clinic ABC will not be able to rely on the exclusions listed under the Eighth Schedule to the PDPA and will need to check the Do Not Call Register before calling or sending a text message to Sarah, unless Clinic ABC had obtained clear and unambiguous consent in written or other accessible form from Sarah. For clarity, even if Sarah was undergoing treatment at Clinic ABC for another medical condition (e.g. migraines), Clinic ABC must comply with the DNC provisions when it sends a marketing message to Sarah about an unrelated condition (e.g.	

		asthma). Dictionary Attacks and Address-Harvesting Software 6.9 Section 48B of the PDPA provides that organisations must not send, cause to be sent, or authorise the sending of messages to recipient telephone numbers that are obtained by dictionary attack or address-harvesting. Dictionary attack is the method by which the telephone number is obtained using automated means that generate possible telephone numbers by combining numbers into numerous permutations, whereas address-harvesting is a software specifically designed or marketed for use for searching the Internet for telephone numbers and the telephone numbers arecollected, compiled, captured or otherwise harvested.	
35	Advisory Guidelines for the Telecommunication Sector	PART III: APPLICATION OF THE DO NOT CALL PROVISIONS TO SCENARIOS FACED IN THE TELECOMMUNICATION SECTOR The following sections and examples outline the application of the Do Not Call Provisions and the Personal Data Protection (Exemption from Section 43) Order (S 817/2013) ("Exemption Order"). They address particular aspects of the PDPA, and are not meant to exhaustively address every obligation in the PDPA that would apply in that scenario. In particular, they do not illustrate the application of the Data Protection Provisions, which were addressed earlier in these Guidelines. 5 The Do Not Call Provisions 5.1 Messages which purposes are to offer to supply, advertise or promote goods or services, land or an interest in land, or a business or investment	

		opportunity, or a supplier of such goods, services, land or opportunity are specified messages and the Do Not Call Provisions will apply to such messages. Messages which do not have any of the purposes listed above will not be considered specified messages. In addition, the Eighth Schedule to the PDPA sets out exclusions from the meaning of "specified message" that relate to, among others, any message sent by an individual acting in a personal or domestic capacity, any message the sole purpose of which is to conduct market research or market survey, any "business-to-business" marketing message and other types of information specified in the Eighth Schedule. 5.2 The Do Not Call Provisions apply to a specified message addressed to a Singapore telephone number if the sender of the specified message is present in Singapore when the specified message is sent or the recipient of the specified message is present in Singapore when the specified message is accessed. 5.3 One significant obligation under the Do Not Call Provisions is that the organisation sending the specified message will have to check the Do Not Call Registers as described above, unless: a) the user or subscriber of the Singapore telephone number has given clear and unambiguous consent in written or other accessible form to the sending of the specified message to that number; or b) the organisation is exempted from complying with its obligation under the Exemption Order.	

		5.4 Under the Exemption Order, a sender that is sending a specified fax message or a specified text message to a Singapore telephone number related to the subject of an ongoing relationship between the sender and a recipient is exemptedfrom the requirement to check the relevant Do Not Call Registers, if certain conditions are met. An "ongoing relationship" under the Exemption Order means a relationship which is on an ongoing basis, between a sender and a subscriber or user of a Singapore telephone number, arising from the carrying on or conduct of a business or activity (commercial or otherwise) by the sender. The Commission's Advisory Guidelines on the Do Not Call Provisions provide further elaboration. 5.5 In determining what constitutes an ongoing relationship, the Commission considers one-off interactions or transactions in themselves to be insufficient to constitute an ongoing relationship. For example, the fact that an individual previously contacted a telecommunication operator to enquire about a particular product or service, or the fact that the individual left his telephone number with a sales representative of the telecommunication operator, in themselves, would be insufficient to establish an ongoing relationship between the individual and the telecommunication operator. Specified messages sent by telecommunication operators 5.6 The Commission understands that telecommunication operators typically send messages with the	

		following characteristics to Singapore telephone numbers: a) Account information, such as that relating to: i. account balance, for example the credit levels pertaining to a pre-paid card, sent at regular periodic intervals; ii. account details, for example on the fact that a pre-paid card has not been active and will be expiring on a certain date, or seeking a change of billing details following the expiry of credit card information previously provided; and iii. reminders for late payments. b) Product or service information, such as that relating to: i. contract expiry and renewal, for example informing the customer that his subscription contract will be expiring; ii. warranty, product recall, safety or security information relating to the individual's subscription; and iii. delivery of product upgrades or updates that the subscriber is entitled to receive under his existing subscription, for example an upgrade in broadband speed of the subscriber's existing broadband plan that the subscriber is entitled to receive under his existing subscription. c) Marketing information, such as: i. promoting a product or service that the individual has not subscribed to. This will include up-selling of products or services, for example promoting a higher speed broadband plan to an existing broadband subscriber, or a mobile package with more free SMSes to a heavy SMS user that has subscribed to a different package. Similarly,	

		cross-selling of products or services, such as the promotion of premium rate services to mobile subscribers or the promotion of home broadband plans to a mobile subscriber will also be included; ii. limited promotions, for example informing certain pre-paid mobile plan subscribers about an International Direct Dial ("IDD") rate promotion to certain destinations for a limited period of time; and iii. promoting the products and services of affiliates or partners, such as offering discounts at certain retail shops or food and beverage outlets. 5.7 As a general guide, the Commission is likely to consider that a message sent to a Singapore telephone number solely to provide account information or product or service information (such as those in sub-paragraphs 4.6 (a) and (b) above) relating to the ongoing use of the service / product by the individual would not constitute the sending of a specified message. In particular, such messages could fall within paragraph 1(d) or 1(e) of the Eighth Schedule to the PDPA. 5.8 Example: 'In-service' messages The following messages from a telecommunication operator to a subscriber could fall within paragraph 1(e) of the Eighth Schedule to the PDPA: a) messages to existing subscribers solely informing them of the expiry of their subscriptions; and b) messages to subscribers of pre-paid mobile plans solely informing them of their account balance, sent at regular periodic intervals.	

		5.9 Example: Messages related to subject of ongoing relationship The following messages from a telecommunication operator to a subscriber could typically be considered to be related to the subject of the ongoing relationship: a) a message to an existing home fixed-line broadband service subscriber offering to supply a fibre broadband subscription to that subscriber; and b) a message to a pre-paid mobile service subscriber informing the subscriber of an IDD rate promotion to certain countries for pre-paid subscribers. Clear and unambiguous consent in evidential form 5.10 The Commission does not prescribe how clear and unambiguous consent in evidential form may be obtained. The Key Concepts Guidelines and the Advisory Guidelines on the Do Not Call Provisions provide some examples on how such consent may be obtained. 5.11 Example: obtaining clear and unambiguous consent in evidential form from pre-paid mobile subscribers If a telecommunication operator wishes to send specified messages to a subscriber of pre-paid mobile services, it would need to comply with the Do Not Call Provisions. In particular, it would have to check that the number is not registered on the relevant Do Not Call Register(s) unless it obtains clear and unambiguous consent in evidential form from the subscriber to the sending of	

		specified messages to his Singapore telephone number (or the Exemption Order applies). In this regard, the telecommunication operator may consider options such as entering into an arrangement with the reseller to obtain such clear and unambiguous consent on its behalf (for example, at the point of purchase).	
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act	The Openness Obligation 9 – Openness Obligation in PDPA An organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available. An organisation is to designate one or more individuals ("data protection officer(s)" or "DPO(s)")to be responsible for ensuring that the organisation complies with the PDPA, and the business contact information of at least one of such individuals designated (or an authorised delegate) shall be made available to the public upon request. An organisation is also required to: (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under the PDPA; (b) develop a process to receive and respond to complaints that may arise with respect to the application of PDPA; (c) communicate to its staff information about the organisation's policies and practices referred to in (a); and (d) make information available	

		on request about policies and practices in (a) and the complaint process in (b). 52. The life insurer may designate one or more of its DPOs to provide assistance and support to tied agents in relation to compliance with the PDPA. 53. The life insurer will make available to the public the business contact information of at least one of the DPOs (or authorised delegate). Tied agents should direct any queries relating to the life insurers' compliance with the PDPA, and/or the complaint process to a DPO (or authorised delegate) designated by the life insurer. 54. The life insurer would support its tied agents by setting up the relevant policies and procedures required to achieve (a) to (d) above. A tied agent conducting activities as a representative of the life insurer will need to comply with such policies and procedures, and communicate them to his agency's office staff.	

#	Regulation	external	external
		Data protection impact assessment	Others
1	Personal Data Protection Act 2012		
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical		

	Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		

18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment	Accountability Data Protection Impact Assessments ("DPIA") To meet the Accountability Obligation under the PDPA, organisations are advised to conduct DPIAs to help them develop and implement appropriate policies and practices. In addition, organisations are encouraged to conduct a DPIA before releasing products or services that are likely to be accessed by children, to identify and address personal data protection risks13. For sample questions to consider when conducting a DPIA, refer to Annex A.	
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems	10 The Accountability Obligation 10.1 The Accountability Obligation refers to how an organisation discharges its responsibility for personal data which it has collected or obtained for processing, or which it has control over. Sections 11 and 12 of the PDPA detail the actions to be carried out by organisations in fulfilment of this obligation16. 10.2 Among other things, Section 12 of the PDPA requires organisations to develop policies and practices to meet its obligations under the PDPA. Written policies and documentation of processes enable organisations to show that their internal governance and supervision structures as well as operational practices ensure the responsible use of personal data. Such use should either in line with purposes that individuals have been notified of and consented to or for legitimate purposes that a reasonable person would consider appropriate in the	

		circumstances17. 10.3 Organisations that make use of AI Systems should be transparent and include in their written policies relevant practices and safeguards to achieve fairness and reasonableness18. The level of detail to be provided should be proportionate to the risks in each use-case, e.g., taking into account potential harm to the individual and the level of autonomy of the AI System. 10.4 Section 12(d) requires organisations to make information about such policies and practices available to individuals upon request. As the raison d'etre for such external communications with consumers is to help build trust with data subjects by demonstrating accountability in compliance with the PDPA, organisations should consider pre-emptively making such written policies available through their website, and not only upon request. Organisations should also consider making policies available in the form of short policy that is simple, clear, and concise. 10.5 Written policies can house more detailed information that organisations ought to provide to obtain meaningful consent19. Where organisations have relied on exceptions to consent, e.g., Business Improvement and Research Exceptions, written policies can also provide information about the practices and safeguards that were adopted to protect the interests of individuals20. Developing industry best practices, such as model cards and system cards, can also form part of an organisation's written policies.	

		10.6 Written policies also play an important function in education and confidencebuilding, which are necessary ingredients for building consumer trust and confidence. Policies could therefore include behind-the-scenes measures taken to ensure that the personal data is used in a safe and trusted manner within the AI System, such as: a) Measures taken to achieve fairness and reasonableness for recommendations, predictions, and decisions for the benefit of consumers during model development and testing stages. These can include measures relating to bias assessment, ensuring quality of training data or other data governance measures, or the repeatability/reproducibility of results using personal data. b) Safeguards and technical measures taken to protect personal data. These can include measures to protect personal data during model development and testing (e.g., pseudonymisation and data minimisation), or steps to ensure personal data is protected in the AI System via ensuring the security of such systems before and after they are deployed. c) For outcomes that have a higher impact on the individual, organisations may wish to consider whether it is useful to provide information on how proper accountability mechanisms and human agency and oversight have been implemented. It may also be useful to provide information on safety and/or robustness of the AI System i.e., how the AI System will operate when encountering adversarial or unexpected input. 10.7 Information on the above-	

		mentioned measures is not always required. Organisations using personal data for model development and testing, and in deployed AI Systems, should consider adopting measures that a reasonable person would consider appropriate in the circumstances. Having done so, organisations are encouraged to consider providing sufficient information about such measures to build consumer trust and confidence. 10.8 Organisations are generally encouraged to provide more information on data quality and governance measures taken during AI System development. This is only if such information is deemed relevant and doing so does not compromise security, safety, or commercial confidentiality. Information that organisations can consider including are: a) Steps taken to ensure the quality of personal data in the training dataset (e.g., how representative it is of the market and how recently it was compiled) to improve model accuracy and performance; b) Whether model development was conducted using pseudonymised data, and if not, what organisation, process or technical safeguards were adopted to restrict access to personal data to developers and/or testers who had access; c) Whether it was necessary to use personal data when conducting bias assessment to check if protected characteristics, such as race or religion, are well represented in the training dataset or to assess the bias of the training dataset; d) If personal data was used, what process or technical	

		safeguards were adopted to secure the testing environment and to limit access to testers; and e) Whether data minimisation was practised at all stages of model and/or AI System development and testing. Additional resources 10.9 Organisations may wish to refer to the Model AI Governance Framework for further suggestions on managing stakeholder interaction (see in particular Section 3, pages 53 – 55). Organisations may also find the guiding questions and examples on stakeholder interaction provided in Section 5 of the Implementation and SelfAssessment Guide for Organisations helpful. 10.10 Organisations can consider using technical tools such as AI Verify to validate the performance of AI Systems. Information from the testing report can be used to support information that organisations wish to include into their notifications or written policies. For example: a) Results of explainability testing can be used to identify the data features that are most likely to influence the recommendation, prediction, or decision. b) Results of fairness testing can be used to illustrate differences in model outcomes across demographic groups to show that there has not been unreasonable discrimination or bias in the use of personal data by an AI System. This can also be supported by process checks for repeatability/reproducibility. c) Process checks for security can support an organisation's statement in their notification that they have taken steps to	

		ensure that personal data used in an AI System is protected. d) AI Verify also includes process checks that organisations may find useful to validate any claims in their notifications that they have included on accountability/human oversight and safety of the AI System. Robustness testing may also be useful if organisations intend to provide information on the robustness of the AI System in their notification. Where possible, improvements should be introduced. 10.11 It is good practice for organisations to develop processes to regularly review the quality of the information provided, as well as the effectiveness of its notifications, policies, and practices for their intended audience. 10.12 Organisations are also encouraged to perform impact assessments, particularly data protection impact assessments, where these are deemed to be useful. These can help support organisations in their efforts to identify and mitigate data protection risks in an AI System. Organisations may wish to refer to the Commission's Guide on Data Protection Impact Assessments for more guidance on this area.	
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act		
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		

23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions		
26	Advisory Guidelines on Application of PDPA to Election Activities		
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		
29	Advisory Guidelines for Management Corporations		
30	Advisory Guidelines for the Education Sector		
31	Advisory Guidelines for the Social Service Sector		
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector		

34	Advisory Guidelines for the Healthcare Sector		
35	Advisory Guidelines for the Telecommunication Sector		
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		

#	Regulation	internal	internal
		technical and organisational measures	Purpose Limitation
1	Personal Data Protection Act 2012	Protection of personal data 24. An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent — (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. [40/2020]	Limitation of purpose and extent 18. An organisation may collect, use or disclose personal data about an individual only for purposes — (a) that a reasonable person would consider appropriate in the circumstances; and (b) that the individual has been informed of under section 20, if applicable.
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		

7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the	Section 18 of the PDPA provides that an organisation may collect,	

	PDPA for Children's Personal Data in the Digital Environment	use, or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances. For example, a purpose that is in violation of the law or which would be harmful to the individual concerned is unlikely to be considered appropriate by a reasonable person. The PDPC will continue to adopt a principles-based approach to consider what is reasonable when collecting, using, or disclosing a child's personal data. Given the potential risks and harms to children in the digital environment, examples of what is reasonable include, but is not limited to: a. collecting and using a child's personal data or profile for age assurance to ensure that only age-appropriate content is accessible; b. collecting and using a child's personal data or profile to protect the child from harmful and inappropriate content; and c. using the behavioural data of a child, such as the use of high-risk search terms including terms relating to self-harm or suicide, to direct the child to relevant safety information. The PDPC will consider as unreasonable, the use of a child's personal data or profile to target harmful or inappropriate content (as defined in the Code of Practice for Online Safety6) at the child. In addition, organisations should adopt data minimisation7 policies to limit the	

		collection and sharing of children's personal data. For instance, the account information of children must not be made public and searchable, by default. Ascertainment of age The PDPC supports organisations' use of age assurance methods for the purpose of conforming to these Guidelines, including age verification or estimation methods to ascertain the user's age, so that organisations can implement relevant safeguards when the user is a child. While doing so, organisations should practice data minimisation and collect the minimum amount of personal data necessary for those age ascertainment purposes. Example: Prompting users to take breaks during gameplay An organisation's online game is accessible by children and does not require a user to sign up for an account before the user can play the game. The organisation wishes to prompt users to take breaks from extended gameplay. The organisation can use age estimation methods to estimate the age or age range of the user, so that if the user is likely to be a child, the game can remind the user to take a break. Organisations performing age assurance do not have to limit themselves to the account registration stage and may do so at appropriate juncture(s). In addition, unless required under applicable laws, organisations are not required to collect national identity documents for age assurance purposes.	

		The PDPC is aware that some age assurance methods involve the collection and analysis of the behavioural and telemetric data of users to build profiles8 that are used to ascertain the age or age range of individual users. Organisations should take note that once they have collected data about a user to such an extent that the user can be identified from that data, or from that data and other information to which the organisation has or is likely to have access, then the user profile will be personal data. Example: Whether the data collected is considered personal data An organisation offering social media services does not require a user to sign up for an account before the user can access social media content. The organisation can ask the user to declare his or her age so that if the user is a child, the organisation can provide the user with age-appropriate content and restrict the user from accessing harmful or inappropriate content, including in the form of advertisements. As it would not be possible to identify who the user is based solely on the age declared by the user, the age that was declared by the user is not considered personal data. However, if browsing history or other behavioural data is collected and associated with the unique identifier of a user such that an individual can be identified from that data, then the	

		data will be considered personal data. Geolocation data Geolocation data refers to data taken from a device which could be used to identify the geographical location of that device. Examples of such data include global navigational satellite system ("GNSS"9) data and data from Wi-Fi access points. The PDPC considers geolocation data to be personal data to the extent that an individual can be uniquely identified when the geolocation data is combined with other identifiers. As the ability to determine or monitor the precise location of a child poses the risk of misuse that may compromise the child's safety, organisations should adopt a data minimisation approach and implement relevant safeguards considering how the product / service would be used by children. One safeguard is disabling the geolocation function by default so that precise location data is not automatically collected when a product or service is first used. Other safeguards include collecting users' approximate location rather than precise location. For other good practices, refer to the PDPC's Guide to Data Protection Practices for ICT Systems. Example: Default settings for geolocation data A child wants to install a photo filter app for children that allow users to take and edit photos. Although the app has a	

		function to tag the precise location of where a photo was taken, this geolocation function should be disabled by default so that precise location data is not automatically collected. The app should use readily understandable language to notify users and obtain consent prior to any collection, use or disclosure of geolocation data. The app should also consider the granularity of the location data needed and not collect more than necessary. In addition, a prominent symbol could be used to indicate when the geolocation function is enabled or disabled. Protection of children's personal data The personal data of children is generally considered to be sensitive personal data and must be accorded a higher standard of protection under the PDPA10. Any organisation that handles children's personal data should implement, where appropriate, the Basic and Enhanced Practices listed in the PDPC's Guide to Data Protection Practices for ICT Systems11, to address potential risks and harms to children in the digital environment. However, this list does not preclude organisations from implementing additional or alternative measures to fulfil their obligation to protect the personal data in their possession or under their control. Some examples include: Basic Practices a. Developing and implementing Infocomm technology ("ICT") security policies for	

		data protection, including policies on account and access control, backup and retention, and passwords. b. Assessing and mitigating the security risks involved in outsourcing or engaging external parties for ICT services. Enhanced Practices c. Using a one-time password ("OTP") or 2-Factor Authentication ("2FA") / MultiFactor Authentication ("MFA") for admin access to personal data and logging all access. d. Conducting network penetration testing prior to the commissioning of any new ICT system to detect and resolve any vulnerabilities before the system goes "live".	
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems	10 The Accountability Obligation 10.1 The Accountability Obligation refers to how an organisation discharges its responsibility for personal data which it has collected or obtained for processing, or which it has control over. Sections 11 and 12 of the PDPA detail the actions to be carried out by organisations in fulfilment of this obligation16. 10.2 Among other things, Section 12 of the PDPA requires organisations to develop policies and practices to meet its obligations under the PDPA. Written policies and documentation of processes enable organisations to show that their internal governance and supervision structures as well as operational practices ensure the responsible use of personal data. Such use should either in line with purposes that individuals have been notified of and consented to or for	

		legitimate purposes that a reasonable person would consider appropriate in the circumstances17. 10.3 Organisations that make use of AI Systems should be transparent and include in their written policies relevant practices and safeguards to achieve fairness and reasonableness18. The level of detail to be provided should be proportionate to the risks in each use-case, e.g., taking into account potential harm to the individual and the level of autonomy of the AI System. 10.4 Section 12(d) requires organisations to make information about such policies and practices available to individuals upon request. As the raison d'etre for such external communications with consumers is to help build trust with data subjects by demonstrating accountability in compliance with the PDPA, organisations should consider pre-emptively making such written policies available through their website, and not only upon request. Organisations should also consider making policies available in the form of short policy that is simple, clear, and concise. 10.5 Written policies can house more detailed information that organisations ought to provide to obtain meaningful consent19. Where organisations have relied on exceptions to consent, e.g., Business Improvement and Research Exceptions, written policies can also provide information about the practices and safeguards that were adopted to protect the interests of individuals20. Developing industry best practices,	

		such as model cards and system cards, can also form part of an organisation's written policies. 10.6 Written policies also play an important function in education and confidencebuilding, which are necessary ingredients for building consumer trust and confidence. Policies could therefore include behind-the-scenes measures taken to ensure that the personal data is used in a safe and trusted manner within the AI System, such as: a) Measures taken to achieve fairness and reasonableness for recommendations, predictions, and decisions for the benefit of consumers during model development and testing stages. These can include measures relating to bias assessment, ensuring quality of training data or other data governance measures, or the repeatability/reproducibility of results using personal data. b) Safeguards and technical measures taken to protect personal data. These can include measures to protect personal data during model development and testing (e.g., pseudonymisation and data minimisation), or steps to ensure personal data is protected in the AI System via ensuring the security of such systems before and after they are deployed. c) For outcomes that have a higher impact on the individual, organisations may wish to consider whether it is useful to provide information on how proper accountability mechanisms and human agency and oversight have been implemented. It may also be useful to provide information on safety and/or robustness of the	

		AI System i.e., how the AI System will operate when encountering adversarial or unexpected input. 10.7 Information on the above-mentioned measures is not always required. Organisations using personal data for model development and testing, and in deployed AI Systems, should consider adopting measures that a reasonable person would consider appropriate in the circumstances. Having done so, organisations are encouraged to consider providing sufficient information about such measures to build consumer trust and confidence. 10.8 Organisations are generally encouraged to provide more information on data quality and governance measures taken during AI System development. This is only if such information is deemed relevant and doing so does not compromise security, safety, or commercial confidentiality. Information that organisations can consider including are: a) Steps taken to ensure the quality of personal data in the training dataset (e.g., how representative it is of the market and how recently it was compiled) to improve model accuracy and performance; b) Whether model development was conducted using pseudonymised data, and if not, what organisation, process or technical safeguards were adopted to restrict access to personal data to developers and/or testers who had access; c) Whether it was necessary to use personal data when conducting bias assessment to check if protected characteristics, such as race or	

		religion, are well represented in the training dataset or to assess the bias of the training dataset; d) If personal data was used, what process or technical safeguards were adopted to secure the testing environment and to limit access to testers; and e) Whether data minimisation was practised at all stages of model and/or AI System development and testing. Additional resources 10.9 Organisations may wish to refer to the Model AI Governance Framework for further suggestions on managing stakeholder interaction (see in particular Section 3, pages 53 – 55). Organisations may also find the guiding questions and examples on stakeholder interaction provided in Section 5 of the Implementation and SelfAssessment Guide for Organisations helpful. 10.10 Organisations can consider using technical tools such as AI Verify to validate the performance of AI Systems. Information from the testing report can be used to support information that organisations wish to include into their notifications or written policies. For example: a) Results of explainability testing can be used to identify the data features that are most likely to influence the recommendation, prediction, or decision. b) Results of fairness testing can be used to illustrate differences in model outcomes across demographic groups to show that there has not been unreasonable discrimination or bias in the use of personal data by an AI System. This can also	

		be supported by process checks for repeatability/reproducibility. c) Process checks for security can support an organisation's statement in their notification that they have taken steps to ensure that personal data used in an AI System is protected. d) AI Verify also includes process checks that organisations may find useful to validate any claims in their notifications that they have included on accountability/human oversight and safety of the AI System. Robustness testing may also be useful if organisations intend to provide information on the robustness of the AI System in their notification. Where possible, improvements should be introduced. 10.11 It is good practice for organisations to develop processes to regularly review the quality of the information provided, as well as the effectiveness of its notifications, policies, and practices for their intended audience. 10.12 Organisations are also encouraged to perform impact assessments, particularly data protection impact assessments, where these are deemed to be useful. These can help support organisations in their efforts to identify and mitigate data protection risks in an AI System. Organisations may wish to refer to the Commission's Guide on Data Protection Impact Assessments for more guidance on this area.	
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal	The Protection Obligation 17.1 Section 24 of the PDPA requires an organisation to make reasonable security arrangements to protect	The Purpose Limitation Obligation Section 18 of the PDPA limits the purposes for which and the extent to which an

	Data Protection Act	personal data in its possession or under its control in order to prevent (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. This obligation of organisations to protect personal data is referred to in these Guidelines as the Protection Obligation. 17.2 There is no 'one size fits all' solution for organisations to comply with the Protection Obligation. Each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances, for example, taking into consideration the nature of the personal data, the form in which the personal data has been collected (e.g. physical or electronic) and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data. For example, in the employment context, it would be reasonable to expect a greater level of security for highly confidential employee appraisals as compared to more general information about the projects an employee has worked on. 17.3 In practice, an organisation should: a) design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach; b) identify reliable and well-trained personnel responsible for ensuring information	organisation may collect, use or disclose personal data. Specifically, section 18 provides that an organisation may collect, use or disclose personal data about an individual only for purposes: a) that a reasonable person would consider appropriate in the circumstances; and b) where applicable, that the individual has been informed of by the organisation (pursuant to the Notification Obligation). The obligation of organisations to collect, use and disclose personal data for the limited purposes specified in section 18 of the PDPA is referred to in these Guidelines as the Purpose Limitation Obligation. The main objective of the Purpose Limitation Obligation is to ensure that organisations collect, use and disclose personal data that are relevant for the purposes, and only for purposes that are reasonable. Consistent with the Notification Obligation, the Purpose Limitation Obligation also limits the purposes for which personal data may be collected, used or disclosed to those which have been informed to the individuals concerned pursuant to the Notification Obligation (where applicable). For the purposes of section 18 (and as stated in that section), whether a purpose is reasonable depends on whether a reasonable person would consider it appropriate in the circumstances. Hence the particular circumstances involved need to be taken

		security; c) implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and d) be prepared and able to respond to information security breaches promptly and effectively. 17.4 In addition, it might be useful for organisations to undertake a risk assessment exercise to ascertain whether their information security arrangements are adequate. In so doing, the following factors may be considered: a) the size of the organisation and the amount and type of personal data it holds; b) who within the organisation has access to the personal data; and c) whether the personal data is or will be held or used by a third party on behalf of the organisation. Examples of security arrangements 17.5 Security arrangements may take various forms such as administrative measures, physical measures, technical measures or a combination of these. The following tables list examples of such measures. Examples of administrative measures an organisation may use to protect personal data: • Requiring employees to be bound by confidentiality obligations in their employment agreements; • Implementing robust policies and procedures (with disciplinary consequences for breaches) regarding confidentiality obligations;	into account in determining whether the purpose of such collection, use or disclosure is reasonable. For example, a purpose that is in violation of a law or which would be harmful to the individual concerned is unlikely to be considered appropriate by a reasonable person. Example: A fashion retailer is conducting a membership drive. It states in the membership registration form that the purposes for which it may use the details provided by individuals who register including providing them with updates on new products and promotions and any other purpose that it deems fit. In this case, providing updates on new products and promotions may be a reasonable purpose but the fashion retailer's unqualified reference to 'any other purpose that it deems fit' would not be considered reasonable. (As noted in Chapter 14 on the "Notification Obligation", this may also be an inadequate notification to the individual of the purposes for which his or her personal data will be collected, used and disclosed.)

		• Conducting regular training sessions for staff to impart good practices in handling personal data and strengthen awareness of threats to security of personal data; and • Ensuring that only the appropriate amount of personal data is held, as holding excessive data will also increase the efforts required to protect personal data. Examples of physical measures an organisation may use to protect personal data: • Marking confidential documents clearly and prominently; • Storing confidential documents in locked file cabinet systems; • Restricting employee access to confidential documents on a need-to-know basis; • Using privacy filters to minimise unauthorised personnel from viewing personal data on laptops; • Proper disposal of confidential documents that are no longer needed, through shredding or similar means; • Implementing an intended mode of delivery or transmission of personal data that affords the appropriate level of security (e.g. registered post instead of normal post where appropriate); • Providing a summary of the personal data contained in storage so that personal data is accessed only when necessary; and • Confirming that the intended recipient of personal data is the correct recipient to avoid undue disclosure of personal data. Examples of technical measures an organisation may use to protect personal data:	

		• Ensuring computer networks are secure; • Adopting appropriate access controls (e.g. considering stronger authentication measures where appropriate); • Encrypting personal data to prevent unauthorised access; • Activating self-locking mechanisms for the computer screen if the computer is left unattended for a certain period; • Installing appropriate computer security software and using suitable computer security settings; • Disposing of personal data in IT devices that are to be recycled, sold or disposed; • Using the right level of email security settings when sending and/or receiving highly confidential emails; • Updating computer security and IT equipment regularly; and • Ensuring that IT service providers are able to provide the requisite sta	
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions	PART VI: DICTIONARY ATTACKS AND ADDRESS-HARVESTING SOFTWARE Prohibition on use of dictionary attacks and address-harvesting software Under section 48B, a person must not send, cause to be sent, or authorise the sending of any message, insofar as the recipient	

		telephone number is obtained by dictionary attack or address-harvesting. Under section 48A(1), "dictionary attack" means the method by which the telephone number of a recipient is obtained using an automated means that generates possible telephone numbers by combining numbers into numerous permutations. For instance, this would include randomly generating strings of 8-digit numbers, in running sequence or otherwise. This can happen even if the recipients have never published their telephone numbers. Section 48A(1) also defines "address-harvesting software" as software that is specifically designed or marketed for use for searching the Internet for telephone numbers and collecting, compiling, capturing or otherwise harvesting those telephone numbers. This happens where the recipients have published their telephone numbers. The primary responsibility lies with the organisation that sends the messages and employees are not liable if they are merely acting in the course of their employment. However, directors, partners27 or other officers 28 of similar level of seniority may also be held liable for their organisation's actions. For instance, an employee A receives instructions to send a message to a list of numbers that was given to him by his director B. He is not aware that the numbers were generated automatically through dictionary attack. While the sending of the	

		messages is prohibited by section 48B(1), section 48B(2) excludes him from the application as he sent the message in good faith, in accordance with instructions given to him in the course of his employment. However, his director B will not be excluded from the application of section 48B(1) as he falls under the meaning of an "officer" under section 48B(3)(b) read with section 52(7).	
26	Advisory Guidelines on Application of PDPA to Election Activities	Protection Obligation 4.20 A political party or election candidate must protect all personal data in its possession or under its control by making reasonable security arrangements to prevent (a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (e.g. cyber-attacks, hacking); and (b) the loss of any storage medium or device on which personal data is stored17. This includes, but is not limited to, protecting the personal data of individuals from whom they have received political donations, persons on the registers of electors, and potential voters. 4.21 Political parties and election candidates should also develop and put in place clear policies to ensure that the personal data of their employees (including election agents and volunteers) is protected.	Purpose Limitation Obligation 4.9 A political party or election candidate may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, have been notified to the individual concerned. 4.10 A political party or election candidate should specify purposes, which should be reasonable, at an appropriate level of detail that will allow the individual to determine the reasons the political party or election candidate is collecting, using or disclosing his or her personal data. To be clear, there is no need for the political party or election candidate to specify every activity that is undertaken in relation to collecting, using or disclosing personal data when notifying individuals of its purposes, provided that an appropriate level of detail is provided. 4.11 The Purpose Limitation Obligation similarly applies in situations where political parties or election candidates collect personal data from third party sources.

27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers	PART III: IMPLEMENTATION 6 Implementation timeframe 6.1 The interpretation of the PDPA in Part II of these Guidelines clarifies the applicable standard for the permissible collection, use or disclosure of NRIC numbers (or copies of NRIC) and retention of physical NRICs. To allow organisations time to review and implement any necessary changes to align their existing business practices and processes with these Guidelines, the PDPC will apply the interpretation of the PDPA in Part II of these Guidelines from 1 September 2019. Organisations collecting, using or disclosing NRIC numbers (or copies of NRIC) should continue to ensure that they protect personal data in their possession or control, in compliance with their obligations under the PDPA. 6.2 Organisations may refer to the Technical Guide to Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers for guidance on replacing the NRIC number for identifying individuals in websites and other public facing computer systems. 5 Alternatives to NRIC 5.1 PDPC does not prescribe the types of identifiers that organisations should adopt in place of NRIC numbers. Organisations should assess the suitability of alternatives to NRIC numbers based on their own business and operational needs. Some alternatives that have been adopted by organisations include organisation or user-generated ID, tracking number, organisation-issued QR code, or	

		monetary deposit. Organisations should also consider whether the alternatives provided are reasonable, and avoid collecting excessive personal data as an alternative to the individual's NRIC number (or a copy of NRIC). Partial NRIC numbers 5.2 PDPC recognises that organisations may wish to collect partial NRIC number when other alternatives are not satisfactory. PDPC considers that organisations that collect partial NRIC number up to the last 3 numerical digits and checksum of the NRIC number (e.g. "567A" from the full NRIC number of "S1234567A") in this manner would not be considered to be collecting the full NRIC number, and therefore not subject to the treatment for NRIC numbers set out in these guidelines. For more information on partial NRIC numbers, please refer to PDPC's Technical Guide to these Guidelines. 5.3 To be clear, partial NRIC numbers are considered personal data under the PDPA to the extent that an individual can be identified from the partial NRIC number, or from the number and other information to which the organisation has or is likely to have access17. The risks associated with the permanent and irreplaceable nature of the NRIC and the potential to unlock large amounts of information relating to the individual are diminished but still exist. These risks together with the safeguards put in place to protect the personal data in an organisation's possession will be taken into consideration by the PDPC in determining whether the collection, use or disclosure of partial NRIC numbers is	

		reasonable. Organisations that collect partial NRIC numbers must still comply with the Data Protection Provisions of the PDPA, such as making reasonable security arrangements to protect the data in their possession or under their control from unauthorised disclosure. 5.4 The following examples illustrate scenarios where the collection, use or disclosure of NRIC numbers (or copies of NRIC), as well as the retention of physical NRICs, is not required under the law, and some alternatives that organisations may consider adopting: 5.12 In certain circumstances, an organisation may merely have sight of an individual's physical NRIC and the information on it for verification purposes. Where there was no intention to obtain control or possession of the physical NRIC in checking the physical NRIC for the purpose of establishing or verifying the identity of the individual, and no personal data will be retained once the NRIC is returned immediately to the individual, PDPC does not consider it a collection of personal data on the physical NRIC.	
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		
29	Advisory Guidelines for Management Corporations	Estate security Visitors and invitees 3.14 The personal data of visitors and invitees (such as subcontractors) may be routinely collected for security purposes. This may be done in various	

		ways. For instance, visitors may be required to provide certain personal data to estate security, such as his or her name, vehicle number (where relevant), contact details and the unit number which he or she is visiting, by filling in a visitor log book at the guard house of a condominium or the reception desk of a commercial building, before being allowed to enter. There may also be CCTV images captured28 of the visitors and invitees. 3.15 MCSTs should only collect personal data that is necessary for the purpose and avoid collecting excessive personal data, taking into consideration what a reasonable person would consider appropriate in the circumstances. Ordinarily, having sight of a visitor's photo identification and recording the visitor's name and contact details (e.g. mobile number) would be considered reasonable for a condominium's security purposes. In exceptional circumstances, where a MCST assesses that the failure to accurately identify the visitor or invitee to a high degree of fidelity will pose significant security risks, it may be reasonable for the MCST to record the NRIC numbers of visitors to accurately establish and verify the identity of the individual. The MCST must be able to justify the recording of the NRIC numbers of visitors or invitees. Please refer to the Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers for more information. 3.16 The MCST must also comply with the obligation in the PDPA to make reasonable security arrangements to protect the personal data of visitors or	

		invitees from unauthorised use or disclosure. In doing so, MCSTs should take into consideration the nature of personal data, the form in which the personal data has been collected (i.e. physical or electronic), and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data. For example, a MCST that collects the name and NRIC numbers of invitees must have in place a greater level of security to protect such personal data (e.g. employing a visitor management system with appropriate technical measures to control access). This is in view of the risk to individuals if NRIC numbers, which could be used to unlock large amounts of information relating to the individual, were obtained and used for illegal activities such as identity theft and fraud. 3.17 Example: Collection of visitor's personal data Amber is visiting a friend at estate PQR. The security guard at the entrance notifies her of the need to record her vehicle number and contact details, for security purposes. She fills in the visitor log book accordingly. Amber is deemed to have consented to the collection, use or disclosure of her personal data under the PDPA. 3.18 Example: Collection and care of visitor's NRIC numbers Brandon is visiting a data centre at STU building. At the reception counter of building, he is asked to fill in his NRIC number, name and contact details in a visitor log book. While doing so, he is able to see the NRIC numbers, names and	

		contact details of all the other visitors. The visitor log book is placed on the counter, open and facing all visitors at the counter. The MCST of STU building has assessed and is able to justify that the collection of NRIC numbers is necessary to accurately establish and identify the identity of every visitor or invitee entering STU building to a high degree of fidelity as the failure to do so will pose significant security risks. The MCST should adopt appropriate security arrangements that would meet the higher level of protection that is required, such as implementing an electronic visitor management system and/or activating auto screen lock mechanisms for the computer screen if left unattended. 3.19 Example: Collection of visitors' partial NRIC numbers Jasmine is visiting a friend at estate VWX. The security guard at the entrance notifies her of the need to fill in the visitor chit with her name, contact number and partial NRIC number (i.e. last three digits and checksum of her NRIC number), for security purposes. After Jasmine fills in the visitor chit, the security guard checks her physical NRIC to verify the name and partial NRIC number provided. In this case, the MCST of VWX is not considered to have collected Jasmine's NRIC number. Nonetheless, the MCST must still comply with the Data Protection Provisions of the PDPA, including making reasonable security arrangements to protect the	

		personal data of visitors or invitees from unauthorised use or disclosure. 4 Protection and retention of personal data 4.1 The BMSMA does not prescribe the measures that MCSTs and managing agents28 should adopt to secure personal data in their possession or under their control. For example, the visitor log book, access card system, facilities log book, documents containing residents' feedback or complaints, and resident's portal are likely to contain personal data. Therefore, MCSTs and managing agents must comply with the Data Protection Provisions in the PDPA, and make reasonable security arrangements29 to protect such personal data in their possession or under their control to prevent accidental or unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Security arrangements may take various forms such as administrative measures, physical measures, technical measures or a combination of these. Please refer to Chapter 17 of the Advisory Guidelines on Key Concepts in the PDPA for more details on the considerations that apply in relation to the Protection Obligation, as well as examples of administrative, physical and technical measures. 4.2 MCSTs and managing agents must also have in place a retention policy that sets out when they cease to retain documents containing personal data (e.g. visitor entries in the log book)30. Under the Retention Limitation Obligation, the PDPA requires an	

		organisation to cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals (i.e. anonymise the data) as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data, and the retention of personal data is no longer necessary for legal or business purposes. In doing so, MCSTs and managing agents must ensure that there is proper and secure disposal of personal data. 4.3 In this regard, as part of their retention policies, MCSTs and managing agents may retain all records, books of account and such other documents relating to any transactions or operations for a period of not less than 5 years from the end of the financial year in which the transactions or operations to which those documents relate are completed, as required by the BMSMA.31 Beyond this period of retention, MCSTs and managing agents should assess on a standard of reasonableness, whether the purposes for which the personal data was collected is served, or if there are other legal or business purposes for which retention of the personal data may be necessary.32 4.4 Please refer to the Guide to Disposal of Personal Data on Physical Medium and the Guide to Securing Personal Data in Electronic Medium for more information on good practices for disposing personal data in physical forms and protecting electronic	

		personal data. 4.5 Example: Documents containing personal data The MCST of estate ABC requires all visitors to record their name, contact details and vehicle licence plate number (where relevant) in the visitor log book located at the security guardhouse situated at the entrance of the estate. The MCST has engaged security staff to be present at the guardhouse around the clock. However, a regular visitor to the estate observed that there were several instances where the guardhouse was left unattended by the security staff, and the visitor log book, which contains personal data of visitors, was left unattended for anyone to access during these periods. The MCST is required to comply with the obligations in the PDPA, including making reasonable security arrangements to protect the personal data in its possession or under its control from loss, misuse or unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Residents or visitors to the estate should not be able to access the personal data of other visitors in the visitor log book, and the MCST should ensure that the visitor log book is kept in a secure place that is only accessible to authorised personnel. In addition, the MCST should have in place a personal data retention policy that governs when it should cease to retain documents such as entries in the visitor log book, which are likely to contain	

		personal data. When ceasing to retain these documents, the MCST would also need to establish processes to ensure the proper and secure disposal of these documents. For the avoidance of doubt, if the security staff are appointed or engaged as data intermediaries to process personal data on behalf of and for the purposes of the MCST, the security staff processing personal data on behalf of and for the purposes of the MCST pursuant to a contract which is evidenced or made in writing will only be subject to the Protection Obligation and Retention Limitation Obligation while the MCST remains fully responsible for complying with all the Data Protection Provisions. Minutes of meeting 3.3 Apart from general meetings of the MCST, MCST councils and executive committees are also required to hold their respective meetings. Under the BMSMA, the council or executive committee of the MCST is required to "cause minutes of general meetings to be kept" 22, as well as keep "full and accurate minutes" of its proceedings23. Since the function and purpose of the minutes of meetings are to accurately record what happened at the meeting, the minutes could include the personal data of estate residents or invitees to identify and record the persons in attendance24 or arising from discussions on matters relating to these individuals during the meetings. Further, the council or executive committee	

		must display a copy of the minutes of its meeting as well as the minutes from the MCST's general meeting on the estate's notice board for a period of not less than 14 days.25 The council may also give each subsidiary proprietor a copy of the minutes after the meeting.26 Personal data captured in the minutes may therefore be disclosed as a consequence. As a good practice, MCSTs should take care to display the minutes of meeting for a reasonable duration and not display it for a longer period than necessary. 3.4 As good practice, MCSTs should notify all subsidiary proprietors and estate residents (particularly new residents) that their personal data will be collected for the dissemination of the minutes of meetings and the voter list in accordance with the BMSMA. This could be done through the MCST's personal data protection policy, or notice of general meeting. 3.5 Example: Minutes of Meeting Following estate GHI's MCST general meeting, the council posted the minutes of meeting on the notice board in the estate as required under the BMSMA. The minutes recorded the discussion surrounding a complaint made by one of the residents in the estate, against another resident. The resident noticed that her name and unit number was disclosed in the minutes, and asked the MCST council about this. The MCST explained to the resident that the BMSMA requires full and accurate minutes of the meeting to be captured and posted. All	

		subsidiary proprietors and residents of estate GHI had also been informed of this requirement through the MCST's personal data protection policy that is available on its website. 3.6 Example: Recording of proceedings to ensure full and accurate minutes of meeting For estate GHI's MCST general meeting, MCST council members wish to take audio recordings of the proceedings of general meeting for the purpose of ensuring that full and accurate minutes of the meeting are captured. As audio recordings may capture more personal data than is necessary for the recording of full and accurate minutes of meeting, the MCST must notify subsidiary proprietors and residents, such as through the MCST's personal data protection policy or notice of general meeting, that audio recordings of the proceedings will be taken during the meeting. Deemed consent for such audio recordings to be taken would be considered to have been given by the attendees of the meeting. The MCST should only use the audio recordings for the purpose of ensuring that full and accurate minutes of meeting are captured. While there are no provisions in the BMSMA that address this issue, the MCST must comply with other Data Protection Provisions of the PDPA. Subsidiary proprietors 3.20 Typically, estate residents in a residential building, and/or certain invitees of a commercial building (such as employees of an occupier), may enter and leave the estate premises using	

		access cards. In the application for access cards and/or the maintenance of the access cards system, MCSTs may require the contact details (i.e. names, telephone numbers and email addresses) of the individuals who hold access cards. 3.21 MCSTs must ensure that the individuals provide their consent (or deemed consent) for the collection, use or disclosure of their personal data for the purpose of providing them access through the use of access cards, in compliance with the PDPA. Photographs or video recordings of social activities 3.22 From time to time, MCSTs may organise social functions or activities for estate residents. Where MCSTs intend to take and use photographs or video recordings of estate residents, visitors or invitees attending these events for a purpose, MCSTs must notify and obtain consent from these individuals to collect, use or disclose their personal data for the purpose. For example, organisers of social activities should notify participants that photographs of them may be taken at the event for the purpose of publishing them in an estate newsletter or annual general meeting presentation, and provide information about how they may withdraw consent. 3.23 The Data Protection Provisions do not prescribe the ways in which consent may be obtained. MCSTs may do so in the most effective way depending on the circ	
30	Advisory Guidelines for the Education Sector		2 The Consent, Purpose Limitation and Notification Obligations 2.1 The Commission understands that an education

			institution5 may collect, use or disclose a student's personal data for purposes such as to provide the student with education services, to evaluate the student's suitability for a course, or to administer bursaries, scholarships and relevant financial assistance schemes to eligible students. The Commission recognises that the purposes for the collection, use or disclosure of personal data may differ across education institutions. Organisations should, therefore, notify and specify purposes at an appropriate level of detail that will allow an individual to determine the reasons that the education institution is collecting, using or disclosing his/her personal data. Education institutions are encouraged to consider factors such as the specific facts of the case, business and operational needs, and to refer to the Advisory Guidelines on Key Concepts in the PDPA ("Key Concepts Guidelines") for more information on providing notification and on stating purposes. 2.2 The Data Protection Provisions in Parts III to VI of the PDPA set out the obligations that organisations are required to comply with if they undertake activities relating to the collection, use or disclosure of personal data6. Among other things, organisations are required to obtain valid consent from the individual for a limited purpose that has been notified to the individual for the collection, use and disclosure of personal data of the individual, unless exceptions apply7. Considerations in obtaining consent

			2.3 The PDPC does not prescribe the manner in which consent should be obtained by an organisation under the Data Protection Provisions. An education institution may decide on the most suitable way to obtain consent in accordance with the PDPA, and may refer to the Key Concepts Guidelines for more information on considerations and good practices when obtaining consent from an individual. 2.4 In relation to the Consent Obligation, prior to collecting, using or disclosing personal data about an individual, an education institution should consider: a) Whether the individual (or a person who has the legal authority to validly8 act on behalf of the individual) had been notified of the purposes for the collection, use or disclosure of his personal data and had given consent to such collection, use or disclosure; b) If consent had not actually been given, whether consent can be deemed to have been given by the individual (or a person who has the legal authority to validly act on behalf of the individual) for the collection, use or disclosure of his personal data for the purpose; and c) Whether the collection, use or disclosure without the consent of the individual is required or authorised under the PDPA or any other written law, and assess whether the circumstances fall within any of the exceptions from the Consent Obligation in the Second, Third or Fourth Schedules to the PDPA. 2.5 The Commission is aware

			that, depending on the nature of their education product or service and demographics of their students, some education institutions may collect, use and disclose the personal data of minors and would accordingly have to obtain consent under the PDPA. Please refer to the Advisory Guidelines on Selected Topics ("Selected Topics Guidelines") for more information relating to considerations when obtaining consent from minors. 2.6 Example: Disclosure of personal data for school buddy orientation programmes Ella is a student currently pursuing a course at School ABC. School ABC intends to pair Ella with an incoming international student under an orientation programme which matches existing students with incoming students and their families, and wishes to disclose Ella's personal data (such as name, age, interests and contact details) to Ella's potential buddy. School ABC should obtain Ella's consent before disclosing her personal data for such a purpose. For avoidance of doubt, School ABC may notify Ella and seek her consent using various avenues and platforms. For example, when collecting Ella's personal data during the enrolment process, School ABC could include a notification in the enrolment forms that the personal data of enrolled students may be used and disclosed to third parties for school-related activities or programmes, such as "buddy systems" for new students, and consent can be obtained via the

			same forms. 2.7 Example: Disclosure of personal data of minors for school field trip A pre-school, ABC, is organising a field trip to the zoo for its students. Pre-school ABC needs to disclose the participants' personal data to the zoo for the purpose of arranging the field trip programme. Generally, Pre-school ABC should obtain consent from the parent or other legal guardians of each student, as a pre-school student would not have legal capacity to give consent. 2.8 Example: Disclosure of personal data to another parent Sue and John are friends whose daughters attend School ABC. One day, Sue is required to attend a meeting at the last minute and she is unable to pick up her daughter, Vera, at school. Sue calls John to pick Vera up on her behalf and send her home. John arrives at the school, informs School ABC that he is picking up Vera as well, and asks School ABC for Vera's home address. In this situation, in the absence of other forms of verification, School ABC should ensure that consent is obtained for the disclosure of Vera's personal data (e.g. home address) for such a purpose. For example, School ABC could make a call to Sue to confirm her agreement to disclose Vera's address to John. 2.9 Example: Disclosure of students' personal data for marketing purposes School ABC would like to publish the names and photographs of

			its top students and renowned alumni in its marketing collateral. As the names and photographs of these individuals are considered personal data relating to them, School ABC should obtain consent from these individuals to use and disclose their personal data for the marketing purposes. 2.10 Example: Disclosure of starting salaries of alumni School ABC conducts a survey on the employability of its alumni. The survey is conducted primarily via email, and personal data of School ABC's alumni are obtained through the survey such as their full names, student registration numbers, field(s) of study, the sector they are currently employed in, and their starting salaries. In the survey, School ABC states that the purpose of the survey is for School ABC to manage career services for its existing students. Organisation DEF, targeting high net worth individuals for their investment services, asks School ABC for a list of alumni who earn more than $X a month, their contact details and salary range in order to contact them to offer investment services. As this would be a different purpose from which the personal data was collected for, School ABC is required to obtain fresh consent from its alumni to disclose their personal data to Organisation DEF for their purposes. Organisation GHI produces a report each year on the starting salaries of fresh graduates in each industry sector and asks School ABC for

			the salary details of its recently-graduated alumni. As this would be a different purpose for which the personal data was collected, School ABC is required to obtain fresh consent from the alumni to disclose their personal data to Organisation GHI for their purposes. School ABC may also consider whether the data required could be anonymised, for example by removing personal identifiers, and aggregating data points so that unique individuals cannot be identified from the data. School ABC should also consider factors which may pose a challenge in keeping data anonymised. Please refer to the chapter in the Selected Topics Guidelines relating to Anonymisation for more information. When consent may be deemed 2.11 An individual is deemed to consent to the collection, use and disclosure of his personal data for a purpose if the individual voluntarily provides the personal data to the organisation for that purpose and it is reasonable that the individual would do so. 2.12 In a situation where an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organisation to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation. 2.13 Although organisations may rely on deemed consent instead of obtaining actual

			consent from the individual, it is good practice for an organisation to review its business processes to determine the situations where it should obtain actual consent instead of relying on deemed consent. 2.14 When it is unclear whether consent may be deemed, organisations should obtain consent from the individual to collect, use or disclose his personal data (as the case may be) for the relevant purposes in order to avoid any dispute over whether consent was given. 2.15 The following examples illustrate situations where the Consent Obligation applies. Please also refer to the Key Concepts Guidelines for more information on the Consent Obligation. 2.16 The following examples illustrate situations where consent may be deemed to have been given. 2.17 Example: Personal data collected for security purposes As part of its security measures, School ABC requires visitors to the school to sign up for a visitor pass at the security guard house. Visitors are requested to provide their full name, NRIC/passport number, contact number and state the purpose for their visit. School ABC is required to comply with the Data Protection Provisions when collecting, using and disclosing personal data. An individual is deemed to have given consent to School ABC's collection of his/her personal data for security purposes if the individual provides his/her personal data voluntarily for the

			purpose. As good practice, to ensure that the individual is aware of the purpose, School ABC may place a prominent sign at the reception desk indicating that visitors' details will be collected for security purposes. 2.18 Example: Personal data provided as administrative contact Jack signs up his son, Mack, for a one-day swimming camp organised by School ABC. In the registration form, Jack writes down his own name and mobile phone number for School ABC to contact him for the purpose of his son's participation in the camp. As Jack had voluntarily provided his name and contact details, he is deemed to have consented to School ABC's collection, use or disclosure of his personal data for such purposes. Should School ABC wish to use or disclose Jack's personal data for another purpose (for which consent had not been given or deemed to have been given), the school will need to separately obtain consent from Jack for that other purpose, unless an exception applies. 5 Organisations and Data Intermediaries 5.1 In some situations, education institutions may engage data intermediaries to process personal data. The PDPA provides that a data intermediary12 that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will only be subject to the Protection

			Obligation and Retention Limitation Obligation and not any of the other Data Protection Provisions. 5.2 A data intermediary remains responsible for complying with all Data Protection Provisions in respect of other activities that do not constitute processing of personal data on behalf of and for the purposes of another organisation that is pursuant to a contract evidenced or made in writing. 5.3 In any case, under section 4(3) of the PDPA, the organisation that engages the data intermediary would still have the same obligations under the PDPA in respect of personal data processed on its behalf as if the personal data were processed by the organisation itself. 5.4 Please refer to the Key Concepts Guidelines which provide further elaboration on when an organisation is considered a data intermediary and the obligations applicable to data intermediaries under the PDPA. 5.5 Example: Provision of transport services School ABC has a written contract with an external Vendor JKL for the provision of transport services to School ABC's students. Among other things, the contract between School ABC and Vendor JKL specifies that Vendor JKL will use personal data of School ABC's students provided by School ABC for the sole purpose of providing transport services on behalf of ABC to these students. Tina is a student currently pursuing a course with ABC. Tina wishes to sign up for transport services provided by School ABC through Vendor JKL.

			Tina provides her personal data by completing the form prepared by School ABC, and ticks the box on the form to give School ABC consent to disclose her personal data to the Vendor JKL for the purpose of arranging the transport services. Vendor JKL will be considered a data intermediary processing Tina's personal data on behalf of and for the purposes of School ABC pursuant to a written contract in relation to the provision of transport services to Tina. In this instance, Vendor JKL will be subject only to the Protection Obligation and the Retention Limitation Obligation, while School ABC will have the same obligations under the PDPA in respect of Tina's personal data processed on its behalf by Vendor JKL, as if the personal data were processed by School ABC itself. 5.6 Example: Engaging a consultancy firm to conduct a survey School ABC has engaged the services of consultancy Firm DEF via a contractual agreement to conduct an email survey among its upcoming cohort of graduates. The purpose of the survey is to study student perceptions on job placement quality, and quality of training. School ABC will use the survey findings to refine its existing policies on job placement and training. According to the terms of the agreement with School ABC, School ABC will provide Firm DEF with a list of graduate students containing their full names, student matriculation numbers, and

			field(s) of study. Firm DEF will categorise the graduates according to their fields of study and then contact them by email to conduct the survey. Following the completion of the email survey, Firm DEF is required to return the list containing the graduate students' personal data and all survey results to School ABC. In this case, Firm DEF will be considered a data intermediary of School ABC when processing students' personal data for the purpose of the email survey. Firm DEF will be subject only to the Protection Obligation and the Retention Limitation Obligation in relation to such processing, while School ABC will have the same obligations under the PDPA in respect of personal data processed on its behalf by Firm DEF, as if the personal data were processed by School ABC itself. 5.7 There are several obligations within the Data Protection Provisions which require organisations to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. Organisations are required to make the information about their data protection policies available. For more information, please refer to the Key Concepts Guidelines and the Selected Topics Guidelines. 6 Rights and obligations, etc under other laws 6.1 Section 4(6) of the PDPA states that unless otherwise provided in the PDPA, nothing in Parts III to VI of the PDPA shall

			affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening the PDPA, and the provisions of other written law shall prevail to the extent that any provision of Parts III to VI is inconsistent with the provisions of that other written law. 6.2 Section 13(b) of the PDPA provides that an organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual without the consent of the individual unless the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under the PDPA or any other written law. 6.3 There are several provisions under the Private Education Act and Regulations that empower the CPE to obtain information (including personal data) from registered PEIs. These provisions include, but are not limited to, the following: a) Section 57 of the Private Education Act provides that an inspector of the CPE may during an inspection of a registered PEI require any person to, amongst others, furnish any information which is within the power of the person to furnish relating to such matters as the inspector may specify. b) Section 62 of the Private Education Act provides that the CPE may issue a requisition to any person to furnish such particulars or supply such information relating to any matter to which the Act applies

			as may be specified in the requisition. c) Regulation 22 of the Private Education Regulations provides that the managers of a registered PEI shall prepare and submit to the CPE, by the 31st day of December of each year, an annual report on the activities and affairs of the PEI in that year. This includes, but is not limited to, personal data on the managers, academic/examination board members, teachers as well as students of the registered PEI. 6.4 Section 19 of the PDPA provides that notwithstanding the other provisions of Part IV of the PDPA, an organisation may use personal data collected before the appointed day for the purposes for which the personal data was collected, unless consent for such use is withdrawn or the individual has indicated to the organisation that he does not consent to the use of the personal data. Such 'use' could include disclosure that is necessarily part of the organisation's use of such personal data. For avoidance of doubt, the Do Not Call Provisions will apply to the sending of specified messages to Singapore telephone numbers, even if the Singapore telephone numbers are collected before the appointed day. PART III: APPLICATION OF THE DO NOT CALL PROVISIONS TO SCENARIOS FACED IN THE EDUCATION SECTOR The following examples outline the application of the Do Not Call Provisions and the Personal Data Protection (Exemption from Section 43) Order (S.817/2013)

			("Exemption Order"). They address particular aspects of the PDPA, and are not meant to exhaustively address every obligation in the PDPA that would apply in that scenario. In particular, they do not illustrate the application of the Data Protection Provisions, which were addressed earlier in these Guidelines. 7 The Do Not Call Provisions 7.1 Messages with a purpose to offer to supply, advertise or promote goods or services, land or an interest in land, or a business or investment opportunity, or a supplier of such goods, services, land or opportunity are specified messages and the Do Not Call Provisions will apply to such messages. Messages which do not have any of the purposes listed above will not be considered specified messages. The Eighth Schedule to the PDPA sets out exclusions from the meaning of "specified message" that relate to, among others, any "business-to-business" marketing message, any message sent by a public agency under, or to promote, any programme carried out by any public agency, which is not for commercial purpose, any message the sole purpose of which is to conduct market research or market survey, and other types of information specified in the Eighth Schedule. 7.2 The Do Not Call Provisions apply to a specified message addressed to a Singapore telephone number if the sender of the specified message is present in Singapore when the specified message is sent or the recipient of the specified message is present in

			Singapore when the specified message is accessed. 7.3 One significant obligation under the Do Not Call Provisions is that the organisation sending the specified message will have to check the Do Not Call Registers as described above, unless: a) the user or subscriber of the Singapore telephone number has given clear and unambiguous consent in written or other accessible form to the sending of the specified message to that number; or b) the organisation is exempted from complying with its obligation under the Exemption Order. 7.4 Under the Exemption Order, a sender that is sending a specified fax message or a specified text message to a Singapore telephone number related to the subject of an ongoing relationship between the sender and a recipient is exempted from the requirement to check the relevant Do Not Call Registers, if certain conditions are met. An "ongoing relationship" under the Exemption Order means a relationship which is on an ongoing basis, between a sender and a subscriber or user of a Singapore telephone number, arising from the carrying on or conduct of a business or activity (commercial or otherwise) by the sender. The Exemption Order does not apply to voice calls and a sender is still required to check the Do Not Call Register before making any telemarketing calls to promote related products or services. The Advisory Guidelines on the Do Not Call

			Provisions provide further elaboration. 7.5 In determining what constitutes an ongoing relationship, the Commission considers one-off interactions or transactions in themselves to be insufficient to be an ongoing relationship. For example, the fact that an individual previously contacted the education institution to enquire about upcoming courses or programmes once, or attended an open house organised by the education institution once, by themselves, would be insufficient to establish an ongoing relationship between the individual and the sender. 7.6 Examples: Whether messages are specified messages13 School ABC is conducting an annual walkathon. (a) School ABC sends an SMS inviting students to attend the annual walkathon. To the extent that the walkathon does not offer to supply a good or service or have any of the other purposes listed in the definition of a specified message, School ABC would not be sending a specified message, therefore the Do Not Call Provisions would not apply. (b) In conjunction with "Healthy Week", School ABC calls to inform students about an upcoming seminar by a shoe retailer on choosing the right shoes for the walkathon. As the seminar involves promoting a supplier, School ABC is likely to be sending a specified message and the Do Not Call

			Provisions will apply. (c) School ABC calls all parents of students to be chaperones at the walkathon. Such messages will not be considered "specified messages" under the PDPA to the extent that they do not involve marketing of any good or service. Hence, the Do Not Call Provisions do not apply.(d) School ABC sends an SMS to thank all parents who volunteered in the walkathon. School ABC is not sending a specified message and the Do Not Call Provisions do not apply. 7.7 In the upcoming school term, School ABC will be organising a school trip to Country XYZ as part of its efforts to enhance students' understanding of history and architecture. School ABC sends an SMS to students announcing the school trip, and possible travel insurance packages offered by various companies available to interested students. In this case, School ABC is considered to be sending a specified message as the SMS was also promoting travel insurance packages from different vendors to students. Hence, the Do Not Call Provisions will apply. 7.8 School DEF sends an SMS to students providing them administrative details of an upcoming examination, such as date, timing, venue and instructions for candidates to bring along their student matriculation card for verification purposes. School DEF is not sending a specified message, and the Do Not Call Provisions do not apply.

			7.9 School ABC calls Albert to remind him of the deadline to settle his tuition fees. In this scenario, School ABC is not sending a specified message, and the Do Not Call Provisions do not apply. 7.10 School ABC sends an SMS to students announcing cancellation of outdoor classes due to inclement weather. School ABC is not sending a specified message, and the Do Not Call Provisions do not apply. 7.11 The following examples illustrate the application of the Exemption Order. 7.12 Examples: Application of the Exemption Order School ABC will be introducing new language courses over the next year. (a) Jim previously enquired with School ABC on another course, and had no further interaction with School ABC thereafter. In this case, School ABC cannot rely on the Exemption Order to send a text or fax message marketing its new programmes to Jim as his enquiry was considered a one-off interaction. (b) Tracy, a former student of School ABC, has joined School ABC's alumni network, which receives regular email updates from School ABC on schoolrelated news including new courses and events open to alumni. School ABC may rely on the Exemption Order to send Tracy text or fax messages containing information about its new language courses. (c) Jason enrols his daughter, Jasmine, in a language course conducted by School

			ABC. In the enrolment form, Jason provides his name and Singapore telephone number as "parent contact information", which School ABC requires for the purposes of sending administrative updates about the course. In this case, the fact that Jason enrolled his daughter and provided his contact information, on its own, does not give rise to an ongoing relationship between him and School ABC. The on-going relationship is generally established between School ABC and Jasmine. School ABC should thus obtain clear and unambiguous consent, evidenced in written or any other form, from Jason if it wishes to send specified messages (e.g., such as promoting the new language courses) to Jason's telephone number. If School ABC wishes to rely on any ongoing relationship to send specified messages under the Exemption Order to Jason, School ABC would need to consider if there are relevant factors that establish an ongoing relationship between itself and Jason.
31	Advisory Guidelines for the Social Service Sector	6 The Protection Obligation 6.1 The PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control to prevent (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on	3 The Consent, Purpose Limitation and Notification Obligations 3.1 The Commission understands that SSAs may collect, use or disclose a client's personal data including full name, NRIC number, contact details, financial and family situation, medical history, etc. for purposes such as evaluating the client's suitability

		which personal data is stored. 6.2 There is no 'one size fits all' solution for organisations to comply with the Protection Obligation. Generally, SSAs should consider factors such as the nature of the personal data in their possession who or under their control (as the case may be), and the adverse impact to individuals if an unauthorised person obtained, modified, or disposed of the personal data, to determine the security arrangements that are reasonable and appropriate in the circumstances. 6.3 Please refer to Chapter 17 of the Key Concepts Guidelines for more information relating to the Protection Obligation, and more examples of security arrangements. The following examples illustrate the application of the Protection Obligation. 6.4 Example: Protecting personal data that has been collected SSA XYZ operates a day activity centre for senior citizens. As part of its security procedures, SSA XYZ requires all visitors to the centre to sign up for a visitor pass at the reception. Visitors are requested to provide their name and contact number in order to be issued a visitor pass. SSA XYZ records such information in their visitor management system which contains a database for visitors. Treatment SSA XYZ should consider the specific circumstances when assessing whether it is reasonable to collect the personal data of visitors to their premises. Generally, SSA XYZ is required to	for social services or administering social services to the clients. 3.2 The PDPA requires organisations to, among other things, notify an individual of the purposes for the collection, use and disclosure of his personal data2 and obtain his consent, unless any relevant exception to consent3 applies. Moreover, organisations shall only collect, use and disclose personal data that are relevant for the purposes, and for purposes that a reasonable person would consider appropriate in the circumstances. 3.3 Section 16 of the PDPA provides that individuals may at any time withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose by an organisation. Please refer to the Advisory Guidelines on Key Concepts in the PDPA (Chapter 12) for the requirements that must be complied with by either the individual or the organisation in relation to the withdrawal of consent. However, the organisation can continue to use and disclose personal data in their possession if allowed under other provisions. 3.4 The Commission is aware that, depending on the nature of their services and demographics of the client or beneficiary, some SSAs may collect, use or disclose the personal data of minors and would accordingly have to obtain consent under the PDPA. Please refer to the Advisory Guidelines on Selected

		comply with the Protection Obligation in respect of the personal data recorded in the visitors' database. Security arrangements implemented by organisations may take various forms such as administrative measures, physical measures, or technical measures. In the case of SSA XYZ, for example, an administrative measure would be to design the visitor digital database on the laptop such that the visitor keying in their personal data is unable to view the personal data of other visitors. SSA XYZ avoids using a visitors' excel sheet where visitors may view the personal data of other visitors when keying in the excel sheet. Other administrative measures include restricting employee access to the visitors' database on a need-to-know basis and using privacy filters to minimise unauthorised persons from viewing the personal data on the laptop. Technical measures that SSA XYZ can implement would be password-encrypting the visitors' database and activating self-locking mechanisms for the laptop screen if the laptop is left unattended for a certain period of time. 6.5 Example: Protecting personal data collected through a website SSA ABC operates an online portal which allows individuals to sign up as volunteers. The registration process involves the collection of personal data of individuals who sign up, such as their full names, mobile numbers and email addresses. Treatment	Topics ("Selected Topics Guidelines") on "data activities relating to minors" for more information relating to persons who may exercise rights or powers under the PDPA, and considerations when obtaining consent from minors. 3.5 The following will highlight how consent may apply in common social service scenarios, how deemed consent applies as well as the exceptions to consent. 3.6 Examples: Using personal data SSA ABC arranges with Company XYZ such that the purpose and amount needed for donations to SSA ABC are listed on Company XYZ's public website. Company XYZ has a database of regular donors to whom it sends emails to solicit donations on a periodic basis. The donors could choose to donate to SSA ABC by referring to the instructions on Company XYZ's website and provide their financial information to Company XYZ for processing of the transaction. Before proceeding, donors will indicate their consent to disclosing their personal data to SSA ABC when they donate through Company XYZ for purposes such as issuing tax deductible receipts to their email address. Treatment In processing the financial transaction from donors on its website, Company XYZ is considered to have collected, used and disclosed personal data. By receiving personal data of donors from Company XYZ, SSA ABC is considered to have collected and

		SSA ABC is required to comply with the Protection Obligation by making reasonable security arrangements to protect the personal data collected by SSA ABC through the portal. An example of a technical measure which SSA ABC could adopt would be to encrypt all personal data captured through the registration process before it is being transferred to SSA ABC's local database for storage. 6.6 Example: Protecting personal data in photographs taken John, a volunteer at SSA ABC, is assisting SSA ABC to organise a gathering for its clients, donors and volunteers at its centre. As John is an avid photographer, SSA ABC requests John to take photographs of the event, so that SSA ABC can post them on its official website and official social media network accounts. SSA obtains the requisite consent from those attending the event for their photographs to be taken for these purposes. Subsequently, John intends to use some of the unpublished photographs from SSA ABC's event to create a montage and post it on his personal social media network profile page. Treatment Even as a volunteer, John is regarded as an employee of SSA ABC under the PDPA. As John was acting as an employee within the meaning of the PDPA when taking the photographs, the unpublished photographs belong to SSA ABC and John should not share them on his personal account without explicit consent from SSA ABC18 .	subsequently used the personal data. Accordingly, Company XYZ and SSA ABC will have to comply with the PDPA in respect of such collection, use and disclosure. 3.7 SSA DEF engages Company GHI for online on its upcoming programmes and events as sponsored social media posts. No individuals' personal data is given to Company GHI for generating the social media posts. The posts appear in the social media feed of users in a random manner. Treatment In this case, neither SSA DEF nor Company GHI would be considered to have collected or used the personal data of the users. Hence, both SSA DEF and Company GHI would not be subject to the Data Protection Provisions for this set of activities. 3.8 2 . 8 Example: Clients voluntarily giving their personal data for welfare services Seniors' activity centre ABC gives out free food items to senior citizens by leaving them at the door of the activity centre for self-collection by the senior citizens. There is a notice pasted at the door of the activity centre indicating that the seniors can leave their contact details if they are interested to be contacted for seniors' programmes, free or subsidized healthcare or financial support. To ensure that the personal data of the interested seniors are not shown to the public, interested seniors will fill

		SSA ABC should implement reasonable security arrangements to safeguard itself against such risks. For example, SSA ABC may implement policies and procedures (e.g. disciplinary measures in the event of breaches) for employees to ensure protection of the personal data in its possession or under its control, including photographs taken of the SSA's clients, donors and volunteers and/or conduct training for employees to impart good practices on handling personal data. Please refer to Chapter 17 on the Protection Obligation in the Key Concepts Guidelines for more information. 6.7 Example: Reasonable security arrangements to protect elderly clients' personal data SSA ABC engages volunteers to distribute care packs to the homes of more than 200 elderlies all over Singapore. The volunteers will need access to the personal data of the elderly clients (e.g. names, home addresses and phone numbers). To comply with the Protection Obligation, SSA ABC puts in place reasonable security arrangements, such as administrative and physical measures etc., to protect the elderly clients' personal data after assessing the nature of personal data in its possession and the possible impact to the elderly clients concerned if the data is obtained by an unauthorised person. For instance, SSA ABC only allows volunteer access to personal data on a need-to-know basis and ensures	in their names and contact details in a blank form placed at the door of the activity centre. They will drop the completed form inside a metal box that can only be accessed when the appropriate personnel from Seniors' activity centre ABC uses a key to open the lock on the box. On the form, there is a question clearly asking the seniors' consent for collection, use and disclosure of their personal data for the specific purpose and a checkbox beside the question for seniors to tick. Treatment If the senior citizen were to fill in their names and contact details in the blank form and indicated at the checkbox that they consent to the collection, use and disclosure of their personal data for the specified purpose, Seniors' activity centre ABC has obtained express consent from the interested seniors. The consent is obtained in writing and provides the clearest indication that the individual has consented to the notified purposes of the collection, use or disclosure of their personal data. Seniors' activity centre ABC must ensure that the words on the notice and on the form are clear and noticeable, so that there is a higher certainty that the seniors would read and understand the purpose of the collection, use and disclosure of their personal data. By taking measures to ensure that the personal data left by interested seniors are not accessible to the public (e.g. using a metal box that can only

		that each volunteer holds only an appropriate amount of the personal data. Volunteer leaders are assigned to each district, and only holds the data of elderly clients in that district. Volunteer leaders will further delegate the work of distributing care packs among the volunteers under them and only provide required personal data of elderly clients to the volunteers (e.g. a pair of volunteers only delivers care packs to five homes, so they only hold the personal data of elderly clients living in those homes). To reduce the risk of personal data being leaked (e.g. elderly clients' personal data accidentally forwarded to unrelated third parties), SSA ABC provides the personal data of the elderly only on the day of distributing the care packs and in hardcopy. After the care packs have been distributed, the volunteers are to return the hardcopy papers of the elderly clients' personal data to the volunteer leaders, who will properly dispose of the documents. SSA ABC sometimes uses messaging platforms (e.g. WhatsApp) to communicate with volunteers and send volunteers the personal data of clients via a photograph for distribution of care packs to their homes. SSA ABC only sends the photograph on the day of distributing the care packs, and instructs the volunteers to delete the photograph from their phones and their "recently deleted" folder after the care packs have been distributed. Alternatively, for added security,	be opened by authorised persons), Seniors' activity centre ABC has also complied with the Protection Obligation of the PDPA. 3.9 Example: Collection, use, and disclosure of personal data for client surveys SSA ABC intends to conduct a survey on the impact of its services on individual clients, which involves the collection and use of personal data (including clients' full names, contact details and income levels). SSA ABC intends to publish the results of the survey in a manner that identifies the individual clients4 in their annual report and on their website. Treatment SSA ABC must obtain consent from the individual clients to collect, use and disclose their personal data before conducting the survey, unless an exception applies. If SSA ABC intends to use or disclose personal data that had previously been collected for other purposes for this survey, SSA ABC may wish to consider whether the exception for use or disclosure of personal data without consent for research in Division 35 of Part 2 of the Second Schedule or Division 26 of Part 3 of the Second Schedule respectively would apply. 3.10 Example: Disclosure of clients' personal data to a third party SSA ZYX receives an email request from a neighbourhood grassroots club for a list of SSA ZYX's needy clients and their addresses in order for the grassroots club to deliver

		SSA ABC may upload the personal data of the clients on a system, where volunteers can only view the data but not download into their phones. It is advisable for SSA ABC to implement measures in selecting and training the volunteer leaders, who hold higher responsibility in handling the personal data of elderly clients. SSA ABC shall also conduct basic data protection training for all their volunteers, and ensure volunteer leaders supervise the volunteers under them. Under the PDPA's Accountability Obligation, organisations are responsible for personal data in their possession or control. As volunteers are considered as employees of an organisation for the purpose of the PDPA, SSA ABC is required to provide training for its volunteers and communicate to its volunteers information about its policies and procedures.	some food rations to these clients. Treatment The Data Protection Provisions will generally apply to SSA ZYX's disclosure of its clients' personal data to the grassroots club. Among other things, consent would be required for such disclosure unless an exception applies, such as when the disclosure is necessary for any purpose which is clearly in the interests of the individual, if consent for its disclosure cannot be obtained in a timely way. Please refer to Chapter 12 of the Key Concepts Guidelines on the "Consent Obligation" for more information. Deemed consent 3.11 Deemed consent by conduct: In situations where an individual (without actually giving consent) voluntarily provides his personal data to an organisation for an appropriate purpose, and it is reasonable that he would voluntarily provide the data, the individual's consent to the collection, use or disclosure of personal data is deemed to have been given by the individual's act of providing his personal data. 3.12 Example: Consent for photo-taking at a private function for clients SSA GHI hosts a private dinner function for families and engages a volunteer photographer to take photographs of attendees for its newsletter. SSA GHI does not explicitly ask the families for consent to take their photographs for the newsletter. However, in this context, consent is deemed to

			have been given when the individual voluntarily permits a photograph or video recording to be taken of him for SSA GHI's intended purpose, and it is reasonable that he would do so (e.g. the individual voluntarily stands in the frame of the photographer's camera without objection). The measures that SSA GHI may take to better ensure that the attendees are aware of the purpose for which their photographs are collected, used and disclosed, could include: a) Clearly stating in its invitation to families that photographs of attendees will be taken at the function for publication in its newsletter; and b) Putting up an obvious notice at the reception or entrance of the function room to inform attendees that photographs will be taken at the event for publication in its newsletter. After seeing the notice at the reception, Mary informed the staff manning the reception that she does not want her photograph to be taken for publication in the newsletter. To facilitate Mary's refusal for her photograph to be taken, the reception staff gives her a lanyard of a different colour from the rest of the participants. This is so that the volunteer photographer can easily identify Mary, to avoid taking her photograph and publishing her photograph in SSA GHI's newsletter. Barry, who was initially deemed to have consented to his photograph being taken during the private function and published in SSA GHI's

			newsletter, subsequently withdraws his consent after the photograph has been published. SSA GHI is required under the PDPA to cease further publication of the photograph, unless such disclosure without Barry's consent is required or authorised under the PDPA or other written law, for example, if the photograph is already publicly available, or SSA GHI is able to effect the withdrawal of consent (e.g. by masking the image of the individual) before publishing or continuing to publish the photograph. 3.13 Deemed consent by contractual necessity: Pursuant to Section 15(3), if an individual gives, or is deemed to have given, consent to the collection, use or disclosure of his personal data to one organisation ("A") for the purpose of a contractual transaction, the consent may cover sharing of his personal data by A with other organisations (and onward sharing by downstream organisations, as the case may be) so long as it is reasonably necessary for A to provide the personal data to the other organisations (likewise, for onward sharing by downstream organisations) to perform or conclude A's contractual obligations. 3.14 2 . 1 5 Example: Disclosing donors' data to downstream organisations involved in fulfilling transaction Mary donates $300 to SSA ABC which provides treatment and care to cancer

			patients. She provides her personal data (i.e. NRIC number, residential address, bank account details) through an online donation form on SSA ABC's website. The form clearly states that the purpose of collection, use and disclosure of donors' personal data is for SSA ABC to process the donation (e.g. through GIRO deduction from the bank) and for tax relief purposes. Treatment As Mary had consented to the collection, use and disclosure of her personal data for the notified purposes, deemed consent by contractual necessity would apply to all other parties involved in the GIRO and tax relief processing chain who collect, use or disclose Mary's personal data, where the collection, use or disclosure is reasonably necessary to fulfil the transaction between Mary and SSA ABC. The parties include, for example, Mary's bank, SSA ABC's bank, the online payment gateway in which payment for the transaction is processed, the banks' processors and the tax authority. 3.15 Example: Disclosure of personal data to medical escorts for caregiving SSA DEF offers caregiving services to patients that need help to move around or have no caregiver to accompany them for their regular medical check-ups at the hospitals or clinics. In the provision of such caregiving services, SSA DEF engages medical escorts who accompany the patients to and from their

			homes and the hospitals or clinics for their medical check-ups, help to note down the doctor's prescriptions and help to schedule the next appointment. SSA DEF provides the patients' name, medical conditions and home addresses to the medical escorts for the purpose of fulfilling these caregiving services. In this case, as it is reasonably necessary for SSA DEF to provide the medical escorts with the personal data of patients for the medical escorts to fulfil the caregiving services for the patients, deemed consent by contractual necessity applies. 3.16 Deemed consent by notification: Section 15A provides that if an individual does not take any action to opt out of the collection, use or disclosure of his personal data for a purpose that he has been notified of, the individual is deemed to consent to the collection, use or disclosure of personal data by the organisation even for secondary use purposes that are different from the primary purposes for which it had originally collected the personal data for7 . 3.17 Nonetheless, the individual must have been notified that their personal data would be used for such secondary use purposes. The organisation must meet stipulated conditions by conducting an assessment to identify any adverse impact on the individuals arising from the proposed collection, use or disclosure of his personal data, and implement mitigating measures in relation to the adverse impacts

			identified. Please refer to the Advisory Guidelines on Key Concepts in the PDPA (Chapter 12) for more information on the stipulated conditions. 3.18 Example: Use of clients' personal data for publicity purposes Various medical institutions refer individuals to SSA ABC for the use of SSA ABC's facilities and services. SSA ABC accepts these individuals as its clients and receives their personal data from the medical institutions for the purpose of facilitating their use of its facilities and services. At the end of each year, SSA ABC engages in publicity to draw attention to its programmes and services, and it wants to use and disclose these clients' names in the publicity materials for that purpose. SSA ABC conducts an assessment to identify any adverse effect and determines that there are no likely adverse effects to the clients in using and disclosing their name for this new purpose. It also assesses that emailing its clients on the intended sharing of their personal data for the stated purpose is an appropriate and effective method of notification, as it regularly sends such emails to them on its latest programmes. It also assesses that 10 days is a reasonable period for the clients to opt out. Treatment SSA ABC sends emails to its clients, notifying them of the intended use and disclosure of their name for the purpose and provides a contact number for any queries on the

			intended use and disclosure. In the email, SSA ABC stipulates that those who wish to opt out should reply to the email within 10 days from the date of the email, stating that they want to opt out. Clients who do not opt out within the 10-day opt-out period are deemed to have consented to the disclosure of their personal data for the purpose. Nonetheless, SSA ABC must allow and facilitate any withdrawal of consent after the 10-day opt-out period. 3.19 Example: Publishing photographs taken at a private event on social media SSA DEF will be conducting a private 1-day retreat for its clients, which include children below the age of 13, and its employees. It wishes to take photographs of the attendees and publish some of the photographs on its social media accounts to generate publicity about its programmes. SSA DEF conducts an assessment to identify any adverse effect and determines that there are no likely adverse effects to the attendees in collecting, using and disclosing their personal data for this purpose. It also assesses that clearly stating in its email invitation to clients or their parents/guardians (for clients below the age of 13) and email notification to employees that photographs of attendees will be taken at the event for publication on its social media accounts is an appropriate and effective method of notification. SSA DEF also assesses that 14 days is a reasonable period to opt out.

			Treatment In its email invitations and notifications to clients and employees respectively, SSA DEF notifies them of the intended collection, use, and disclosure of their personal data for the purpose and provides a contact number for any queries. In the email, SSA DEF stipulates that those who wish to opt out of having their photographs taken at the event should reply to the email within 14 days from the date of the email, stating that they want to opt out. Clients and employees who do not opt out within the 14-day opt-out period are deemed to have consented to the collection, use and disclosure of their personal data for the purpose. Nonetheless, SSA DEF must allow and facilitate any withdrawal of consent after the 14-day opt-out period.8 11 Rights and obligations, etc under other laws 11.1 Section 4(6) of the PDPA states that unless otherwise provided in the PDPA, nothing in Parts 3 to 6 of the PDPA shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening the PDPA, and the provisions of other written law shall prevail to the extent that any provision of Parts 3 to 6 is inconsistent with the provisions of that other written law. 11.2 Similarly, section 13(b) of the PDPA provides that an organisation shall not, on or after the appointed day (i.e., 2 July 2014), collect, use or disclose

			personal data about an individual without the consent of the individual unless the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under the PDPA or any other written law. 11.3 Section 19 of the PDPA provides that notwithstanding the other provisions of Part 4 of the PDPA, an organisation may use personal data collected before the appointed day (i.e., 2 July 2014) for the purposes for which the personal data was collected, unless consent for such use is withdrawn or the individual has indicated to the organisation that he does not consent to the use of the personal data. Such 'use' could include disclosure that is necessarily part of the organisation's use of such personal data. For avoidance of doubt, the Do Not Call Provisions will apply to the sending of specified messages to Singapore telephone numbers, even if the Singapore telephone numbers are collected before the appointed day. PART III: APPLICATION OF THE DO NOT CALL PROVISIONS TO THE SOCIAL SERVICE SECTOR The following sections and examples set out the application of the Do Not Call Provisions to scenarios faced in the social service sector. They are not meant to exhaustively address every obligation in the PDPA that would apply in that scenario. In particular, they do not illustrate the application of the Data Protection Provisions, which were addressed earlier in these

			Guidelines. 12 The Do Not Call Provisions 12.1 Messages with a purpose to offer to supply, advertise or promote goods or services, land or an interest in land, or a business or investment opportunity, or a supplier of such goods, services, land or opportunity are specified messages and the Do Not Call Provisions will apply to such messages. Messages which do not contain any of such purposes would not be considered specified messages. 12.2 In addition, some types of messages, listed in the Eighth Schedule to the PDPA, are excluded from the definition of a specified message. Some examples include: a) "business-to-business" marketing messages; b) any message sent by a public agency under, or to promote, any programme carried out by any public agency, which is not for a commercial purpose; c) any message the sole purpose of which is to facilitate, complete or confirm a transaction that the recipient of the message has previously agreed to enter into with the sender; d) any message that is sent while the sender is in an ongoing relationship with the recipient of the message; and the sole purpose of which relates to the subject matter of the ongoing relationship; or e) any message the sole purpose of which is to conduct market research or market survey. 12.3 The Do Not Call Provisions apply to a specified message (in the form of voice calls, text messages or faxes) addressed to a Singapore telephone number, if the sender of the

			specified message is present in Singapore when the specified message is sent, or the recipient of the specified message is present in Singapore when the specified message is accessed. Duty to check the Do Not Call Registers 12.4 One significant obligation under the Do Not Call Provisions is that the organisation sending the specified message will have to check the Do Not Call Registry (the "DNC Registry") established by the Commission under the PDPA to confirm that the number is not listed on the DNC Register, unless the user or subscriber of the Singapore telephone number has given clear and unambiguous consent in written or other accessible form. 12.5 The PDPA lists obligations for third-party checkers23 who check the DNC Registry for an organisation and provide to the organisation information on whether the Singapore telephone number is listed in the relevant DNC Register. The checker must make sure that information provided to the organisation is accurate and up-to-date in accordance with the provisions relating to the DNC Registry24, and to provide to the organisation the date of retrieval of this information and its validity period. 12.6 Examples: Whether messages are specified messages25 SSA ABC runs a caregiver support group for families taking care of the elderly and will be conducting a seminar to impart skills in caring for the elderly. a) SSA ABC sends an SMS to various individuals who are

			clients and volunteers to publicise the event. The message is likely to be a specified message to the extent that it is an offer to provide a service. b) SSA ABC calls SSA XYZ's office line to inform SSA XYZ about the seminar and ascertain whether SSA XYZ would like to promote the upcoming seminar to SSA XYZ's clients and volunteers. Such a call is not a specified message as under the Eighth Schedule, a message sent to an organisation (other than an individual acting in a personal or domestic capacity) for any business purposes of the receiving organisation is excluded from the meaning of specified message. c) Should SSA XYZ market SSA ABC's seminar to individuals listed in SSA XYZ's own database of clients and volunteers by sending messages to their telephone numbers, SSA XYZ will be sending a specified message to those individuals. d) SSA ABC sends an SMS to its clients and volunteers, who had signed up for the seminar, informing of a postponement in the seminar. SSA ABC is not sending a specified message to the extent that the message does not offer to supply a good or service or have any of the other purposes listed in the definition of a specified message. 12.7 SSA XYZ is organising an annual charity fund-raiser. e) SSA XYZ sends an SMS to its donors and volunteers to donate money during the annual fund-raiser. To the extent that the SMS does not offer to supply a good or service or have any of

			the other purposes listed in the definition of a specified message, such a message would not be a specified message. f) SSA XYZ sends an SMS to its clients, donors and volunteers informing that it has partnered Company ABC to sell ABC's limited-edition products at the annual fund-raiser. In this case, as SSA XYZ is offering to supply or promoting Company ABC's products, it is considered to be sending a specified message. g) SSA XYZ calls its donors and volunteers to thank them for the donations/assistance rendered at the charity fund-raiser. SSA XYZ is not sending a specified message as the message does not offer to supply a good or service or have any of the other purposes listed in the definition of a specified message. 12.8 Example: Obtaining clear and unambiguous consent for future volunteering opportunities John volunteers at SSA GHI where volunteers accompany elderly clients for an outdoor walk at the nature park. When John signed up for this volunteering activity in a form, he checked a box to indicate that he consents to receiving specified messages by SMS for future volunteering opportunities with SSA GHI, even after the outdoor walk with elderly clients. John would be considered to have provided clear and unambiguous consent for SSA GHI to send text messages for future volunteering opportunities. Therefore, SSA GHI may send such messages to John without checking the DNC Registry. Dictionary Attacks and Address-Harvesting Software

			12.9 Section 48B of the PDPA provides that organisations must not send, cause to be sent, or authorise the sending of messages to recipient telephone numbers that are obtained by dictionary attack or address-harvesting. Dictionary attack is the method by which the telephone number is obtained using automated means that generate possible telephone numbers by combining numbers into numerous permutations, whereas address-harvesting is a software specifically designed or marketed for use for searching the Internet for telephone numbers and the telephone numbers are collected, compiled, captured or otherwise harvested.
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire	PART II: APPLICATION OF THE DATA PROTECTION PROVISIONS TO THE USE OF IVRDS 2 Application of the PDPA to the use of IVRDs Does the PDPA apply to in-vehicle recordings in transport vehicles for hire? 2.1 Under the PDPA, the term "personal data" refers to data (whether true or false) about an individual who can be identified from the data (whether alone or in combination with other information that the organisation has or is likely to have access to). In general, images, audio recordings5 and video recordings of identifiable individuals captured in in-vehicle recordings in transport vehicles for hire would comprise personal data. However, the content of communicationsin audio and video recordings, in and of themselves	Purpose Limitation and Notification Obligations for in-vehicle recordings? 3.1 Leasing Companies, Hirers and Service Providers who are subject to the Consent, Purpose Limitation and Notification Obligations are required to notify individuals of the purposes and obtain their consent9 for collecting, using and disclosing their personal data if they record personal data of individuals through IVRDs, unless any exception applies. For example, consent need not be obtained for the collection, use or disclosure of personal data that is publicly available. For more information on the publicly available exception, please refer to paragraph 3.18 of this document. 3.2 Leasing Companies, Hirers and Service Providersshould also ensure that they collect, use or disclose personal data

		may not be considered personal data, unless they contain information about an individual that can identify the individual. For more information on what constitutes personal data, please refer to Chapter 5 of the Key Concepts Guidelines. Does the PDPA apply to Leasing Companies, Hirers and Service Providers? 2.2 Every organisation6 is required to comply with the PDPA in respect of its personal data activities in Singapore, unless the organisation falls within a category of organisations specified in the PDPA as being excluded from the application of the PDPA. For more information relating to the categories of organisations which are excluded from the application of the PDPA, please refer to Chapter 6 of the Key Concepts Guidelines. 2.3 Generally, the PDPA would apply to Leasing Companies, Hirers and Service Providers in respect of their personal data activities in Singapore. What data protection obligations are Leasing Companies, Hirers and Service Providers required to comply with? 2.4 Organisations that undertake activities relating to personal data are required to comply with the PDPA. In particular, the Data Protection Provisions are set out in Parts III to VI of the PDPA. The Data Protection Provisions contain nine main obligations – Consent, Purpose Limitation, Notification, Access and Correction, Accuracy, Protection, Retention Limitation, Transfer Limitation,	only for purposes that are reasonable. Reasonableness of a purpose would depend on whether a reasonable person would consider it appropriate in the circumstances10 . How should notification be provided so as to obtain consent? 3.3 Leasing Companies, Hirers and Service Providers who are subject to the Consent, Purpose Limitation and Notification Obligations must notify individuals of the purposes for collecting, using and disclosing the individuals' personal data in order to obtain consent under the PDPA. 3.4 The PDPC notes that there are various means of notifying an individual of the purposes for collection, use and disclosure of his personal data. For example, Leasing Companies, Hirers and Service Providers may wish to place a prominent notice at an appropriate location on the window of the passenger door such that individuals boarding the vehicle are made aware, before they board the vehicle, that IVRDs are deployed in the vehicle for a particular purpose. Within the vehicle, notices setting out the purpose of the recording could also be placed at prominent locations and a recorded message may be played in the vehicle before the start of the journey to inform individuals that IVRDs are in operation. The PDPA does not prescribe the manner of notification11 and the persons responsible for complying with the

		and Openness Obligations. More information on the Data Protection Provisions can be found in the Key Concepts Guidelines. 2.5 The PDPA defines a category of organisations known as "data intermediaries" that process personal data on behalf of other organisations. The organisation that engages a data intermediary to process personal data on its behalf will be responsible for complying with all the Data Protection Provisions as if the personal data were processed by the organisation itself. The data intermediary that processes personal data for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will only be subject to the Protection and Retention Limitation Obligations. 2.6 The Hirer may be considered a data intermediary of the Leasing Company in respect of the in-vehicle recording if the Hirer records, stores or retrieves personal data in the in-vehicle recording on behalf of and for the purposes of the Leasing Company. Where the Hirer records, stores or retrieves personal data in the in-vehicle recording on behalf of and for the purposes of the Leasing Company pursuant to a contract that is evidenced or made in writing, the Hirer will only be subject to the Protection and Retention Limitation Obligations. If the Hirer records, stores or retrieves personal data in the in-vehicle recording on his own behalf and for his own purposes, the Hirer will not be considered a	Notification Obligation should assess the most appropriate manner of notifying the individual of the purposes. 3.5 The PDPA also does not prescribe the content of such notifications. Generally, the notification should indicate that IVRDs are operating within the vehicle, and specify the purposesfor the collection, use and disclosure of the personal data. For example, the notice could state that "in-vehicle video and/or audio recording is in operation for security and safety purposes". If there are other purposes for the collection, use and disclosure of personal data, these should be stated as well. 3.6 Example: Complying with the Consent, Purpose Limitation and Notification Obligations of the PDPA Taxi operator JKL places a prominent outward-facing notice indicating that IVRDs are in use in its taxis on the window of its taxis' passenger doors. Within the taxis, another notice is placed on the dashboard and the back of the head rests facing the passenger seats, which states clearly that the collection, use and disclosure of invehicle video recordings are for the purposes of ensuring the safety and security of the taxi driver and the passengers. A passenger sees the notices when boarding the taxi, and continues to take the taxi service. In this case, JKL would be considered to have obtained consent for the collection, use and disclosure of the passenger's personal data for those purposes12 .

		data intermediary of the Leasing Company in respect of the recording, and will be responsible for complying with all the Data Protection Provisions in the PDPA. 2.7 It is important that Leasing Companies, Hirers and Service Providers are clear as to their obligations under the PDPA, and put in place the necessary policies and practices to meet these obligations. The Leasing Company should ensure that its Hirers are made aware of and exercise proper data protection practices when handling personal data captured in IVRDs. It is also important that Leasing Companies clearly set out in contracts which are evidenced or made in writing the respective responsibilities and liabilities of the Leasing Company and the Hirers in relation to the personal data collected, used or disclosed in the course of providing the transport services, including whether the Hirer is to record, store or retrieve personal data in IVRDs on behalf of and for the purposes of the Leasing Company. In the event of an investigation, PDPC will take into account such contracts and policies7 in determining whether or not the Hirer is processing personal data on behalf and for the purposes of the Leasing Company. 2.8 Example: Hirer who is a data intermediary of the Leasing Company in respect of the in-vehicle recordings A taxi operator ABC has in place policies regarding the IVRDs it installs in its taxis8	JKL would also be in compliance with the Purpose Limitation Obligation under the PDPA if the collected personal data was subsequently used or disclosed for the purposes as specified in the notice. 3.7 Example: Leasing Company complying with the Consent, Purpose Limitation and Notification Obligations of the PDPA Leasing Company MNO provides limousine rental services. MNO has in place policies regarding the IVRDs it installs in its limousines, which stipulate that recordings will only be collected, used or disclosed for the purposes of ensuring the safety and security of the limousine driver and the passengers, as well as for the processing of insurance claims. MNO is contracted by an overseas-based company XYZ to provide limousine services in Singapore for XYZ's client, John. XYZ provides John with a form prepared by MNO that sets out the purposes for MNO's collection, use and disclosure of personal data, in particular personal data captured by in-vehicle recordings, and requires each prospective passenger to sign the form if he consents. XYZ provides MNO with a signed copy of the form that evidence John's consent. In this case, MNO would be considered to be in compliance with the Consent Obligation. 3.8 Example: Hirer complying with the Consent, Purpose Limitation and Notification Obligations of the PDPA

		, which stipulate that taxi drivers are only authorised to use these IVRDs on behalf of ABC and for ABC's purposes of ensuring the safety and security of passengers and the taxi driver, the processing of its insurance claims, as well as for investigations and law enforcement purposes. Where a taxi driver collects, uses or discloses the personal data contained in the in vehicle recordings on behalf and for the purposes of ABC, he is likely to be a data intermediary of ABC. 2.9 Where the Hirer uses or discloses personal data from the IVRD on his own behalf or for purposes beyond what is required for the purposes of the Leasing Company, the Hirer will not be considered a data intermediary of the Leasing Company, and is subject to all the Data Protection Provisions in respect of such use or disclosure of personal data. 2.10 Example: Hirer who is not a data intermediary of the Leasing Company in respect of the in-vehicle recordings A taxi operator DEF has in place policies regarding the use of IVRDs in its taxis, which stipulate that taxi drivers are only authorised to use IVRDs installed by DEF within the taxi and only for DEF's purposes of ensuring the safety and security of passengers and the taxi driver, the processing of its insurance claims, as well as for investigations and law enforcement purposes. DEF's policies also state that taxi drivers are not permitted to collect, use or disclose personal	Andy is a sole proprietor who provides transport services. He leases a limousine from Leasing Company PQR which has an IVRD installed. It is clearly stated in the leasing contract that the memory card for IVRDs is not provided and IVRDs are installed for use at the lessees' discretion and not for PQR's purposes. In addition, the contract provides that the lessee is responsible for complying with all the Data Protection Provisions in respect of the collection, use and disclosure of the personal data recorded in the in-vehicle recordings, and as any recording is not on behalf of the PQR, the lessee must not represent or do anything that may imply that it is collecting, using, disclosing or processing personal data on behalf of PQR. Andy wishes to collect, use and disclose in-vehicle recordings for safety and security purposes, but he does not intend to place IVRD notices within the limousine. In this case, Andy could consider using other methods to notify his prospective passengers of the purposes for the collection, use or disclosure of their personal data, for example, in his email to a prospective passenger together with other terms of his transport services (e.g. costs) and requesting that consent be given (with confirmation of the booking) by replying to his email. 3.9 Further information on the Consent, Purpose Limitation and Notification Obligations can be found in Chapters 12, 13 and 14 of the Key Concepts

		data using personal recording devices within the taxi. Where a taxi driver collects, uses or discloses the in-vehicle recordings, regardless of whether the recordings are captured by the IVRD installed by DEF or captured by his personal mobile phone, for his own purposes and not on behalf of DEF, he is unlikely to be considered to be a data intermediary of DEF. 2.11 The Commission understands that while some Leasing Companies may have IVRDs installed in their rental vehicles, they may not require their Hirers to use the IVRDs or to otherwise process personal data captured in the IVRDs on their behalf and for their purposes. In addition, the lease agreements may not include any specific policies on the use of IVRDs, except that any use of the IVRDs are for the Hirers' own purposes and not that of the Leasing Companies. In such cases, the Leasing Company would typically not be responsible for complying with all the Data Protection Provisions in respect of the Hirers' collection, use and disclosure of the personal data in the in-vehicle recordings. Leasing Companies are nevertheless encouraged to inform its Hirers who provide transport services for hire of their responsibilities under the PDPA on the collection, use and disclosure of personal data collected in the in-vehicle recordings. 2.12 Example: Hirer who provides transport service for hire is responsible for complying with all the Data	Guidelines respectively. Can Leasing Companies, Hirers and Service Providers require individuals to consent to the in-vehicle recording to use their transport services? 3.10 The PDPA provides that an organisation shall not as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of the individual's personal data beyond what is reasonable to provide the product or service to that individual. 3.11 Nonetheless, the PDPC recognises that there are certain situations where consent may be required for the provision of transport services. For example, it may be reasonable for Leasing Companies, Hirers and Service Providersto require those who wish to use their transport services to consent to the collection, use or disclosure of their personal data through in-vehicle recording to ensure the safety and security of the drivers, or to deter fare evasion. 3.12 Example: Passenger does not consent to the in-vehicle recording A taxi operator STU has in place policies on the use of IVRDs in its taxis, which stipulate that the IVRDs installed by STU in its taxis must remain in operation in the course of providing the taxi service for the purposes of ensuring the safety and security of the taxi driver and passengers. STU places prominent outward-facing notices on the windows of its taxis' passenger doors indicating that IVRDs are in use

		Protection Provisions of the PDPA Leasing Company GHI owns a fleet of cars, some of which have IVRDs installed. GHI states in its rental contract that the memory card for IVRDs is not provided and IVRDs are installed for use at the Hirers' discretion and not for GHI's purposes. In addition, the contract provides that GHI will not be responsible for any collection, use and disclosure of in-vehicle recordings and, as any recording is not on behalf of GHI, the Hirer must not represent or do anything that may imply that it is collecting, using, disclosing or processing personal data on behalf of GHI. GHI also highlights in the contract that the Data Protection Provisions in the PDPA will have to be complied with in respect of any collection, use or disclosure of personal data in the in-vehicle recordings. Where a Hirer uses the rented car to provide transport service for hire and decides to use the IVRD to collect in-vehicle recordings, the Hirer is responsible for complying with all the Data Protection Provisions in respect of the collection, use and disclosure of the personal data recorded in the in-vehicle recordings. 2.13 In general, the PDPC will consider the facts of each particular case to determine whether the Leasing Company, the Hirer, or both will be held responsible for the collection, use or disclosure of the personal data, for example, whether the Hirer was processing personal data on	in its taxis. Before entering the taxi, the passenger sees the notices and is notified that invehicle video recordings are collected, used and disclosed for the safety and security purposes of the taxi driver and passengers. A passenger informs the taxi driver, before the start of the journey, that he does not consent to the collection, use and disclosure of his personal data in the in-vehicle recording. As the collection, use or disclosure of personal data for the stipulated purpose is reasonable to provide the taxi service, consent of passengers can be required for the in-vehicle recording in order to provide the service. In this case, the taxi driver may inform the passenger of STU's requirement on the use of IVRD for the stipulated purposes, and allow the passenger to decide whether to use the taxi service. Can individuals withdraw consent for the use or disclosure of their personal data in the in-vehicle recording after using the transport service? 3.13 Leasing Companies, Hirers and Service Providers who are subject to the Consent, Purpose Limitation and Notification Obligations must allow individuals to withdraw any consent given under the PDPA, and put in place policies and practices to facilitate such withdrawal of consent. Leasing Companies, Hirers and Service Providers are advised to make their consent withdrawal policies easily accessible to individuals,

		behalf of and for the purposes of the Leasing Company. 2.14 Please refer to Chapter 6 of the Key Concepts Guidelines for more information on data intermediaries. Further details on the Protection and Retention Limitation Obligations can be found in Chapters 17 and 18 of the Key Concepts Guidelines. 3 Complying with Consent, Purpose Limitation and Notification Obligations How can Leasing Companies, Hirers and Service Providers comply with the Consent, 5 Complying with Protection Obligation How can Leasing Companies, Hirers and Service Providers comply with the Protection Obligation for in-vehicle recordings? 5.1 Leasing Companies, Hirers and Service Providers who record personal data of individuals through IVRDs19 are required to make reasonable security arrangements to protect the personal data in their possession or under their control in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Please refer to Chapter 17 of the Key Concepts Guidelines for more details on the Protection Obligation. 5.2 There is no 'one size fits all' solution for complying with the Protection Obligation. Each Leasing Company, Hirer and Service Provider should consider adopting security arrangements that are reasonable and appropriate in the circumstances. Security arrangements may take various	and to include ways on how consent can be withdrawn. 3.14 If an individual withdraws consent for the use or disclosure of his personal data in the in-vehicle recording after using the transport service, the Leasing Company, Hirer and Service Provider must cease (and cause its data intermediaries and agents to cease13) using or disclosing the personal data in the in-vehicle recording, unless the use or disclosure of the personal data without consent is required or authorised under the PDPA or any other written law. For example, the Leasing Company, Hirer and Service Provider may rely on exceptions provided in the Third and Fourth Schedules to the PDPA to use and disclose the passenger's personal data from the in-vehicle recording without consent where the use and disclosure are necessary for any investigation or proceedings. Leasing Companies, Hirers and Service Providers need not delete or destroy such personal data upon withdrawal of consent, and may retain the in-vehicle recording if there are any legal or business purposes to retain it. 3.15 Example: Withdrawal of consent after using the hired transport service John, a passenger, when boarding the taxi, consents to the taxi operator's collection of his personal data through in-vehicle recordings and to the use and disclosure of such personal data for safety and security purposes. At the end of the taxi journey, John withdraws his consent for the use and disclosure of his

		forms such as administrative measures, physical measures, technical measures or a combination of these. 6 Other Obligations 6.1 Leasing Companies, Hirers and Service Providers should be mindful that Parts III to VI of the PDPA do not affect any legal rights or obligations under other laws20. In the event of any inconsistency with other written laws, such other written laws will prevail to the extent of such inconsistency21. As such, a Leasing Company, Hirer and Service Provider will still be subject to obligations under other relevant laws in addition to their obligations under the PDPA22 . The Hirer may also be subject to any contract that he may have with the Leasing Company. Please refer to Chapter 22 of the Key Concepts Guidelines for more information. 6.2 It should be noted that this document is not meant to exhaustively address every obligation of Leasing Companies, Hirers and Service Providers under the PDPA. Leasing Companies, Hirers and Service Providers should not rely solely on this document to ensure their compliance with the PDPA.	personal data in the invehicle recording and requests for its deletion. The taxi operator must cease, and cause its data intermediaries (which may be the taxi driver) to cease the use and disclosure of John's personal data in the in-vehicle recording, unless otherwise authorised or required under any written law. However, they need not delete the recording upon withdrawal of consent, and may retain it if there are any legal or business purposes to retain it. 3.16 Example: Withdrawal of consent in the event of an investigation Ben, a passenger, when boarding the taxi, consents to the collection of his personal data through the taxi operator's in-vehicle recordings and to the use and disclosure of such personal data for safety and security purposes.During the journey, an incident takes place between Ben and the taxi driver. The taxi driver makes a police report for an alleged physical assault by Ben. Ben writes in to the taxi operator to withdraw consent for the use and disclosure of his personal data in the taxi's in-vehicle recording. The taxi operator may rely on exceptions provided in the Third and Fourth Schedules to the PDPA, to use and disclose the passenger's personal data in the in-vehicle recording without consent where it is necessary for any investigation or proceedings. In addition, the taxi operator need not delete the recording, and may

			retain it if there are any legal or business purposes to retain it. 3.17 For more information on withdrawal of consent, please refer to Chapter 12 of the Key Concepts Guidelines. How does the exception for "publicly available" personal data apply to in-vehicle recordings? 3.18 The PDPA does not require organisations to obtain the consent of individuals to collect personal data that is publicly available14. This includes personal data that is observed by reasonably expected means at a location or event at which the individual appears and that is open to the public. The PDPC recognises that personal data of individuals appearing in public may be captured by outward-facing video cameras installed in hired transport services. Where such outward-facing cameras capture the images of individuals appearing in a public location outside the vehicle, the exception for "publicly available data" is likely to apply, and Leasing Companies, Hirers and Service Providers who are subject to the Consent, Purpose Limitation and Notification Obligations will not be required to notify and obtain consent from the individuals for the recording. 3.19 However, the exception for "publicly available data" does not apply where IVRDs capture images and/or voices of individuals inside the vehicle when it is hired. This is because the interior cabin of the vehicle would be considered a private space when it is hired. In such cases, Leasing Companies, Hirers and Service

			Providers must provide appropriate notification and obtain consent of the individuals before collecting, using or disclosing their personal data. 3.20 For more information on the exception for publicly available data, please refer to Chapter 12 of the Key Concepts Guidelines.
33	Advisory Guidelines for the Real Estate Agency Sector	3 The Data Protection Provisions 3.1 The Data Protection Provisions in Parts III to VI of the PDPA set out the obligations that organisations are required to comply with if they undertake activities relating to the collection, use or disclosure of personal data. Among other things, organisations are required to obtain valid consent from the individual for a limited purpose that has been notified to the individual for the collection, use and disclosure of personal data of the individual, unless exceptions apply. 3.2 The PDPC does not prescribe the manner in which consent is obtained by an organisation under the Data Protection Provisions. An organisation may decide on the most suitable way to obtain consent in accordance with the PDPA, and may refer to Chapter 12 of the Key Concepts Guidelines for more information on considerations and good practices when obtaining consent from an individual 3.3 In situations where an individual voluntarily provides his personal data to an organisation for a purpose, and it is reasonable that he would	

		voluntarily provide the data, the individual is deemed to consent5 to the collection, use or disclosure of the personal data. If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organisation to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation. 3.4 Example: Personal data collected from clients Sarah will be relocating overseas and is putting up her apartment (which she co-owns with her husband, Sam) for sale. She approaches Jack, a salesperson representing estate agent ABC, to sell her property. To understand the characteristics of the property, Jack discusses with Sarah the strengths and weaknesses of the property and Sarah's reasons for selling the property. (a) Jack indicates to a prospective buyer that "the seller says the afternoon sun does not reach the bedroom". In this case, Jack has not disclosed the personal data of Sarah. (b) Jack indicates to a prospective buyer who visits the apartment that the seller Sarah and her husband have two children attending school in the vicinity of the apartment, and the couple is selling the apartment because they are relocating to country XYZ. In this	

		situation, Jack is disclosing personal data of Sarah. Jack should obtain Sarah's consent6 to disclose her personal data to prospective buyers. For example, when Jack discusses the sale with Sarah, Jack could obtain Sarah's consent to mention some of her personal details to prospective buyers7 . (c) After Sarah has signed an estate agency agreement8 , Jack obtains Sarah's personal data from her for the purposes of providing the agency service to her, including her contact details. As Sarah had voluntarily provided such personal data to Jack for this purpose, Sarah is likely to be deemed to have consented to Jack's collection, use and disclosure of such personal data for the purpose of providing her with the agency service, for example calling her to discuss offers received for her property or to arrange for prospective buyers to view her property. (d) Sarah asks Jack to suggest a law firm which she could engage to obtain conveyancing services. Jack recommends law firm XYZ and obtains consent from Sarah to disclose her email address to XYZ in order for XYZ to contact her directly to provide more details about its conveyancing services. 3.5 Example: Marketing of potential en-bloc sale	

		Estate agent ABC is assisting the Management Corporation ("MC") of a condominium to market a potential en-bloc sale of the condominium to owners of units in the condominium. ABC has compiled a list containing the names, addresses and telephone numbers of owners taken from various sources including online title search services, the MC and communications with neighbours of some of the owners. ABC intends to first contact the owners by mailing letters to inform them of the potential en-bloc sale, and then place follow-up calls to these owners. In this case, the Data Protection Provisions will apply as ABC has collected and used personal data relating to the individual owners to market the potential en-bloc sale. Among other things, ABC will have to obtain consent from the individual owners on or before collecting and using their personal data, unless exceptions apply9. In this regard, possible exceptions may include if the personal data is publicly available. 3.6 Example: Disclosure of client's personal data in a co-broking10 situation Sarah approached Jack, a property salesperson representing estate agent ABC, to sell her apartment. Another salesperson, Tommy, has a client who is interested in making an offer for Sarah's apartment. Tommy	

		and Jack agree to enter into a co-broking arrangement for this property. After viewing the apartment, the potential buyer decides to proceed with the purchase. Tommy wishes to disclose the potential buyer's personal data, including his name, NRIC and contact details, to Jack. In this case, Tommy would be required to obtain consent from the buyer, though he may decide on the most suitable way to obtain consent. 3.7 Example: Valid consent for personal data of multiple individuals John and Sarah intend to purchase a residential property together. They engage Jack, a salesperson with estate agent ABC, to help source for suitable properties. John provides Jack with the personal data (such as full name and address) of himself and Sarah for Jack to prepare the estate agency agreement and other documentation required for the purchase of the property (should they wish to proceed with the purchase) In this scenario, the Data Protection Provisions would generally apply in respect of Jack's collection, use or disclosure of John and Sarah's personal data. Jack may therefore wish to obtain consent from John and Sarah such as through the signing of the estate agency agreement. Jack would then be able to collect, use and disclose their personal data for such purposes for which consent had been	

		obtained. Alternatively, certain exceptions to the Consent Obligation may potentially apply, depending on the specific facts of the case. For example, if John and Sarah are a married couple purchasing the property for their own residential use, the exception to the Consent Obligation in paragraph 1(m) of the Second Schedule to the PDPA11 may potentially be applicable in respect of Jack's collection of Sarah's personal data from John. However, if Jack is relying on this exception to collect Sarah's personal data from John without Sarah's consent, Jack can only use her details for the purposes of the services that he is providing for the personal or domestic purposes of John (i.e. buying a home for residential use). Please also refer to the Key Concepts Guidelines for more information on obtaining personal data from third party sources with/without the consent of the individual. 3.8 Example: Business contact information12 of client(s) Jim and Lisa are the directors of company GEF and are looking for a commercial property to be used as GEF's office premises. They engage Andy, a salesperson with estate agent XYZ, to help source for suitable office space. Jim provides the business contact information of himself and Lisa to Andy so that Andy may liaise	

		with both of them. The Data Protection Provisions do not apply to business contact information. Hence, Andy is not required to obtain the consent of Jim or Lisa to collect, use or disclose their business contact information. However, the Data Protection Provisions would apply if Andy collects, uses or discloses Jim's or Lisa's personal data, beyond the business contact information provided to Andy. 3.9 Example: Personal data of salespersons A prospective buyer enquires about a property listed on estate agent ABC's website. ABC provides the prospective buyer with the business phone number of its salesperson, Alan, for the buyer to enquire about the listing. Since that phone number forms part of Alan's business contact information, ABC does not require Alan's consent to disclose his business contact information to the prospective buyer.	
34	Advisory Guidelines for the Healthcare Sector	The Accuracy, Protection, Retention Limitation, Transfer Limitation, Data Breach Notification and Accountability Obligations The Advisory Guidelines on Key Concepts in the PDPA elaborates on these obligations. Like other organisations, healthcare institutions should consider the application of these obligations to their specific contexts. The Accuracy Obligation Pursuant to the Accuracy Obligation (PDPA section 23), an	

		organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be used by the organisation to make a decision that affects the individual concerned or disclosed by the organisation to another organisation. For more information on the Accuracy Obligation, do refer to Chapter 16 of the Advisory Guidelines on Key Concepts in the PDPA. The Protection Obligation According to the Protection Obligation (PDPA section 24), an organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent (i) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (ii) the loss of any storage medium or device on which personal data is stored. For more information on the Protection Obligation, do refer to Chapter 17 of the Advisory Guidelines on Key Concepts in the PDPA. The Retention Limitation Obligation The Retention Limitation Obligation (PDPA section 25) states that an organisation must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that (i) the purpose for which the personal data was collected is no longer being served by	

		retention of the personal data; and (ii) retention is no longer necessary for legal or business purposes. The PDPA does not prescribe a specific retention period for personal data. However, healthcare institutions should review the personal data they hold on a regular basis to determine if that personal data is still needed. The retention period for personal data under the PDPA can depend on whether the personal data is required for research or archival purposes that benefit the wider public or a segment of the public. Healthcare institutions should not keep personal data "just in case", when it is no longer necessary for the purposes for which the personal data was collected or for any legal or business purpose. Attention is drawn to Regulation 12(3) of the PHMC Regulations, Regulation 37(1) of the Healthcare Services (General) Regulations, and the MOH's 2022 Revised Guidelines for the Retention Periods of Medical Records. For more information on the Retention Limitation Obligation, do refer to Chapter 18 of the Advisory Guidelines on Key Concepts in the PDPA.	
35	Advisory Guidelines for the Telecommunication Sector	3 The Data Protection Provisions 3.1 The Data Protection Provisions in Parts III to VI of the PDPA set out the obligations that organisations are required to comply with if they undertake activities relating to the collection, use or disclosure of personal data. Among other things, organisations are required to obtain valid consent from the	

		individual for a limited purpose that has been notified to the individual for the collection, use and disclosure of personal data of the individual, unless exceptions apply2 . In situations where an individual voluntarily provides his personal data to an organisation for a purpose, and it is reasonable that he would voluntarily provide the data, the individual is deemed to consent to the collection, use or disclosure of the personal data. If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organisation to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation. Inbound and outbound roaming Inbound roaming 3.2 In the case of inbound roaming, a Singapore telecommunication operator may collect some personal data of a foreign mobile user using its network ("inbound roamer") in order for the foreign telecommunication operator (the "home operator") to provide a roaming service to the inbound roamer. For example, the Singapore telecommunication operator might collect the telephone number and device identifier of the inbound roamer and his service usage patterns and transfer	

		such information to the home operator for the home operator to bill the inbound roamer. 3.3 To the extent that a Singapore telecommunication operator is processing the personal data of inbound roamers on behalf of and for the purposes of their respective home operators, the Singapore telecommunication operator could be a data intermediary ("DI") of the home operators. In this regard, where a Singapore telecommunication operator is acting as a DI processing personal data on behalf of and for the purposes of a home operator pursuant to a contract evidenced or made in writing with that home operator, the Singapore telecommunication operator is only required to comply with the Protection Obligation and Retention Limitation Obligation of the PDPA in relation to its processing of the personal data of inbound roamers3. More details on the treatment and obligations of DIs are available in the Key Concepts Guidelines. 3.4 Where the Singapore telecommunication operator is not acting as a DI processing personal data on behalf of and for the purposes of a home operator pursuant to a contract evidenced or made in writing with that home operator, such as when it is collecting, using, disclosing or otherwise processing the personal data of inbound roamers for its own purposes (for	

		example to market the Singapore telecommunication operator's own pre-paid card options) the Data Protection Provisions would apply to such activities unless exceptions apply. One of these exceptions would be an exception to the Consent Obligation where the collection, use or disclosure without the consent of the individual is required or authorised under a written law. In this regard, the Commission understands that IDA is considering authorising telecommunication licensees to collect, use or disclose the personal data of inbound roamers to offer such inbound roamers roaming-related information4 . 3.5 To be clear, the Data Protection Provisions generally apply where the personal data of inbound roamers is collected, used or disclosed. Where the Singapore telecommunication operator carries out an activity for a purpose without involving personal data, for example when analysing anonymised data of inbound roamers (for which it has no means of re-identification) for business planning purposes, the Data Protection Provisions do not apply to that activity. Outbound roaming 3.6 In the case of outbound roaming, a Singapore telecommunication operator typically has contractual agreements with foreign telecommunication	

		operators to provide telecommunication services to the subscribers of the Singapore telecommunication operator when overseas ("outbound roamers"). 3.7 The Commission notes that there may be some exchange of data (including personal data) between a Singapore telecommunication operator and foreign telecommunication operators in order for the latter to provide mobile services to outbound roamers who are the Singapore telecommunication operator's subscribers, pursuant to the contractual agreements between the Singapore telecommunication operator and the foreign telecommunication operators. In such situations, the Singapore telecommunication operator will need to comply with the Notification, Consent and Transfer Limitation Obligations in respect of the disclosure of personal data to foreign telecommunication operators and the related transfer of personal data out of Singapore to foreign telecommunication operators5. Telecommunication operators should refer to the Personal Data Protection Regulations 2014 ("Data Protection Regulations") and corresponding guidance on the Transfer Limitation Obligation in the latest Key Concepts Guidelines for more information on the Transfer Limitation Obligation. Provision of subscriber identity for calls or text messages 3.8 Currently, when a subscriber	

		who is an individual makes a telephone call or sends a text message, his telephone number (which may be personal data relating to him) would typically be disclosed to the receiving party and both the subscriber and receiving party's telecommunication operators, unless the subscriber had chosen to have his telephone number 'blocked'/ 'unlisted'6 . Telecommunication operators may wish to obtain the consent of the individuals for the purpose of such disclosures to recipients of his calls and messages7 . 3.9 Even if the telecommunication operators do not obtain such actual consent, given established practice, the Commission is of the view that a subscriber who opts to have an 'unblocked'/ a 'listed' telephone number would typically be aware that the telephone number would be collected, used or disclosed for the purpose of identifying that subscriber to other parties. Where the telephone number is personal data relating to a subscriber, a subscriber with an 'unblocked'/ a 'listed' telephone number initiating a call or sending a message may be deemed to have consented to the collection, use or disclosure of the number for the purpose of identifying himself to the receiving party, since the subscriber would have voluntarily provided the	

		data, and it would be reasonable for the subscriber to have done so. 3.10 Conversely, a subscriber who has opted for a 'blocked'/ an 'unlisted' number at the outset would not be considered to have consented to the collection, use or disclosure of the number for that purpose. A subscriber with an 'unblocked'/ a 'listed' telephone number who subsequently applies to 'block'/ 'unlist' that telephone number would be considered to have withdrawn consent for the collection, use or disclosure of that telephone number for the purpose of identifying himself to other parties when making a call or sending a message. 3.11 Where an individual subscriber is deemed to have given consent for disclosure of his telephone number by one telecommunication operator to another telecommunication operator for the purpose of identifying himself to the recipient of his call or message, consent may be deemed to have been given to the collection, use or disclosure of the telephone number by that other telecommunication operator for the same purpose. Alternatively, consent may not be required if the purpose for collection, use or disclosure of the personal data falls within an exception, such as when it is required or authorised under written law. Displaying personal data in itemised bills 3.12 Itemised bills for	

		telecommunication services display information such as telephone numbers that a subscriber contacts or is contacted by, and the timing and duration of calls made or received (collectively, "call data"). As call data may be personal data, an itemised bill may reflect the personal data of the subscriber, as well as the personal data of other individuals, through the display of call data. 3.13 The Commission regards the display of call data in itemised bills as a reproduction of the record of the subscriber's transactions carried out using the telecommunication operator's service. As such, where call data is personal data, consent obtained by the subscriber to make a call or send a message to an individual would suffice for the call data pertaining to the call or message to be displayed in the subscriber's itemised bill. Similarly, consent given (or deemed to be given) by an individual who makes a call or sends a message to the subscriber would extend to the display of the caller's/sender's (as the case may be) call data in the subscriber's itemised bill. 3.14 In addition, the Commission considers that an individual subscriber who applies for itemised billing may be considered to have made an access request for personal data that resides in call data. Thus, a telecommunication operator may provide such personal data in response to an	

		application for itemised billing in a manner that would respond to an access request. Pre-paid mobile services 3.15 The Commission understands that the purchase of pre-paid cards for telecommunication services typically does not involve the signing of a written contract and the current practice among many telecommunication licensees is for a pre-paid card to contain a general statement directing individuals to the terms and conditions of the contract that may be made available by telecommunication operators, for example on their websites. 3.16 When selling a pre-paid card, the telecommunication operator (or the reseller, on the telecommunication operator's behalf) may collect various types of personal data from the individual, including the individual's name and identification details such as NRIC numbers, passport numbers or work permit numbers. In addition, the telecommunication operator would possess data such as the telephone number tied to that pre-paid card, as well as details of the pre-paid card account including account balance and usage profile. 3.17 The Commission further understands that the purposes for the telecommunication operators' collection, use and disclosure of such personal data generally include: a) providing the individual with the telecommunication services,	

		which may be voice calls, SMSes, mobile data or international call services; b) complying with requirements under written law, for example regulatory requirements; c) sending various messages to the Singapore telephone number tied to the pre-paid card, some of which may be targeted at specific sets of pre-paid card holders (for example, based on a certain usage characteristic); and d) analysing usage profiles of the pre-paid subscriber base to plan new pre paid products and services. 3.18 In general, the telecommunication operator collecting, using or disclosing the personal data of individuals who buy pre-paid cards will have to comply with all the relevant provisions in the PDPA, including the Data Protection Provisions and the Do Not Call Provisions. Depending on the arrangements between the telecommunication operators and resellers of pre-paid cards, resellers may be considered to be DIs acting pursuant to a contract made or evidenced in writing with the respective telecommunication operator, and will therefore be subject only to the Protection Obligation and Retention Limitation Obligation. 3.19 The telecommunication operator should assess how best it can ensure compliance with the Data Protection Provisions. For example, it would be required to adopt an appropriate	

		procedure to notify the individual subscriber of the purposes for which their personal data may be collected, used or disclosed and obtain consent from the individual subscriber for the collection, use or disclosure of his personal data, unless exceptions apply. In the case where an individual voluntarily provides the personal data to the reseller for such purposes, that individual could also be deemed to have consented to the disclosure of his personal data by the reseller to the telecommunication operator for the stated purposes. For the avoidance of doubt, some relevant exemptions may apply to the Consent Obligation, such as where the collection, use or disclosure of personal data is required under written law. More details on the Notification Obligation and Consent Obligation are provided in the Key Concepts Guidelines. 3.20 Example: obtaining consent from pre-paid mobile subscribers A telecommunication operator wishes to notify and obtain consent from its pre-paid mobile subscribers for purposes for which it will collect, use or disclose their personal data. However, the form factor of the pre-paid card is too small to allow an elaborate statement of the purposes. The telecommunication operator may consider options such as: a) adopting the 'layered notice' approach described in the Advisory	

		Guidelines on Key Concepts, by briefly stating the purposes on the pre paid card or in the service activation message, and referring the individual to the telecommunication operator's website for a more detailed statement of purposes and the operators' data protection policy; or b) stating the purposes for collection, use and disclosure of personal data on a separate notice, for example at the reseller's counter. Inclusion of advertisements with bills 3.21 The Commission understands that telecommunication operators may include advertisements for specific products or services as inserts in bills addressed to individuals or in the form of promotional messages printed on the bills themselves. 3.22 Where a telecommunication operator packages such advertisements together with bills that are addressed to an identifiable individual (whether as an insert, or as a message printed on the bills themselves), the telecommunication operator would generally be considered to have used personal data for advertising purposes, even if the advertisements themselves are not addressed to the individual. Correspondingly, the Data Protection Provisions would apply to such use. Among other things, when an individual withdraws consent under the PDPA for such	

		purposes, the telecommunication operator would be required to allow and facilitate such withdrawal. The Key Concepts guidelines contain more details of the actions to be taken when receiving a notice of withdrawal of consent. 3.23 There are several obligations within the Data Protection Provisions which require organisations to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. Organisations are required to make the information about their data protection policies and practices available. For more information, please refer to the latest Key Concepts Guidelines and the latest Advisory Guidelines on the PDPA for Selected Topics. 4 Rights and obligations, etc under other laws 4.1 Section 4(6) of the PDPA states that unless otherwise provided in the PDPA, nothing in Parts III to VI of the PDPA shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening the PDPA, and the provisions of other written law shall prevail to the extent that any provision of Parts III to VI is inconsistent with the provisions of that other written law.	

		4.2 Example: Caching of data by an Internet Service Provider ("ISP") In the course of providing network services, a Network Service Provider, such as an ISP, may cache data in relation to certain websites, which may result in personal data being collected and used without consent. Section 67 of the PDPA amends Section 26 of the Electronic Transactions Act (Cap. 88) to provide that a Network Service Provider shall not be subject to any liability under the PDPA in respect of third-party material in the form of electronic records to which it merely provides access. The provision of access, in relation to third party-material, includes the automatic and temporary storage of the third-party material for the purpose of providing access. The temporary and automatic caching of third party material in the form of electronic records (that contains personal data) by a Network Service Provider thus does not impose additional liability on it, provided that such caching is carried out for the purpose of its service of merely providing access to the third party material. 4.3 Section 13(b) of the PDPA provides that an organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual without the consent of the individual unless the collection,	

		use or disclosure, as the case may be, without the consent of the individual is required or authorised under the PDPA or any other written law. In the telecommunication context, the Commission understands that regulatory frameworks issued pursuant to the Telecommunications Act sets out certain purposes for which telecommunication operator may collect, use or disclose End User Service Information, some of which qualify as personal data, without consent. 4.4 Section 19 of the PDPA provides that notwithstanding the other provisions of Part IV of the PDPA, an organisation may use personal data collected before the appointed day for the purposes for which the personal data was collected, unless consent for such use is withdrawn or the individual has indicated to the organisation that he does not consent to the use of the personal data. Such 'use' could include disclosure that is necessarily part of the organisation's use of such personal data. For avoidance of doubt, the Do Not Call Provisions will apply to the sending of specified messages to Singapore telephone numbers, even if the Singapore telephone numbers are collected before the appointed day.	
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied	The Protection Obligation 6 – Protection Obligation in PDPA	

	Agents of Life Insurers on the Singapore Personal Data Protection Act	An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. 45. The tied agent shall comply with the Protection Obligation pertaining to personal data in his possession or control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or other similar risks. 46. In addition, the tied agent shall adhere to the life insurer's standards on information and data security with regard to the protection of personal data.	

#	Regulation	internal	internal
		Accuracy	Retention Limitation
1	Personal Data Protection Act 2012	Accuracy of personal data 23. An organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data — (a) is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or (b) is likely to be disclosed by the organisation to another organisation.	Retention of personal data 25. An organisation must cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that — (a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and (b) retention is no longer necessary for legal or business purposes.
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		

5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		

17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment		
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act	16 The Accuracy Obligation 16.1 Section 23 of the PDPA requires an organisation to make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data: a) is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or b) is likely to be disclosed by the organisation to another organisation. 16.2 This obligation to ensure that personal data is accurate and complete is referred to in these Guidelines as the Accuracy Obligation. The aim of the Accuracy Obligation is to ensure that where personal data may be used to make a decision that affects the individual, the data is reasonably correct and complete so as to ensure that the decision is made taking into account all relevant parts of accurate personal data.	The Retention Limitation Obligation 18.1 Section 25 of the PDPA requires an organisation to cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data, and retention is no longer necessary for legal or business purposes. This obligation to cease to retain personal data is referred to in these Guidelines as the Retention Limitation Obligation. How long personal data can be retained 18.2 The Retention Limitation Obligation prevents organisations from retaining personal data in perpetuity where it does not have legal or business reasons to do so. Holding personal data for an

		16.3 In order to ensure that personal data is accurate and complete, an organisation must make a reasonable effort to ensure that: a) it accurately records personal data which it collects (whether directly from the individual concerned or through another organisation); b) personal data it collects includes all relevant parts thereof (so that it is complete); c) it has taken the appropriate (reasonable) steps in the circumstances to ensure the accuracy and correctness of the personal data; and d) it has considered whether it is necessary to update the information. Requirement of reasonable effort 16.4 The Accuracy Obligation requires organisations to make a reasonable effort to ensure the accuracy and completeness of personal data. Hence the effort required of an organisation depends on the exact circumstances at hand. In determining what may be considered a reasonable effort, an organisation should take into account factors such as the following: a) the nature of the data and its significance to the individual concerned (e.g. whether the data relates to an important aspect of the individual such as his health); b) the purpose for which the data is collected, used or disclosed; c) the reliability of the data (e.g. whether it was obtained from a reliable source or through reliable	indeterminate duration of time increases the risk of a contravention of the Data Protection Provisions. However, as each organisation has its own specific business needs, the Retention Limitation Obligation does not specify a fixed duration of time for which an organisation can retain personal data. Instead, the duration of time for which an organisation can legitimately retain personal data is assessed on a standard of reasonableness, having regard to the purposes for which the personal data was collected and other legal or business purposes for which retention of the personal data may be necessary. 18.3 It should be noted that although the PDPA does not prescribe a specific retention period for personal data, organisations would need to comply with any legal or specific industry-standard requirements that may apply. 18.4 In practice, the retention period for personal data under the PDPA will depend on the following factors: a) The purpose(s) for which the personal data was collected. That is: i. personal data may be retained so long as one or more of the purposes for which it was collected remains valid; and ii. personal data must not be kept by an organisation "just in case" it may be needed for other purposes that have not been notified to the individual concerned. Example: A dance school has collected personal data of its tutors and students. It retains

		means); d) the currency of the data (that is, whether the data is recent or was first collected some time ago); and e) the impact on the individual concerned if the personal data is inaccurate or incomplete (e.g. based on how the data will be used by the organisation or another organisation to which the first organisation will disclose the data). 16.5 For the avoidance of doubt, an organisation may not be required to check the accuracy and completeness of an individual's personal data each and every time it makes a decision about the individual. An organisation may also not be required to review all the personal data currently in its possession to ensure that they are accurate and complete each and every time it is likely to make a decision about the individual. Organisations should perform their own risk assessment and use reasonable effort to ensure the accuracy and completeness of such personal data that is likely to be used to make a decision that will affect the individual. Ensuring accuracy when personal data is provided directly by the individual 16.6 Organisations may presume that personal data provided directly by the individual concerned is accurate in most circumstances. When in doubt, organisations can consider requiring the individual to make a verbal or written declaration that the personal data provided is	and uses such data (with the consent of the individuals), even if a tutor or student is no longer with the dance school, for the purpose of maintaining an alumni network. As the dance school is retaining the personal data for a valid purpose, it is not required to cease to retain the data under the Retention Limitation Obligation. A retailer retains billing information, including personal data, collected from its customers beyond the Point of Sale for the purposes of accounting and billing administration. As the retailer is retaining the personal data for a valid purpose, it is not required to cease to retain the data under the Retention Limitation Obligation. b) Other legal or business purposes for which retention of the personal data by the organisation is necessary. For example, this may include situations where: i. the personal data is required for an ongoing legal action involving the organisation; ii. retention of the personal data is necessary in order to comply with the organisation's obligations under other applicable laws, regulations, international/regional/bilateral standards which require the retention of personal data; iii. the personal data is required for an organisation to carry out its business operations, such as to generate annual reports, or

		accurate and complete. In addition, where the currency of the personal data is important, the organisation should take steps to verify that the personal data provided by the individual is up to date (for example, by requesting a more updated copy of the personal data before making a decision that will significantly impact the individual). Example: Nick applies for a credit card from a bank. The bank asks Nick to provide relevant details such as his name, address, current employment status and income, which constitute personal data, in order to assess the application. Related to this, the bank asks Nick to provide supporting documents including an identity document and his most recent payslip, in order to verify the information provided by Nick. It also asks Nick to declare that the information he has provided is accurate and complete. In this scenario, the bank has made a reasonable effort to ensure that the personal data collected from Nick is accurate and complete. Two years later, Nick applies for a home loan from a bank. The bank has not made any checks during the two years that Nick's personal data is accurate and complete. When the bank received the home loan application, the bank showed Nick their records of his personal data and asked Nick to make a fresh declaration that the record is	performance forecasts; iv. the personal data is used for an organisation's business improvement purposes such as improving, enhancing or developing goods or services, or learning about and understanding the behaviour and preferences of its customers; or v. retention of the personal data is necessary for research, archival, historical, artistic or literary purpose(s) that benefits the wider public or a segment of the public. Example: Under the Limitation Act (Cap. 163), actions founded on a contract (amongst others) must be brought within 6 years from the date on which the cause of action accr

		accurate and complete. In addition, noting that the supporting documents previously obtained for the credit card application are now dated two years back, the bank asked Nick to provide a copy of his most recent payslip and proof of employment. In this scenario, the bank has made a reasonable effort to ensure that the personal data collected from Nick is accurate and complete. Ensuring accuracy when collecting personal data from a third party source 16.7 An organisation should also be more careful when collecting personal data about an individual from a source other than the individual in question. It is allowed to take differing approaches to ascertain the accuracy and completeness of personal data it collects depending on the reliability of the source of the data. For example, the organisation may obtain confirmation from the source of the personal data that the source had verified the accuracy and completeness of that personal data. It may also conduct further independent verification if it deems prudent to do so. Example: Nick will be attending an adventure camp for his company's team-building purposes. The adventure camp operator obtains relevant health check-up records from his company to determine whether Nick is sufficiently fit to participate in the adventure activities. The records were dated eight years ago, when Nick first joined the company.	

		In this scenario, the adventure camp company should consider asking Nick for a more recent health record. Similar considerations apply when deciding whether personal data should be updated. Not all types of personal data require updates. Obvious examples include factual data, for example, historical data. However, where the use of outdated personal data in a decision-making process could affect the individual, then it would be prudent for the organisation to update such personal data. Example: A company is considering whether an existing employee, John, should be transferred to take on a different role in its IT department. One of the criteria for the transfer is the possession of certain qualifications and professional certifications. The company has information about John's qualifications and professional certifications that was provided by John (which form part of his personal data) when he joined the company five years before. The company asks John to update them with any new qualifications or certifications he may have obtained in the last five years since joining the company but does not ask him to re-confirm the information about the qualifications he provided when he joined the company. In this scenario, the company is likely to have met its obligation to update John's personal data. Accuracy of derived personal data 16.9 The Commission recognises that organisations may derive personal data from	

		the raw personal data collected either directly from the individual or from third party sources. In such cases, organisations should ensure that the raw personal data is materially accurate before further processing takes place, as well as the accuracy of processing (e.g. computation of mean and median from the range of input data is accurate). Where the derived data involves grouping or labelling individuals based on pre-defined categories and profiles, organisations should ensure that the categorisation and selection criteria (i.e. business rules) are applied accurately at the data processing stage.	
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions		

26	Advisory Guidelines on Application of PDPA to Election Activities	Accuracy Obligation 4.19 A political party or election candidate must make a reasonable effort to ensure that personal data collected by or on behalf of the political party or election candidate is accurate and complete if the personal data is likely to be used by the political party or election candidate to make a decision that affects the individual concerned, or is likely to be disclosed by the political party or election candidate to another organisation.	Retention Limitation Obligation 4.23 A political party and election candidate must cease to retain documents containing personal data, or anonymise it, as soon as it is reasonable to assume that (a) the purpose for which the personal data was collected is no longer being served by retention of the personal data, and (b) retention is no longer necessary for legal or business purposes. 4.24 The PDPA does not prescribe a specific retention period for personal data. When developing or reviewing its retention policy and period for personal data, a political party and election candidate should consider whether one or more of the purposes for which the personal data was collected is still being served by the retention of the personal data, and whether retention of the personal data is necessary for other legal or business purposes. Political parties and election candidates should be mindful not to unnecessarily preserve personal data "just in case" or in order to meet unforeseen circumstances.
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		4 Retention of Physical NRIC 4.1 Given the importance of the NRIC as a national identification document that is issued to all citizens and permanent residents of Singapore, and the impact to the individual should the physical NRIC be misplaced, stolen or used for illegal activities such as identity theft and fraud, organisations should generally not retain an individual's physical NRIC unless the retention of the physical NRIC is required under the law.

28	Advisory Guidelines on Requiring Consent for Marketing Purposes		
29	Advisory Guidelines for Management Corporations		
30	Advisory Guidelines for the Education Sector		
31	Advisory Guidelines for the Social Service Sector	5 The Accuracy Obligation 5.1 Pursuant to the Accuracy Obligation (PDPA section 23), an organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be used by the organisation to make a decision that affects the individual concerned or disclosed by the organisation to another organisation. For more information on the Accuracy Obligation, do refer to Chapter 16 of the Advisory Guidelines on Key Concepts in the PDPA. 5.2 The following examples illustrate the application of the Accuracy Obligation. 5.3 Example: Giving of bursary awards to students based on household income data SSA ABC administers bursary awards to high performing students from lowincome households every year. The information required to assess if a student meets the conditions to receive the bursary award may include the student's household income, CPF contributions from the parents and the student's school examination results. SSA ABC collects the required information every year and do not rely on previous	7 The Retention Limitation Obligation 7.1 The Retention Limitation Obligation requires an organisation to cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data, and the retention is no longer necessary for legal or business purposes. 7.2 The PDPA does not prescribe a specific retention period for personal data. However, SSAs should review the personal data they hold on a regular basis to determine if that personal data is still needed. The retention period for personal data under the PDPA can depend on whether the personal data is required for research or archival purposes that benefit the wider public or a segment of the public. SSAs should not keep personal data "just in case", when it is no longer necessary for the purposes for which the personal data was

		years' information to assess the students' eligibility for the current year. Treatment SSA ABC has put in place the processes and mechanisms to collect the personal data of students every year that the bursary is administered. This ensures that the information used to assess the eligibility of the students for the bursary is up to date and complete such that a reliable assessment can be made. In this case, SSA ABC has complied with the Accuracy Obligation. 5.4 Example: Providing of intervention services based on case diagnosis SSA DEF provides case interventions for families (e.g. domestic abuse, strained relationships, neglected children), where their case officers have consultations with the familiesto understand and administer the appropriate care and support (e.g. intervention programs to help family members reconcile differences, financial assistance, medical care). Personal data that are collected by the case officers and stored in SSA DEF's database may comprise family history, state of relationships, household income and past inflicted injuries. Treatment As the appropriate care and support are provided to the families based on the case diagnosis by officers, it is important that SSA DEF puts in place processes to ensure that the case diagnosis is up to date and complete, for example, case workers follow their agency's standard practice to update the case notes and interventions after significant case milestones	collected or for any legal or business purpose. 7.3 Please refer to Chapter 18 of the Key Concepts Guidelines for more information relating to the Retention Limitation Obligation. The example below illustrate the application of the Retention Limitation Obligation to the social service context. 7.4 Example: Retention of volunteers' data for organisational use SSA ABC engages volunteers over a period of one week to distribute food to elderlies living alone. SSA ABC keeps a record of personal data of the volunteers within their Volunteer Management System (VMS). After the week, SSA ABC retains these personal data as, based on past experience, the volunteers may wish to retrieve their volunteering records in the future, and SSA ABC has assessed based on past experiences that these identifiers (e.g. full name, type of volunteering activity, date(s) of volunteering and number of volunteering hours) are sufficient for such purpose. As SSA ABC is retaining the personal data of volunteers for a valid business purpose, the Retention Limitation Obligation does not require SSA ABC to cease to retain the personal data after the volunteering activity ends. As a good practice, SSA ABC sets an appropriate retention period based on its experience with ex-volunteers requesting access to their volunteering records. At the end of the retention period, the VMS automatically purges these data.

		and close the case promptly when it is resolved or referred to another agency. In general, SSAs shall determine the frequency of case sessions based on the specific circumstances of the cases. SSAs must do their due diligence and reasonably ensure the accuracy of personal data collected from their clients. 5.5 Example: Ensuring the contact information of bone marrow donors are up to date SSA GHI provides bone marrow donation services where they match the DNA patterns of donors with patients in need of a bone marrow transplant. They store the records of DNA patterns together with the contact information of the donors within their database until they are able to match the donor with a patient. After many years have lapsed since the donors' information were obtained, their contact information may be outdated. Treatment As the contact information of the donors are not used by SSA GHI to make a decision that affects the donor but is merely used as a means of communication with the donor, it is not mandatory under the Accuracy Obligation to ensure that the contact information is up to date and complete. On the other hand, donors' DNA patterns are used to match with patients and to make a decision on whether the donor is suitable for bone marrow transplant with a particular patient. However, DNA patterns generally remain the same throughout a person's life and do not need to be updated. As a good practice and for the	

		effectiveness of the bone marrow donation services, SSA GHI can regularly contact the donors via emails or other channels to reaffirm their willingness as a donor and update their contact information if needed.	
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector		
34	Advisory Guidelines for the Healthcare Sector	The Accuracy, Protection, Retention Limitation, Transfer Limitation, Data Breach Notification and Accountability Obligations The Advisory Guidelines on Key Concepts in the PDPA elaborates on these obligations. Like other organisations, healthcare institutions should consider the application of these obligations to their specific contexts. The Accuracy Obligation Pursuant to the Accuracy Obligation (PDPA section 23), an organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be used by the organisation to make a decision that affects the individual concerned or disclosed by the organisation to another organisation. For more information on the Accuracy Obligation, do refer to Chapter 16 of the Advisory Guidelines on Key Concepts in the PDPA. The Protection Obligation According to the Protection Obligation (PDPA section 24), an organisation must	The Accuracy, Protection, Retention Limitation, Transfer Limitation, Data Breach Notification and Accountability Obligations The Advisory Guidelines on Key Concepts in the PDPA elaborates on these obligations. Like other organisations, healthcare institutions should consider the application of these obligations to their specific contexts. The Accuracy Obligation Pursuant to the Accuracy Obligation (PDPA section 23), an organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be used by the organisation to make a decision that affects the individual concerned or disclosed by the organisation to another organisation. For more information on the Accuracy Obligation, do refer to Chapter 16 of the Advisory Guidelines on Key Concepts in the PDPA. The Protection Obligation According to the Protection Obligation (PDPA section 24), an organisation must

		protect personal data in its possession or under its control by making reasonable security arrangements to prevent (i) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (ii) the loss of any storage medium or device on which personal data is stored. For more information on the Protection Obligation, do refer to Chapter 17 of the Advisory Guidelines on Key Concepts in the PDPA. The Retention Limitation Obligation The Retention Limitation Obligation (PDPA section 25) states that an organisation must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that (i) the purpose for which the personal data was collected is no longer being served by retention of the personal data; and (ii) retention is no longer necessary for legal or business purposes. The PDPA does not prescribe a specific retention period for personal data. However, healthcare institutions should review the personal data they hold on a regular basis to determine if that personal data is still needed. The retention period for personal data under the PDPA can depend on whether the personal data is required for research or archival purposes that benefit the wider public or a segment of the public. Healthcare institutions should not keep personal data "just in case", when it is no longer necessary for the	protect personal data in its possession or under its control by making reasonable security arrangements to prevent (i) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (ii) the loss of any storage medium or device on which personal data is stored. For more information on the Protection Obligation, do refer to Chapter 17 of the Advisory Guidelines on Key Concepts in the PDPA. The Retention Limitation Obligation The Retention Limitation Obligation (PDPA section 25) states that an organisation must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that (i) the purpose for which the personal data was collected is no longer being served by retention of the personal data; and (ii) retention is no longer necessary for legal or business purposes. The PDPA does not prescribe a specific retention period for personal data. However, healthcare institutions should review the personal data they hold on a regular basis to determine if that personal data is still needed. The retention period for personal data under the PDPA can depend on whether the personal data is required for research or archival purposes that benefit the wider public or a segment of the public. Healthcare institutions should not keep personal data "just in case", when it is no longer necessary for the

		purposes for which the personal data was collected or for any legal or business purpose. Attention is drawn to Regulation 12(3) of the PHMC Regulations, Regulation 37(1) of the Healthcare Services (General) Regulations, and the MOH's 2022 Revised Guidelines for the Retention Periods of Medical Records. For more information on the Retention Limitation Obligation, do refer to Chapter 18 of the Advisory Guidelines on Key Concepts in the PDPA.	purposes for which the personal data was collected or for any legal or business purpose. Attention is drawn to Regulation 12(3) of the PHMC Regulations, Regulation 37(1) of the Healthcare Services (General) Regulations, and the MOH's 2022 Revised Guidelines for the Retention Periods of Medical Records. For more information on the Retention Limitation Obligation, do refer to Chapter 18 of the Advisory Guidelines on Key Concepts in the PDPA.
35	Advisory Guidelines for the Telecommunicati on Sector		
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		The Retention Limitation Obligation 7 – Retention Limitation Obligation in PDPA An organisation must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that: i. the purpose for which the personal data was collected is no longer being served by retention of the personal data; and ii. retention is no longer necessary for legal or business purposes. 47. The tied agent shall comply with the requirements under the Retention Limitation Obligation pertaining to personal data in his possession or control. In addition, the tied agent shall comply with any applicable retention policies instituted by the life insurer. 48. Where the tied agent has

			collected personal data from an individual or a customer directly or indirectly solely on behalf of the life insurer, he shall: i. file and keep records of the personal data (including the relevant forms which contains the personal data) until the purpose for which the personal data had first been collected is no longer served, or for any other period prescribed by the life insurer in accordance with the Retention Limitation obligation, whichever is later; ii. destroy or anonymise the personal data when the purpose for which the personal data had first been collected is no longer served, or on expiry of the period prescribed by the life insurer in accordance with the Retention Limitation obligation, whichever is later; 49. The tied agent shall destroy the relevant forms and personal data in a secure manner which renders them irretrievable or inaccessible to the tied agent. Examples could include destroying physical copies of the forms by shredding them or anonymising the personal data.9 50. In the event that the tied agent's agency agreement with the insurer is terminated, the agent shall hand over all data and documentation (including all personal data) still in possession of or under control of the tied agent to the life insurer in accordance with the life insurer's handover procedures.

#	Regulation	internal	internal
		drawing up of codes of conduct	record of processing activities
1	Personal Data Protection Act 2012	Policies and practices 12. An organisation must — (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the	

		organisation under this Act; (b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act; (c) communicate to its staff information about the organisation's policies and practices mentioned in paragraph (a); and (d) make information available on request about — (i) the policies and practices mentioned in paragraph (a); and (ii) the complaint process mentioned in paragraph (b).	
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection		

	(Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment		
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems	10 The Accountability Obligation 10.1 The Accountability Obligation refers to how an organisation discharges its responsibility for personal data which it has collected or obtained for processing, or which it has control over. Sections 11 and 12 of the PDPA detail the actions to be carried out by organisations in fulfilment of this obligation16 . 10.2 Among other things, Section 12 of the PDPA requires	

		organisations to develop policies and practices to meet its obligations under the PDPA. Written policies and documentation of processes enable organisations to show that their internal governance and supervision structures as well as operational practices ensure the responsible use of personal data. Such use should either in line with purposes that individuals have been notified of and consented to or for legitimate purposes that a reasonable person would consider appropriate in the circumstances17 . 10.3 Organisations that make use of AI Systems should be transparent and include in their written policies relevant practices and safeguards to achieve fairness and reasonableness18 . The level of detail to be provided should be proportionate to the risks in each use-case, e.g., taking into account potential harm to the individual and the level of autonomy of the AI System. 10.4 Section 12(d) requires organisations to make information about such policies and practices available to individuals upon request. As the raison d'etre for such external communications with consumers is to help build trust with data subjects by demonstrating accountability in compliance with the PDPA, organisations should consider pre-emptively making such written policies available through their website, and not only upon request.	

		Organisations should also consider making policies available in the form of short policy that is simple, clear, and concise. 10.5 Written policies can house more detailed information that organisations ought to provide to obtain meaningful consent19. Where organisations have relied on exceptions to consent, e.g., Business Improvement and Research Exceptions, written policies can also provide information about the practices and safeguards that were adopted to protect the interests of individuals20. Developing industry best practices, such as model cards and system cards, can also form part of an organisation's written policies. 10.6 Written policies also play an important function in education and confidencebuilding, which are necessary ingredients for building consumer trust and confidence. Policies could therefore include behind-the-scenes measures taken to ensure that the personal data is used in a safe and trusted manner within the AI System, such as: a) Measures taken to achieve fairness and reasonableness for recommendations, predictions, and decisions for the benefit of consumers during model development and testing stages. These can include measures relating to bias assessment, ensuring quality of training data or other data governance measures, or the repeatability/reproducibility of results using	

		personal data. b) Safeguards and technical measures taken to protect personal data. These can include measures to protect personal data during model development and testing (e.g., pseudonymisation and data minimisation), or steps to ensure personal data is protected in the AI System via ensuring the security of such systems before and after they are deployed. c) For outcomes that have a higher impact on the individual, organisations may wish to consider whether it is useful to provide information on how proper accountability mechanisms and human agency and oversight have been implemented. It may also be useful to provide information on safety and/or robustness of the AI System i.e., how the AI System will operate when encountering adversarial or unexpected input. 10.7 Information on the above-mentioned measures is not always required. Organisations using personal data for model development and testing, and in deployed AI Systems, should consider adopting measures that a reasonable person would consider appropriate in the circumstances. Having done so, organisations are encouraged to consider providing sufficient information about such measures to build consumer trust and confidence. 10.8 Organisations are generally encouraged to provide more information on data quality	

		and governance measures taken during AI System development. This is only if such information is deemed relevant and doing so does not compromise security, safety, or commercial confidentiality. Information that organisations can consider including are: a) Steps taken to ensure the quality of personal data in the training dataset (e.g., how representative it is of the market and how recently it was compiled) to improve model accuracy and performance; b) Whether model development was conducted using pseudonymised data, and if not, what organisation, process or technical safeguards were adopted to restrict access to personal data to developers and/or testers who had access; c) Whether it was necessary to use personal data when conducting bias assessment to check if protected characteristics, such as race or religion, are well represented in the training dataset or to assess the bias of the training dataset; d) If personal data was used, what process or technical safeguards were adopted to secure the testing environment and to limit access to testers; and e) Whether data minimisation was practised at all stages of model and/or AI System development and testing. Additional resources 10.9 Organisations may wish to refer to the Model AI Governance Framework for further suggestions on managing stakeholder interaction (see in	

		particular Section 3, pages 53 – 55). Organisations may also find the guiding questions and examples on stakeholder interaction provided in Section 5 of the Implementation and SelfAssessment Guide for Organisations helpful. 10.10 Organisations can consider using technical tools such as AI Verify to validate the performance of AI Systems. Information from the testing report can be used to support information that organisations wish to include into their notifications or written policies. For example: a) Results of explainability testing can be used to identify the data features that are most likely to influence the recommendation, prediction, or decision. b) Results of fairness testing can be used to illustrate differences in model outcomes across demographic groups to show that there has not been unreasonable discrimination or bias in the use of personal data by an AI System. This can also be supported by process checks for repeatability/reproducibility. c) Process checks for security can support an organisation's statement in their notification that they have taken steps to ensure that personal data used in an AI System is protected. d) AI Verify also includes process checks that organisations may find useful to validate any claims in their notifications that they have included on accountability/human oversight and safety of the AI System. Robustness testing	

		may also be useful if organisations intend to provide information on the robustness of the AI System in their notification. Where possible, improvements should be introduced. 10.11 It is good practice for organisations to develop processes to regularly review the quality of the information provided, as well as the effectiveness of its notifications, policies, and practices for their intended audience. 10.12 Organisations are also encouraged to perform impact assessments, particularly data protection impact assessments, where these are deemed to be useful. These can help support organisations in their efforts to identify and mitigate data protection risks in an AI System. Organisations may wish to refer to the Commission's Guide on Data Protection Impact Assessments for more guidance on this area.	
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act		
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		

25	Advisory Guidelines on the Do Not Call Provisions		
26	Advisory Guidelines on Application of PDPA to Election Activities	Accountability Obligation 4.31 A political party and election candidate must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available23 . 4.32 As good practice, political parties and election candidates who collect, use or disclose personal data may consider making their data protection policies available via their websites. 4.33 A political party and election candidate should also designate at least one individual responsible for ensuring its compliance with the PDPA (i.e. a data protection officer or "DPO"). The business contact information of that individual has to be made available and as good practice, should be readily accessible and operational during Singapore business hours and in the case of telephone numbers, be Singapore telephone numbers. The intent is to allow individuals to contact the DPO easily for any data protection related queries or concerns, so that the individual's queries or concerns may be addressed in a timely manner.	
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on		

	Requiring Consent for Marketing Purposes		
29	Advisory Guidelines for Management Corporations	Data Protection Policies and Data Protection Officer 2.6 In complying with the PDPA, a MCST is required to develop and implement policies and practices that are necessary for it to meet its obligations under the PDPA, and to make information about the data protection policies and practices available on request16. A MCST is also required to designate at least one individual to be responsible for ensuring its compliance with the PDPA, commonly known as the Data Protection Officer ("DPO")17	
30	Advisory Guidelines for the Education Sector		
31	Advisory Guidelines for the Social Service Sector		
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector		
34	Advisory Guidelines for the Healthcare Sector	The Accountability Obligation The Accountability Obligation (PDPA sections 11 and 12) states that an organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available. For more information on the Accountability Obligation, do refer to Chapter 21	

		of the Advisory Guidelines on Key Concepts in the PDPA.	
35	Advisory Guidelines for the Telecommunication Sector		
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act	The Openness Obligation 9 – Openness Obligation in PDPA An organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available. An organisation is to designate one or more individuals ("data protection officer(s)" or "DPO(s)") to be responsible for ensuring that the organisation complies with the PDPA, and the business contact information of at least one of such individuals designated (or an authorised delegate) shall be made available to the public upon request. An organisation is also required to: (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under the PDPA; (b) develop a process to receive and respond to complaints that may arise with respect to the application of PDPA; (c) communicate to its staff information about the organisation's policies and practices referred to in (a); and (d) make information available on request about policies and practices in (a) and the complaint process in (b).	

		52. The life insurer may designate one or more of its DPOs to provide assistance and support to tied agents in relation to compliance with the PDPA. 53. The life insurer will make available to the public the business contact information of at least one of the DPOs (or authorised delegate). Tied agents should direct any queries relating to the life insurers' compliance with the PDPA, and/or the complaint process to a DPO (or authorised delegate) designated by the life insurer. 54. The life insurer would support its tied agents by setting up the relevant policies and procedures required to achieve (a) to (d) above. A tied agent conducting activities as a representative of the life insurer will need to comply with such policies and procedures, and communicate them to his agency's office staff.	

#	Regulation	internal	internal
		Designation of the data protection officer	Others
1	Personal Data Protection Act 2012	Compliance with Act 11.—(1) In meeting its responsibilities under this Act, an organisation must consider what a reasonable person would consider appropriate in the circumstances. (2) An organisation is responsible for personal data in its possession or under its control. (3) An organisation must designate one or more individuals to be responsible for ensuring that the organisation complies with this Act.	

		(4) An individual designated under subsection (3) may delegate to another individual the responsibility conferred by that designation. (5) An organisation must make available to the public the business contact information of at least one of the individuals designated under subsection (3) or delegated under subsection (4). (5A) Without limiting subsection (5), an organisation is deemed to have satisfied that subsection if the organisation makes available the business contact information of any individual mentioned in subsection (3) in any prescribed manner. [40/2020] (6) The designation of an individual by an organisation under subsection (3) does not relieve the organisation of any of its obligations under this Act.	
2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		

10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment		
19	Advisory Guidelines on use of Personal Data in AI		

	Recommendation and Decision Systems		
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act		
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions		
26	Advisory Guidelines on Application of PDPA to Election Activities	Accountability Obligation 4.31 A political party and election candidate must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available23 . 4.32 As good practice, political parties and election candidates who collect, use or disclose personal data may consider making their data protection policies available via their websites. 4.33 A political party and election candidate should also designate at least one individual responsible for ensuring its compliance with the PDPA (i.e. a data protection officer or "DPO"). The business contact information of that individual has	

		to be made available and as good practice, should be readily accessible and operational during Singapore business hours and in the case of telephone numbers, be Singapore telephone numbers. The intent is to allow individuals to contact the DPO easily for any data protection related queries or concerns, so that the individual's queries or concerns may be addressed in a timely manner.	
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		
29	Advisory Guidelines for Management Corporations	Data Protection Policies and Data Protection Officer 2.6 In complying with the PDPA, a MCST is required to develop and implement policies and practices that are necessary for it to meet its obligations under the PDPA, and to make information about the data protection policies and practices available on request16. A MCST is also required to designate at least one individual to be responsible for ensuring its compliance with the PDPA, commonly known as the Data Protection Officer ("DPO")17 2.7 Responsibilities of the DPO include: a. Putting together a personal data protection policy that sets out the purposes for which	

		personal data may be collected, used or disclosed by the MCST as well as other data protection practices of the MCST to ensure compliance with the PDPA18 and making information about this policy available to all stakeholders19; b. Raising awareness and fostering a culture of data protection among staff (e.g. estate security guard), subsidiary proprietors, estate residents and council as well as executive committee members of the MCST; c. Developing and implementing policies and processes for the proper handling and management of personal data protection related queries and complaints (e.g. access and correction requests) and making information about the complaints process available on request; and d. Alerting the MCST to any risks that might arise with regard to the collection, use or disclosure of personal data. 2.8 In view that the managing agent of the MCST may be appointed to carry out one or more of the MCST's duties or functions, the MCST may designate an individual within the MCST as its DPO, who may in turn delegate certain data protection duties and functions to the managing agent. The MCST remains fully responsible for complying with the PDPA. 2.9 The following section clarifies how the PDPA applies to common scenarios involving the collection, use or disclosure of personal data by MCSTs, and highlights good data protection practices that could be adopted.	

30	Advisory Guidelines for the Education Sector		
31	Advisory Guidelines for the Social Service Sector		
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector		
34	Advisory Guidelines for the Healthcare Sector		
35	Advisory Guidelines for the Telecommunication Sector		
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act	The Openness Obligation 9 – Openness Obligation in PDPA An organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available. An organisation is to designate one or more individuals ("data protection officer(s)" or "DPO(s)")to be responsible for ensuring that the organisation complies with the PDPA, and the business contact information of at least one of such individuals designated (or an authorised delegate) shall be made available to the public upon request.	

		An organisation is also required to: (a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under the PDPA; (b) develop a process to receive and respond to complaints that may arise with respect to the application of PDPA; (c) communicate to its staff information about the organisation's policies and practices referred to in (a); and (d) make information available on request about policies and practices in (a) and the complaint process in (b). 52. The life insurer may designate one or more of its DPOs to provide assistance and support to tied agents in relation to compliance with the PDPA. 53. The life insurer will make available to the public the business contact information of at least one of the DPOs (or authorised delegate). Tied agents should direct any queries relating to the life insurers' compliance with the PDPA, and/or the complaint process to a DPO (or authorised delegate) designated by the life insurer. 54. The life insurer would support its tied agents by setting up the relevant policies and procedures required to achieve (a) to (d) above. A tied agent conducting activities as a representative of the life insurer will need to comply with such policies and procedures, and communicate them to his agency's office staff.	

Data Cross Boarder Dist

#	Regulation	Cross-border data transfer & Exceptions	Data localization
		Provisions for Transborder Data Transfer. What are the exceptions?(e.g., sufficient authorization, transfers based on contracts equivalent to Standard Contract Clauses (SCC) or Binding Corporate Rules (BCR), transfers based on corporate certification, etc.), Transborder transfer assessment (TIA)	Presence or absence of provisions, stipulations regarding the types of data that must be stored in the country
		Provisions for cross boarder data transfer	Provisions on requirement of localization; and Type of data required for localization
1	Personal Data Protection Act 2012	Transfer of personal data outside Singapore 26.—(1) An organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act. (2) The Commission may, on the application of any organisation, by written notice exempt the organisation from any requirement prescribed pursuant to subsection (1) in respect of any transfer of personal data by that organisation. (3) An exemption under subsection (2) — (a) may be granted subject to such conditions as the Commission may specify in writing; and (b) need not be published in the Gazette and may be revoked at any time by the Commission. (4) The Commission may at any time add to, vary or revoke any condition imposed under this section.	

2	Public Sector (Governance) Act 2018		
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021	Requirements for transfer 10.—(1) For the purposes of section 26 of the Act, a transferring organisation must, before transferring an individual's personal data to a country or territory outside Singapore on or after 1 February 2021, take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data is bound by legally enforceable obligations (in accordance with regulation 11) to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the Act. (2) A transferring organisation is taken to have satisfied the requirements of paragraph (1) in respect of an individual's personal data which it transfers to a recipient in a country or territory outside Singapore if — (a) subject to paragraph (3), the individual consents to the transfer of the individual's personal data to that recipient in that country or territory; (b) the individual is deemed to have consented to the disclosure by the transferring organisation of the individual's personal data to that recipient under section	

		15(3), (4), (5), (6), (7) or (8) of the Act; (c) the transfer of the personal data to the recipient is necessary for the personal data to be used or disclosed under Part 1 or paragraph 2 of Part 2 of the First Schedule to the Act, and the transferring organisation has taken reasonable steps to ensure that the personal data so transferred will not be used or disclosed by the recipient for any other purpose; (d) the personal data is data in transit; or (e) the personal data is publicly available in Singapore. (3) For the purposes of paragraph (2)(a), an individual is not taken to have consented to the transfer of the individual's personal data to a country or territory outside Singapore if — (a) the individual was not, before giving his or her consent, given a reasonable summary in writing of the extent to which the personal data to be transferred to that country or territory will be protected to a standard comparable to the protection under the Act; (b) the transferring organisation required the individual to consent to the transfer as a condition of providing a product or service, unless the transfer is reasonably necessary to provide the product or service to the individual; or (c) the transferring organisation obtained or attempted to obtain the individual's consent for the transfer by providing false or misleading information about the transfer, or by using other deceptive or misleading practices. (4) This Part does not prevent an individual from withdrawing any consent given for the	

		transfer of the personal data to a country or territory outside Singapore. Legally enforceable obligations 11.—(1) For the purposes of regulation 10(1), legally enforceable obligations include obligations imposed on a recipient of personal data under — (a) any law; (b) any contract in accordance with paragraph (2); (c) any binding corporate rules in accordance with paragraph (3); or (d) any other legally binding instrument. (2) A contract mentioned in paragraph (1)(b) must — (a) require the recipient to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the Act; and (b) specify the countries and territories to which the personal data may be transferred under the contract. (3) The binding corporate rules mentioned in paragraph (1)(c) — (a) must require every recipient of the transferred personal data that is related to the transferring organisation and does not already satisfy paragraph (1)(a), (b) or (d), to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the Act; (b) must specify — (i) the recipients of the transferred personal data to which the binding corporate rules apply; (ii) the countries and territories to which the personal data may be transferred under the binding corporate rules; and (iii) the rights and obligations	

		provided by the binding corporate rules; and (c) may only be used for recipients that are related to the transferring organisation. (4) For the purposes of paragraph (3)(a) and (c), a recipient of personal data is related to the transferring organisation transferring that personal data if — (a) the recipient, directly or indirectly, controls the transferring organisation; (b) the recipient is, directly or indirectly, controlled by the transferring organisation; or (c) the recipient and the transferring organisation are, directly or indirectly, under the control of a common person. Recipients holding specified certifications 12.—(1) For the purposes of regulation 10(1), a recipient of an individual's personal data in a country or territory outside Singapore is taken to be bound by legally enforceable obligations to provide a standard of protection for the transferred personal data that is at least comparable to the protection under the Act if the recipient holds a specified certification that is granted or recognised under the law of that country or territory to which the personal data is transferred. (2) In this regulation, "specified certification", in relation to a recipient of an individual's personal data, means a certification under — (a) where the recipient is a data intermediary — the Asia-Pacific Economic Cooperation Privacy Recognition for Processors System or the Asia-Pacific Economic Cooperation Cross Border Privacy Rules System; or (b) in any other case — the	

		Asia-Pacific Economic Cooperation Cross Border Privacy Rules System.	
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021		
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's		

	Personal Data in the Digital Environment		
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act	Applicability to Inbound Data Transfers The Data Protection Provisions apply to organisations carrying out activities involving personal data in Singapore. Where personal data is collected overseas and subsequently transferred into Singapore, the Data Protection Provisions will apply in respect of the activities involving the personal data in Singapore6. Example: ABC, an organisation based overseas, has a contractual agreement with JKL, a data hosting company based in Singapore, for JKL to host ABC's client database. The Data Protection Provisions apply in respect of the personal data in the client database when it is in Singapore. Since JKL is acting as ABC's data intermediary in relation to the hosting of the client database pursuant to their contractual agreement, JKL is subject to the Protection, Retention Limitation and Data Breach Notification (in relation to notifying ABC of data breaches without undue delay) Obligations in respect of such hosting. ABC discloses personal data of its clients to DEF, a company based in Singapore, for DEF to conduct its own market research. Since DEF is not a data intermediary, DEF is subject to	

		all the Data Protection Provisions in respect of its collection, use and disclosure of personal data for its purposes. Where personal data originating from outside Singapore is collected by an organisation in Singapore for use or disclosure for its own purposes in Singapore (that is, not as a data intermediary of another organisation), the organisation is required to comply with all Data Protection Provisions from the time it seeks to collect the personal data (if such collection occurs in Singapore) or from the time it brings the personal data into Singapore. This includes obtaining consent for the collection, use and disclosure of the personal data (where such activities will be conducted in Singapore) unless the personal data may be collected, used or disclosed without consent under the PDPA or consent may be deemed. The Commission notes that where personal data is collected outside Singapore, such collection may be subject to the data protection laws of the country or territory in which it was collected (if any). In determining whether an organisation has complied with the Consent and Notification Obligations before collecting, using or disclosing the personal data in Singapore, the Commission will take into account the manner in which the personal data was collected in compliance with such data protection laws. Where personal data collected from outside Singapore is transferred to an organisation in Singapore, the Transfer Limitation Obligation could apply to the latter organisation if it transfers the personal data	

		outside Singapore, although the avenues for compliance depend on whether the personal data is data in transit. Please refer to Chapter 19 on the Transfer Limitation Obligation for more details. The Transfer Limitation Obligation 19.1 Section 26 of the PDPA limits the ability of organisations to transfer personal data to another organisation outside Singapore in circumstances where it relinquishes possession or direct control over the personal data. Such circumstances include transferring personal data to another company within the same group for centralised corporate functions, or to a data intermediary for data processing. In situations where personal data transferred or situated overseas remains in the possession or control of an organisation, the organisation has to comply with all the Data Protection Provisions. Such situations include where an employee travels overseas with customer lists on his notebook; an organisation owns or leases and operates a warehouse overseas for archival of customer records; or an organisation stores personal data in an overseas data centre on servers that it owns and directly maintains. In these examples, the organisation has direct primary obligations under the Data Protection Provisions to, inter alia, protect the personal data, give effect to access and correction requests, and include these overseas data repositories in its data retention policy. 19.2 This is because the Transfer	

		Limitation Obligation is a manifestation of the Accountability Obligation. When an organisation discloses personal data to another organisation, and both are in Singapore, the receiving organisation is subject to the PDPA and has to protect the personal data that it thereby receives. Likewise, when an organisation discloses personal data to its data intermediary, and both are in Singapore, the data intermediary is subject to the Protection, Retention Limitation and Data Breach Notification Obligations for the personal data that it thereby receives. However, when an organisation transfers personal data to another organisation that is outside Singapore (for example, a data intermediary or another company in the same group), the recipient organisation is not subject to the PDPA. The Accountability Obligation requires that the transferring organisation takes steps to ensure that the recipient organisation will continue to protect the personal data that it has received to a standard that is comparable to that established in PDPA. This is the raison d'etre for the Transfer Limitation Obligation. 19.3 Thus, section 26(1) provides that an organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA, i.e. to ensure that organisations provide a standard of protection to transferred personal data that is comparable to the protection under the PDPA. This requirement not to transfer	

		personal data unless in accordance with the prescribed requirements is referred to in these Guidelines as the Transfer Limitation Obligation. Conditions for transfer of personal data overseas. 19.4 The Personal Data Protection Regulations 2021 specify the conditions under which an organisation may transfer personal data overseas. In essence, an organisation may transfer personal data overseas if it has taken appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations or specified certifications to provide the transferred personal data a standard of protection that is comparable to that under the PDPA. 19.5 Legally enforceable obligations may be imposed in two ways. First, it may be imposed on the recipient organisation under: a) any law; b) any contract that imposes a standard of protection that is comparable to that under the PDPA, and which specifies the countries and territories to which the personal data may be transferred under the contract; c) any binding corporate rules that50 require every recipient of the transferred personal data to provide a standard of protection for the transferred personal data that is comparable to that of the PDPA, and which specify (i) the recipients of the transferred personal data to which the binding corporate rules apply; (ii) the countries and territories to which the personal data may be transferred under the binding	

		corporate rules; and (iii) the rights and obligations provided by the binding corporate rules; or d) any other legally binding instrument. 19.6 Second, if the recipient organisation holds a "specified certification" that is granted or recognised under the law of that country or territory to which the personal data is transferred, the recipient organisation is taken to be bound by such legally enforceable obligations. Under the Personal Data Protection Regulations 2021, "specified certification" refers to certifications under the Asia Pacific Economic Cooperation Cross Border Privacy Rules ("APEC CBPR") System, and the Asia Pacific Economic Cooperation Privacy Recognition for Processors ("APEC PRP") System. The recipient is taken to satisfy the requirements under the Transfer Limitation Obligation if: a) it is receiving the personal data as an organisation51 and it holds a valid APEC CBPR certification; or b) it is receiving the personal data as a data intermediary and it holds either a valid APEC PRP or CBPR certification, or both. 19.7 Organisations are encouraged to rely on legally enforceable obligations or specified certifications outlined in paragraphs 19.5 and 19.6, especially when they have an ongoing relationship with the recipient organisation. Legally enforceable obligations provide better accountability. In addition, under the Personal Data Protection Regulations 2021, a transferring organisation is also taken to have satisfied the Transfer Limitation Obligation in certain circumstances. As good	

		practice, organisations are encouraged to rely on these circumstances only if they are unable to rely on legally enforceable obligations or specified certifications: a) the individual whose personal data is to be transferred gives his consent to the transfer of his personal data, after he has been informed about how his personal data will be protected in the destination country52; b) the individual is deemed to have consented to the disclosure by the transferring organisation of the individual's personal data where the transfer is reasonably necessary for the conclusion or performance of a contract between the organisation and the individual, including the transfer to a third party organisation); c) the transfer is necessary for a use or disclosure that is in the vital interests of individuals or in the national interest, and the transferring organisation has taken reasonable steps to ensure that the personal data will not be used or disclosed by the recipient for any other purpose; d) the personal data is data in transit; or e) the personal data is publicly available in Singapore. 19.8 The examples below illustrate certain situations in which organisations may transfer personal data overseas in compliance with the Transfer Limitation Obligation. Example: Organisation ABC is transferring personal data of its customers to its parent company overseas via the group's centralised customer management system. The conditions of the transfer, including the protections that	

		will be accorded to the personal data transferred, are set out in binding corporate rules that apply to both ABC and its head office. ABC has reviewed these binding corporate rules and assessed that they comply with the conditions prescribed under the Personal Data Protection Regulations 2021 and would provide protection that is comparable to the standard under the PDPA. In this case, ABC's transfer of the personal data to its parent company overseas would be in compliance with the Transfer Limitation Obligation. Example: Karen purchases an overseas tour with travel agency DEF. In order to perform its obligation under its contract with Karen to make the necessary hotel reservations, travel agency DEF relies on section 15(6) of the PDPA to transfer her personal data (such as her name, nationality and passport number) overseas to the hotels that Karen will be staying at during the tour. Travel agency DEF's transfer of Karen's personal data in this case would be in compliance with the Transfer Limitation Obligation as it is necessary for the performance of the contract between travel agency DEF and Karen. Example: Cedric is a client of Organisation GHI. GHI notifies Cedric in writing that it is adopting a cloud-based solution to store and analyse its client data, which includes personal data such as clients' identification details, address, contact details and income range, and asks for Cedric's consent to	

		move his client data to the cloud-based solution. GHI also provides Cedric with a written summary of the extent to which Cedric's personal data will be protected to a standard comparable to that under the PDPA, in the countries and territories that it will be transferred to. Should Cedric provide his consent, GHI would be able to transfer his personal data in compliance with the Transfer Limitation Obligation. Example: John is injured in an accident while travelling overseas. To aid John's treatment, his family doctor in Singapore transfers some of his medical records (including personal data such as his identification details, blood type, allergies, and existing medical conditions) to the overseas hospital so that John can receive medical treatment. In this case, the transfer of John's personal data would be in compliance with the Transfer Limitation Obligation as the disclosure to the overseas hospital is necessary to respond to an emergency that threatens John's life, health or safety (pursuant to paragraph 2 under Part 1 of the First Schedule to the PDPA), and John's family doctor has taken reasonable steps to ensure that the personal data transferred will not be used or disclosed by the recipient for any other purpose. Example: Company JKL films a commercial at a location open to the public in Singapore. The commercial captures images of individuals who pass by the filming location. Company JKL wishes to transfer the commercial to its overseas	

		partners for use in an advertising campaign. In this instance, Company JKL's transfer of the commercial would be in compliance with the Transfer Limitation Obligation as the personal data in the commercial would be publicly available to the extent that the filming of images would be reasonably expected at that location53. Example: Alpha.com, a travel website that is based in Singapore, is launching a joint travel promotion with Japanese airline company, Air Bravo. Both organisations determine the specific categories of personal data to be collected from customers for the purpose of the joint promotion. Alpha.com will need to transfer the customers' personal data to Air Bravo, which is located in Japan, for the joint promotion. Air Bravo informs Alpha.com that it is certified under the APEC CBPR System in Japan. Alpha.com carries out due diligence and determines that Air Bravo is indeed certified under the APEC CBPR System by referring to the list of certified organisations on the APEC website (www.cbprs.org). In this case, Alpha.com is taken to have satisfied the requirement under the Transfer Limitation Obligation to ensure that Air Bravo is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to that under the PDPA. Example: Organisation MNO engages a firm based in the US, Company PQR, as a data intermediary to	

		use its CRM system to process and store customers' information. MNO will need to transfer its customers' personal data to Company PQR in the US to use its CRM system. Company PQR informs MNO that it is certified under the APEC CBPR System but not under the APEC PRP System. MNO carries out due diligence and determines that Company PQR is indeed certified under the APEC CBPR System by referring to the list of certified organisations on the APEC website (www.cbprs.org). In this case, MNO is taken to have satisfied the requirement under the Transfer Limitation Obligation to ensure its data intermediary, Company PQR, is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to that under the PDPA. Example: Organisation STU, an e-commerce retailer, engages the services of a data analytics firm based in the US, Company XYZ, as its data intermediary to conduct analyses on its consumers' preferences on its behalf. STU will need to transfer its customers' personal data to Company XYZ in the US to conduct the analyses. Company XYZ informs STU that it is certified under the APEC PRP System. STU carries out due diligence and determines that Company XYZ is indeed certified under the APEC PRP System by referring to the list of certified organisations on the APEC website (www.cbprs.org). In this case, STU is taken to have satisfied the requirement under	

		the Transfer Limitation Obligation to ensure its data intermediary, Company XYZ, is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to that under the PDPA. Example: Company Charlie, a travel agent in Singapore, offers US travel packages with resort stays at Resort Delta, a resort and travel services provider based in the US. Resort Delta determines the specific categories of personal data of customers to be provided for making room reservations for customers. Company Charlie will need to transfer customers' personal data to Resort Delta in the US for their room reservations. Resort Delta informs Company Charlie that it is certified under the APEC PRP System in the US. Company Charlie carries out due diligence and determines that Resort Delta is only certified under the APEC PRP System and not the APEC CBPR System. As Resort Delta is not receiving the personal data as a data intermediary of Company Charlie, Company Charlie may not rely on Resort Delta's APEC PRP certification to transfer personal data to Resort Delta. Company Charlie should consider whether it can rely on any other avenue as set out at paragraph 19.5 above, such as consent given by the customers for the transfer of their personal data or where it is necessary for the performance of a contract between the customers and Company Charlie.	
22	Advisory Guidelines on the		

	Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions		
24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions		
26	Advisory Guidelines on Application of PDPA to Election Activities	Transfer Limitation Obligation 4.25 A political party and election candidate must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA18 . 4.26 A political party or election candidate should ensure that any overseas transfer of personal data as a result of engaging a cloud service provider ("CSP")19 will be done in accordance with the requirements under the PDPA, namely, the organisation could ensure that the CSP it uses only transfers data to locations with comparable data protection regimes, or has legally enforceable obligations to ensure a comparable standard of protection for the transferred personal data20.	
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for		

	Marketing Purposes		
29	Advisory Guidelines for Management Corporations		
30	Advisory Guidelines for the Education Sector	4 The Transfer Limitation Obligation 4.1 Section 26 of the PDPA limits the ability of an organisation to transfer personal data outside Singapore unless in accordance with prescribed requirements ("the Transfer Limitation Obligation"). The conditions under which an organisation may transfer personal data overseas are specified in the Personal Data Protection Regulations 2014. 4.2 An organisation may transfer personal data overseas if it has taken appropriate steps to ensure that it will comply with the Data Protection Provisions in respect of the transferred personal data while such personal data remains in its possession or under its control; and if the personal data is transferred to a recipient in a country or territory outside Singapore, that the recipient is bound by legally enforceable obligations to provide to the personal data transferred a standard of protection that is at least comparable to that under the PDPA (such as obligations imposed under law or contract). 4.3 Organisations may be taken to have satisfied the requirement to take appropriate steps to ensure that the recipient is bound by legally enforceable obligations to provide to the personal data transferred a standard of protection that is at least comparable to that under the PDPA under certain circumstances, such as:	

		a) when the transfer is necessary for the performance of a contract between the transferring organisation and the individual, or to do anything at the individual's request with a view to his entering a contract with the transferring organisation; or b) when the personal data is publicly available in Singapore. 4.4 Please refer to Chapter 19 of the Key Concepts Guidelines and the aforementioned Regulations for more information on the Transfer Limitation Obligation. 4.5 The following examples illustrate the application of the Transfer Limitation Obligation. While each example illustrates reliance on particular avenues to transfer personal data overseas, an education institution is not precluded from relying on other avenues to transfer personal data in compliance with the Transfer Limitation Obligation in the respective scenarios. 4.6 Example: Transferring personal data of research participant to overseas research partners School ABC is conducting a research study in collaboration with School XYZ, an education institution located in Country X. As part of their collaboration, School ABC will transfer the personal data of individual research participants to School XYZ for the latter's analysis. School ABC provides each potential research participant with a written summary of the extent to which his personal data will be protected to a standard comparable to that under the PDPA in Country X and asks each potential research participant whether he consents to the transfer of his personal	

		data to School XYZ in Country X. In such circumstances, School ABC may transfer a participant's personal data to School XYZ in compliance with the Transfer Limitation Obligation should the participant provide his consent. 4.7 Example: Transferring student data overseas for an exchange programme School DEF intends to send its students' personal data to School MNO in Country Y for the administration of an exchange programme between the two schools. School DEF reviews the obligations under Country Y's data protection law that School MNO is subject to, and determines that School MNO would be bound by legally enforceable obligations to provide a standard of protection to its students' personal data that is comparable to the PDPA. School DEF may transfer the personal data to School MNO in compliance with the Transfer Limitation Obligation in such circumstances. Alternatively, School DEF may also be taken to have transferred a student's personal data to School MNO in compliance with the Transfer Limitation Obligation, if it provides the student with a written summary of the extent to which his personal data will be protected to a standard comparable to that under the PDPA in Country Y, and obtains consent from the student. 4.8 Example: Transferring teaching staff's research history to reviewers overseas School GHI wishes to transfer a document describing the research achievements of Ben, a member of its teaching staff, to reviewers overseas, to assess if he should be promoted	

		in accordance with the terms of his employment contract. To the extent that the transfer is necessary for the performance of the employment contract between School GHI and Ben, School GHI may transfer the personal data to School MNO in compliance with the Transfer Limitation Obligation.	
31	Advisory Guidelines for the Social Service Sector	8 The Transfer Limitation Obligation 8.1 The Transfer Limitation Obligation (PDPA section 26) states that an organisation must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA. For more information on the Transfer Limitation Obligation, do refer to Chapter 19 of the Advisory Guidelines on Key Concepts in the PDPA. 8.2 The examples below illustrate certain situations in which organisations may transfer personal data overseas in compliance with the Transfer Limitation Obligation. 8.3 Example: Transferring clients' personal data across borders for research to improve welfare services SSA ABC provides welfare services to clients in Singapore and intends to transfer clients' personal data out of Singapore to their headquarters situated in another country via the group's centralized clients' management system. The agency headquarters is accumulating the data from various countries for the purpose of conducting demographic research to improve the welfare services administered to their clients in the region. Treatment SSA ABC has to ensure that it takes appropriate	

		steps to ensure that their agency headquarters situated overseas is bound by legally enforceable obligations or specified certifications to provide the transferred personal data a standard of protection that is comparable to that under the PDPA. Since SSA ABC and the agency headquarters belong under the same group, they may rely on binding corporate rules. The conditions of the transfer, including protections that will be accorded to the personal data transferred, can be set out in binding corporate rules that apply to both SSA ABC and the agency headquarters. In this case, SSA ABC's transfer of clients' personal data to its agency headquarters would be in compliance with the Transfer Limitation Obligation. If the data that is being exchanged between SSA ABC across borders is aggregated and does not contain personal identifiers of clients, such data will not be considered personal data, and the Transfer Limitation Obligation of the PDPA will not apply. 8.4 Example: Outsourcing outreach services for donors to overseas call centre SSA 123 operates in and provides charity services to clients in Singapore. In terms of reaching out to donors to financially support their charity programs, they have outsourced the outreach services to a call centre located in a neighbouring country. SSA 123 will have to transfer the personal data (e.g. name, contact details) of regular donors with an existing relationship with them to the call centre to inform about new charity programs and to encourage donations.	

		Treatment The call centre that processes donors' personal data given by SSA 123 for outreach services can be considered a data intermediary of SSA 123. Therefore, SSA 123 is responsible for complying with all the obligations under the PDPA in respect of personal data processed by the call centre. To ensure that the overseas call centre is bound by legally enforceable obligations to provide the transferred personal data of donors a standard of protection that is comparable to that under the PDPA, SSA 123 may establish a written contract with the overseas call centre that imposes such a standard. 8.5 Example: Engaging a cloud service provider to store personal data of clients SSA DEF engages a cloud service provider (CSP) to store a sizeable volume of personal data of their clients (e.g. name, age, gender, home address, household income). Before signing up for its services, SSA DEF enquired on where the data centres that store the personal data of their clients are located, and they understand from the CSP that the data centres are located overseas. Treatment Where the CSP is processing personal data on behalf and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing, the CSP is considered a data intermediary. SSA DEF is still responsible for complying with all obligations under the PDPA in respect of personal data processed by the CSP on its behalf and for its	

		purposes. The CSP is specifically subject to the Protection, Retention Limitation and Data Breach Notification Obligations under the PDPA with regards to the personal data that it processes or hosts in data centres outside Singapore. Any issues of compliance can be provided for in the written contract between SSA DEF and its CSP. Before signing up for the CSP's services to store clients' personal data, SSA DEF can notify its clients in writing that it is adopting a cloud-based solution to store its clients' personal data, and asks for the clients' consent to move their data to the cloud-based solution. SSA DEF also provides its clients with a written summary of the extent to which their data will be protected to a standard comparable to that under the PDPA, in the countries and territories that it will be transferred to. Should the clients provide their consent, SSA DEF would be able to rely on the CSP's services to transfer its clients' personal data to data centres located overseas in compliance with the Transfer Limitation Obligation. Alternatively, SSA DEF can use the services of a CSP that has legally enforceable obligations to ensure a comparable standard of protection for the transferred personal data. For example, SSA DEF can carry out due diligence and determine if the CSP is certified under the APEC CBPR system in the overseas country, which will ensure that the clients' personal data stored in the overseas data centres are protected to a standard comparable to the PDPA. SSA	

		DEF can refer to the list of CBPR-certified organisations on the APEC website (www.cbprs.org). For more information on using cloud service providers in relation to the PDPA, please refer to Chapter 9 of the Advisory Guidelines on the PDPA for Selected Topics.	
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector		
34	Advisory Guidelines for the Healthcare Sector	The Transfer Limitation Obligation The Transfer Limitation Obligation (PDPA section 26) states that an organisation must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA. For more information on the Transfer Limitation Obligation, do refer to Chapter 19 of the Advisory Guidelines on Key Concepts in the PDPA.	
35	Advisory Guidelines for the Telecommunication Sector		
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act	The Transfer Limitation Obligation 8 – Transfer Limitation Obligation in PDPA An organisation must not transfer personal data to a country or territory outside Singapore except in	

		accordance with the requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA. 51. Unless instructed by the life insurer and/or in accordance with the life insurer's internal policy and procedures, the tied agent shall not transfer any personal data outside Singapore.	

#	Regulation	Governent Access
		National Security Law, Cybersecurity Law Provisions
		Provision allowed govt to access regulated data/to not comply to data regulation
1	Personal Data Protection Act 2012	Powers of investigation 50.—(1) The Commission may, upon complaint or of its own motion, conduct an investigation under this section to determine whether or not an organisation or a person is complying with this Act, including a voluntary undertaking given by the organisation or person under section 48L(1). [40/2020] (2) The powers of investigation under this section of the Commission and the inspectors are set out in the Ninth Schedule. (3) The Commission may suspend, discontinue or refuse to conduct an investigation under this section if it thinks fit, including but not limited to any of the following circumstances: (a) the complainant has not complied with a direction under section 48G(2); (b) the parties involved in the matter have mutually agreed to settle the matter; (c) any party involved in the matter has commenced legal proceedings against another party in respect of any contravention or alleged contravention of this Act by the other party; (ca) the Commission accepts a voluntary undertaking given by an organisation or a person under section 48L(1) in relation to the matter; (d) the Commission is of the opinion that the matter may be more appropriately investigated by another regulatory authority and has referred the matter to that authority; (e) the Commission is of the opinion that — (i) a complaint is frivolous or vexatious or is not made in good faith; or (ii) any other circumstances warrant refusing to conduct, suspending or discontinuing the investigation. [40/2020] (3A) To avoid doubt, despite subsection (3)(ca), the Commission may conduct or resume an investigation under this section at any

		time if an organisation or a person fails to comply with a voluntary undertaking given by the organisation or person under section 48L(1) in relation to any matter. [40/2020] (4) An organisation must retain records relating to an investigation under this section for one year after the conclusion of the investigation or any longer period specified in writing by the Commission.
2	Public Sector (Governance) Act 2018	Authority to share 6.—(1) Where a data sharing direction is given to a Singapore public sector agency — (a) the Singapore public sector agency and every officer of that agency; and (b) where the Singapore public sector agency is a public body, the members of the public body, are authorised to share the information under the control of the Singapore public sector agency with another Singapore public sector agency to the extent permitted by the data sharing direction despite any obligation as to confidentiality under the common law. (2) However, subsection (1) does not override any obligation as to confidentiality because of legal privilege or contract. (3) To avoid doubt, this Act is not intended to prevent or discourage the sharing of information by Singapore public sector agencies as permitted or required by or under any Act or other law (apart from this Act).
3	Telecommunications Act 1999	Sealing of telecommunication system or equipment, etc. 58.—(1) Where it appears to any police officer not below the rank of sergeant or any employee authorised by the Authority that it is not practicable to remove from where it is found any telecommunication system or equipment or any radio-communication system or equipment seized by him or her under section 57 by reason of its nature, size or amount, he or she may by any means seal the telecommunication system or equipment or the radio-communication system or equipment. (2) Any person who, without lawful authority, breaks, tampers with or damages any seal referred to in subsection (1), or removes any telecommunication system or equipment or any radio-communication system or equipment which has been sealed under that subsection, or attempts to do so, shall be guilty of an offence.
4	CRIMINAL PROCEDURE CODE 2010	Power to order production of any document or other thing 20.—(1) Where a police officer of or above the rank of sergeant, or an authorised person, considers that any document or thing (other than a document or thing in the custody of the Postal Authority, a public postal licensee or the public parcel locker network operator) is necessary or desirable for any investigation, inquiry, trial or other proceeding under this Code, the police officer or authorised person may — (a) issue a written order to require a person in whose possession or power the document or thing is believed to be — (i) to produce the document or thing at the time and place stated in the order;

		(ii) to give a police officer or an authorised person access to the document or thing; or (iii) in the case of a document or thing that is in electronic form — (A) to produce a copy of the document or thing, at the time and place stated in the order; or (B) to give a police officer or an authorised person access to a copy of the document or thing; or (b) in the case of a document or thing that is contained in or available to a computer — issue a written order to require a person who is believed to have power to access the document or thing from that computer — (i) to produce a copy of the document or thing, at the time and place stated in the order; or (ii) to give a police officer or an authorised person access to a copy of the document or thing. Power to access computer 39.—(1) A police officer or an authorised person investigating an arrestable offence may, at any time — (a) access, inspect and check the operation in or from Singapore of a computer (whether in Singapore or elsewhere) that the police officer or authorised person has reasonable cause to suspect is or has been used in connection with, or contains or contained evidence relating to, the arrestable offence; (b) use any such computer in or from Singapore, or cause any such computer to be used in or from Singapore — (i) to search any data contained in or available to such computer; and (ii) to make a copy of any such data; (c) prevent any other person from gaining access to, or using, any such computer (including by changing any username, password or other authentication information required to gain access to the computer); or (d) order any person — (i) to stop accessing or using or to not access or use any such computer; or (ii) to access or use any such computer only under such conditions as the police officer or authorised person may specify. [19/2018] (2) The police officer or authorised person may also order any of the following persons to provide any assistance mentioned in subsection (2A): (a) any person whom the police officer or authorised person reasonably suspects of using, or of having used, the computer in connection with the arrestable offence; (b) any person having charge of, or otherwise concerned with the operation of, the computer; (c) any person whom the police officer or authorised person reasonably believes has knowledge of or access to any username, password or other authentication information required to gain access to the computer. [19/2018] (2A) For the purposes of subsection (2), the types of assistance are

		as follows: (a) assistance to gain access to the computer (including assistance through the provision of any username, password or other authentication information required to gain access to the computer); (b) assistance to prevent a person (other than the police officer or authorised person) from gaining access to, or using, the computer, including assistance in changing any username, password or other authentication information required to gain access to the computer. [19/2018] (2B) Without limiting subsection (1), where the police officer or authorised person knows that the computer mentioned in that subsection is located outside Singapore, or does not know whether that computer is located in or outside Singapore, the police officer or authorised person — (a) may exercise the powers under subsection (1) in relation to that computer, or any data contained in or available to that computer, if — (i) the owner of that computer consents to the exercise of those powers; or (ii) the police officer or authorised person obtains access to that computer through the exercise of any power of investigation under any written law, such as in any of the following circumstances: (A) the access is obtained with the assistance mentioned in subsection (2A)(a) provided under subsection (2) by a person having charge of, or otherwise concerned with the operation of, that computer; (B) the access is obtained through an active connection with, or through any username, password or other authentication information stored in, another computer, which has been seized under section 35 and accessed under subsection (1); (C) the access is obtained through any username, password or other authentication information contained in any document seized under section 35; (D) the access is obtained through any username, password or other authentication information provided in any statement made by any person examined under section 22; and (b) may exercise the powers under subsection (1)(b) in relation to any data contained in or available to that computer, if the owner of that data consents to the exercise of those powers. [19/2018] (3) Any person who obstructs the lawful exercise by a police officer or an authorised person of any power under subsection (1)(a), (b) or (c), or who fails to comply with any order of the police officer or authorised person under subsection (1)(d) or (2), shall be guilty of an offence and shall be liable on conviction — (a) in any case where the person is a body corporate, a limited liability partnership, a partnership or an unincorporated association — to a fine not exceeding $10,000; or (b) in any other case — to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 6 months or to both. [19/2018] (4) An offence under subsection (3) is an arrestable offence.

		(5) A person who had acted in good faith under subsection (1) or in compliance with a requirement under subsection (1)(d) or (2) shall not be liable in any criminal or civil proceedings for any loss or damage resulting from the act. [19/2018] (6) In this section and section 40 — "authorised person" means — (a) a forensic specialist appointed under section 65A of the Police Force Act 2004, or any other person, who is authorised in writing by the Commissioner of Police for the purposes of this section or section 40 or both; or (b) any officer of a prescribed law enforcement agency who is authorised in writing, by the head of that law enforcement agency, for the purposes of this section or section 40 or both; "prescribed law enforcement agency" means a law enforcement agency prescribed, by order in the Gazette, by the Minister charged with the responsibility for that law enforcement agency.
5	Cybersecurity Act 2018	Emergency cybersecurity measures and requirements 23.—(1) The Minister may, if satisfied that it is necessary for the purposes of preventing, detecting or countering any serious and imminent threat to — (a) the provision of any essential service; or (b) the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore, by a certificate under the Minister's hand, authorise or direct any person or organisation specified in the certificate (called in this section the specified person) to take such measures or comply with such requirements as may be necessary to prevent, detect or counter any threat to a computer or computer system or any class of computers or computer systems. (2) The measures and requirements mentioned in subsection (1) may include, without limitation — (a) the exercise by the specified person of the powers in sections 39(1)(a) and (b) and (2)(a) and (b) and 40(2)(a), (b) and (c) of the Criminal Procedure Code (Cap. 68); (b) requiring or authorising the specified person to direct another person to provide any information that is necessary to identify, detect or counter any such threat, including — (i) information relating to the design, configuration or operation of any computer, computer program or computer system; and (ii) information relating to the cybersecurity of any computer, computer program or computer system; (c) providing to the Minister or the Commissioner any information (including real-time information) obtained from any computer controlled or operated by the specified person, or obtained by the specified person from another person pursuant to a measure or requirement under paragraph (b), that is necessary to identify, detect or counter any such threat, including — (i) information relating to the design, configuration or operation of any computer, computer program or computer system; and (ii) information relating to the cybersecurity of any computer, computer program or computer system; and

		(d) providing to the Minister or the Commissioner a report of a breach or an attempted breach of cybersecurity of a description specified in the certificate under subsection (1), relating to any computer controlled or operated by the specified person. (3) Any measure or requirement mentioned in subsection (1), and any direction given by a specified person for the purpose of taking any such measure or complying with any such requirement — (a) does not confer any right to the production of, or of access to, information subject to legal privilege; and (b) subject to paragraph (a), has effect despite any obligation or limitation imposed or right, privilege or immunity conferred by or under any law, contract or rules of professional conduct, including any restriction on the disclosure of information imposed by law, contract or rules of professional conduct. (4) A specified person who, without reasonable excuse, fails to take any measure or comply with any requirement directed by the Minister under subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both. (5) Any person who, without reasonable excuse — (a) obstructs a specified person in the taking of any measure or in complying with any requirement under subsection (1); or (b) fails to comply with any direction given by a specified person for the purpose of the specified person taking any such measure or complying with any such requirement, shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both. (6) No civil or criminal liability is incurred by — (a) a specified person for doing or omitting to do any act if the specified person had done or omitted to do the act in good faith and for the purpose of or as a result of taking any measure or complying with any requirement under subsection (1); or (b) a person for doing or omitting to do any act if the person had done or omitted to do the act in good faith and for the purpose of or as a result of complying with a direction given by a specified person for the purpose of taking any such measure or complying with any such requirement. (7) The following persons are not considered to be in breach of any restriction upon the disclosure of information imposed by law, contract or rules of professional conduct: (a) a specified person who, in good faith, obtains any information for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection, or who discloses any information to the Minister or the Commissioner, in compliance with any requirement under that subsection; (b) a person who, in good faith, obtains any information, or discloses any information to a specified person, in compliance with a direction given by the specified person for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection. (8) The following persons, namely:

		(a) a specified person to whom a person has provided information in compliance with a direction given by the specified person for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection; (b) a person to whom a specified person provides information in compliance with any requirement under subsection (1), must not use or disclose the information, except — (i) with the written permission of the person from whom the information was obtained or, where the information is the confidential information of a third person, with the written permission of the third person; (ii) for the purpose of preventing, detecting or countering a threat to a computer, computer system or class of computers or computer systems; (iii) to disclose to any police officer or other law enforcement authority any information which discloses the commission of an offence under this Act or any other written law; or (iv) in compliance with a requirement of a court or the provisions of this Act or any other written law. (9) Any person who contravenes subsection (8) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both. (10) Where an offence is disclosed in the course of or pursuant to the exercise of any power under this section — (a) no information for that offence may be admitted in evidence in any civil or criminal proceedings; and (b) no witness in any civil or criminal proceedings is obliged — (i) to disclose the name, address or other particulars of any informer who has given information with respect to that offence; or (ii) to answer any question if the answer would lead, or would tend to lead, to the discovery of the name, address or other particulars of the informer. (11) If any book, document, data or computer output which is admitted in evidence or liable to inspection in any civil or criminal proceedings contains any entry in which any informer is named or described or which may lead to the informer's discovery, the court must cause those entries to be concealed from view or to be obliterated so far as may be necessary to protect the informer from discovery.
6	Workplace Safety and Health (Medical Examinations) Regulations 2011	Designated workplace doctor to report results of medical examinations to employers 9.—(1) It shall be the duty of the designated workplace doctor to report the results of the medical examination of a person employed in any hazardous occupation in a workplace to the responsible person of that person. (2) The report under paragraph (1) shall be submitted by the designated workplace doctor in a form determined by the Commissioner. (3) The responsible person of a person employed in any hazardous occupation shall — (a) keep the report of every medical examination of that person

		employed in a hazardous occupation for a period of at least 5 years from the date of the medical examination; and (b) whenever required by the Commissioner within the period referred to in sub-paragraph (a), make available to the Commissioner the report or a summary of the report, as the Commissioner may specify. (4) Any person who contravenes paragraph (1), (2) or (3) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000.
7	Banking Act 1970	Privacy of customer information 47.—(1) Customer information must not, in any way, be disclosed by a bank in Singapore or any of its officers to any other person except as expressly provided in this Act. [5/2016] (2) A bank in Singapore or any of its officers may, for such purpose as may be specified in the first column of the Third Schedule, disclose customer information to such persons or class of persons as may be specified in the second column of that Schedule, and in compliance with such conditions as may be specified in the third column of that Schedule.
8	PERSONAL DATA PROTECTION REGULATIONS 2021	
9	Personal Data Protection (Appeal) Regulations 2021	
10	Personal Data Protection (Composition of Offences) Regulations 2021	
11	Personal Data Protection (Do Not Call Registry) Regulations 2013	
12	Personal Data Protection (Enforcement) Regulations 2021	
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021	
14	Personal Data Protection (Prescribed Healthcare	

	Bodies) Notification 2015	
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014	
16	Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020	
17	Personal Data Protection (Statutory Bodies) Notification 2013	
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment	
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems	
20	Introduction to the Guidelines	
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act	
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics	
23	Advisory Guidelines on Enforcement of Data Protection Provisions	PART IV: INVESTIGATIONS 16. Circumstances under which the Commission may commence an investigation 16.1 Section 50 of the PDPA sets out the Commission's powers of investigation in respect of contraventions of the PDPA. In general, the Commission may commence an investigation either upon receiving a complaint from an individual

		against an organisation or of its own motion. 16.2 Where the Commission receives a complaint or other information that indicates that an organisation has, or may have, contravened the PDPA, the Commission will first consider whether the matter may be more appropriately resolved in the manner set out in Part II of these Guidelines, that is, by resolving the underlying dispute between the complainant and the organisation. If so, the Commission may adopt the measures described in Part II before deciding whether to commence an investigation. In addition, where a complaint relates to a matter that may be reviewed by the Commission under section 48H(1) of the PDPA (i.e. a refusal to provide access to or correct personal data; fees required in relation to access or correction requests; or a failure to provide access or correction within a reasonable time), the Commission will generally conduct a review instead of an investigation. In such circumstances, the Commission may proceed on the complainant's complaint as if it was an application for a review or it may require the complainant to submit an application for a review. 16.3 The Commission may commence an investigation into the conduct of an organisation if the Commission considers that an investigation is warranted, based on the information it has obtained (whether through a complaint or from any other source). In deciding whether to commence an investigation, the Commission will generally consider whether any of the following factors indicate that an investigation should be conducted: (a) whether the organisation may have failed to comply, whether intentionally, negligently or for any other reason or cause, with all or a significant part of its obligations under the PDPA; (b) whether the organisation's conduct36 indicates a systemic failure by the organisation to comply with the PDPA or to establish and maintain the necessary policies and procedures to ensure its compliance; (c) the number of individuals who are, or may be, affected by the organisation's conduct;

		(d) the impact of the organisation's conduct on the complainant or any individual who may be affected including, for example, whether the complainant or affected individual(s) may have suffered a loss, injury or other damage as a result of the organisation's contravention of the PDPA or whether they may have been exposed to a significant risk that they may suffer such a loss, injury or damage; (e) whether the organisation had previously contravened the PDPA or may have failed to implement the necessary corrective measures to prevent the recurrence of a previous contravention; (f) where the complainant had previously approached the organisation to seek a resolution of the issues in the complainant but failed to reach a resolution; (g) where the Commission has sought to facilitate dispute resolution between the complainant and the organisation, whether the complainant and the organisation agreed to participate in the dispute resolution process, their conduct during the dispute resolution process and the outcome of the dispute resolution process; (h) where a review has been commenced by the Commission, whether the organisation has complied with its obligations under the Enforcement Regulations in relation to a review, the organisation's conduct during the review and the outcome of the review; (i) the public interest; and (j) any other factor that, in the Commission's view, indicates that an investigation should or should not be commenced. 16.4 In addition, section 50(3) of the PDPA lists some situations in which the Commission may refuse to conduct an investigation. These include (amongst others) situations where: (a) the Commission has issued a direction under section 48G(2) of the PDPA to a complainant to attempt to resolve the complaint in the way directed by the Commission and the complainant has not complied with the direction; (b) the parties have mutually agreed to settle the matter; (c) the complainant has commenced legal proceedings against the

		organisation in respect of the contravention or alleged contravention of the PDPA by the organisation; (d) the Commission accepts a voluntary undertaking given by an organisation or a person under section 48L(1) of the PDPA in relation to the matter; or (e) the Commission is of the opinion that: (i) the complaint is frivolous or vexatious or is not made in good faith; or (ii) any other circumstances warrant refusing to conduct an investigation. 16.5 For the avoidance of doubt, the Commission may commence an investigation notwithstanding that the complainant and the organisation have resolved the issues in the complaint or that the complaint is withdrawn by the complainant if there are other factors that indicate, in the Commission's view, that an investigation should be conducted. These may include (without limitation) the factors noted in paragraph 16.3 (a) to (j) above. 16.6 Where the Commission has conducted a review under section 48H of the PDPA and made a decision or issued a direction under section 48H(2) of the PDPA, the Commission will generally not commence an investigation in relation to the organisation's compliance with section 21 or 22 of the PDPA unless there appears to the Commission to be a significant non-compliance with section 21 or 22 of the PDPA or there are exceptional circumstances which, in the Commission's view, indicate that an investigation should be commenced. For this purpose, a significant non-compliance with section 21 or 22 of the PDPA may include the following: (a) systemic failure on the part of the organisation including (without limitation) where an organisation does not have any processes in place to comply with section 21 or 22 of the PDPA; or (b) intentional non-compliance with section 21 or 22 of the PDPA or a decision or direction under section 48H(2) of the PDPA, for example, where an organisation has sought, through its processes, to deny individuals' requests for reasons that are not permitted under the PDPA. 16.7 The Commission may, in certain circumstances, commence an investigation of its own motion. This may include (without limitation) situations where the

		Commission receives information concerning the conduct of an organisation. In such situations, the Commission may, if it considers it appropriate, proceed with an investigation of its own motion based on the information received. 17. Making a complaint to the Commission 17.1 A complaint concerning a contravention or possible contravention of the PDPA may be made to the Commission by providing the relevant information and, where applicable, copies of documents supporting the complaint. A complainant may also use the form provided on the Commission's website to assist him in lodging the complaint. 17.2 As a complaint may result in formal action being taken by the Commission against an organisation that has infringed the PDPA, complainants should note that they may be required to give a formal statement and appear before the Commission in relation to the statement or other matters within their knowledge. 18. Commission's powers of investigation 18.1 The Commission's powers of investigation are set out in the Ninth Schedule to the PDPA. In brief, these include: 18.1.1 the power to require production of documents and information37; 18.1.2 the power to require the attendance of persons, and to orally examine and take statements from them38 ; 18.1.3 the power to enter premises without a warrant;39 and 18.1.4 the power to enter premises with a warrant.40 These powers are further described in the following sections of these Guidelines. 18.2 In general, the Commission may use its powers of investigation to obtain from any organisation (including organisations that are not the subject of the Commission's investigation) any information that the Commission considers relates to any matter relevant to an investigation. The Commission's powers of investigation may also be exercised by an inspector appointed by the Commission. 18.3 All organisations and individuals are required to comply with any notice or other requirement imposed by the Commission pursuant to its powers of investigations (described further in the following paragraphs). In this regard, any individual who obstructs or impedes the Commission in the exercise of its powers,

		or who knowingly or recklessly makes a false statement to the Commission, or who knowingly attempts to mislead the Commission, shall be guilty of an offence under the PDPA and is liable, upon conviction, to a fine not exceeding S$10,000 or to imprisonment for a term not exceeding 12 months or to both. Organisations that are found to have committed such an offence are liable to a fine not exceeding S$100,000.41 Further, any individual who, without reasonable excuse, neglects or refuses to provide any information or produce any document to the Commission or attend before the Commission, shall be guilty of an offence under the PDPA and is liable, upon conviction, to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding 6 months or to both. Organisations that are found to have committed such an offence are liable to a fine not exceeding S$10,000. 42 19. Power to require production of documents and information 19.1 Under paragraph 1 of the Ninth Schedule to the PDPA, the Commission may, by notice in writing to any organisation, require the organisation to produce any document or information which the Commission considers relates to any matter relevant to an investigation. 19.2 The term "document" includes "information recorded in any form". This definition includes records stored in any form, electronic or otherwise, for example, on a computer. 19.3 A notice issued by the Commission under paragraph 1 of the Ninth Schedule shall: 19.3.1 specify the document or information, or the category of documents or information,43 which the organisation is required to produce; and 19.3.2 indicate the purpose for which the specified document or specified information is required by the Commission. 19.4 Such a notice may also: 19.4.1 specify the time and place at which any document or information is to be produced or provided to the Commission; 19.4.2 specify the manner and form in which any document or information is to be produced or provided; 19.4.3 require the organisation, or any past or present officer or

		employee of the organisation, to provide an explanation of the document; and 19.4.4 if the document is not produced, require the organisation or any past or present officer or employee of the organisation to state, to the best of his knowledge and belief, where it is. 19.5 Under paragraph 1(4) of the Ninth Schedule, the Commission is empowered to take copies of or extracts from any document that is produced pursuant to its notice. 19.6 The Commission may issue a notice under paragraph 1 of the Ninth Schedule to any person or entity falling within the definition of the term "organisation" in the PDPA. This includes any individual (including, without limitation, sole proprietors and partners of a partnership), company, association or body of persons, corporate or unincorporated.44 As noted above, this may also include present or past officers or employees of an organisation, including volunteers and persons who are or were working under an unpaid volunteer relationship). 45 19.7 The Commission may also issue a written notice to any person to produce any information or document believed to be in their custody or control which is relevant to an investigation. The information or document must be provided within the time and in the manner specified in the notice. 46 19.8 All individuals, companies, associations or other bodies of persons to whom such a notice is issued are required to comply with the notice.47 19.9 A person or organisation may receive multiple notices requiring the production of documents or information during the course of an investigation. For example, an organisation may be required to produce further information or documents after consideration of the documents produced in response to an earlier notice. 20. Power to require attendance of persons, and to orally examine and take statements 20.1 The Commission may by written notice, require any person within Singapore, who appears to be acquainted with the facts or circumstances of a matter pertaining to an investigation, to attend before the Commission. 48

		20.2 The Commission may also orally examine any person who appears to be acquainted with the facts or circumstances of the matter. 49 A statement made by any person so examined will be: 20.2.1 reduced to writing; 20.2.2 read over to the person; 20.2.3 interpreted to him in a language that the person understands (if the person does not understand English; and 20.2.4 after correction (if necessary), be signed by the person. 50 21. Power to enter premises without a warrant 21.1 Under paragraph 2 of the Ninth Schedule to the PDPA, the Commission is empowered to enter premises without a warrant in connection with an investigation. Depending on the circumstances, entry may be effected with or without giving the occupier of the premises prior notice of the intended entry. 21.2 An inspector appointed by the Commission (and any other persons he may require to assist him) may, in connection with any investigation, enter any premises after giving the occupier of the premises a written notice which: 21.2.1 gives at least 2 working days' notice of the intended entry; and 21.2.2 indicates the subject matter and purpose of the investigation. 21.3 If the inspector has taken all such steps as are reasonably practicable to give such written notice but has not been able to do so, he (or any person assisting him) may enter the premises if he has reasonable grounds for suspecting that the premises are, or have been, occupied by an organisation which is being investigated in relation to a contravention of the PDPA. In such cases, the inspector must produce: 21.3.1 evidence of his appointment; and 21.3.2 a document containing the subject matter and purpose of the investigation. 21.4 Upon such entry, the inspector (or any person assisting him) may: 21.4.1 take with him any equipment which appears to him to be necessary; 21.4.2 in relation to any document which he considers relates to any matter relevant to the investigation: (a) require any person on the premises to produce the document and provide an explanation of it (if produced); (b) require any person to state, to the best of his knowledge and belief, where the document may be found; (c) take copies of, or extracts from, any document which is produced;

		(d) take any step which appears to be necessary for the purpose of preserving or preventing interference with the document; and (e) require any information which is stored in any electronic form and is accessible from the premises and which he considers relates to any matter relevant to the investigation, to be produced in a visible and legible form, which can be taken away. 22. Power to enter premises with a warrant Conditions for issuance of warrant 22.1 Under paragraph 3 of the Ninth Schedule to the PDPA, the Commission is empowered to enter and search premises without prior notice, upon production of a warrant. 22.2 Paragraph 3 of the Ninth Schedule to the PDPA identifies three circumstances in which a court may issue a warrant to authorise an inspector appointed by the Commission (and any other persons assisting him) to enter and search the premises specified in the warrant. The court must be satisfied that there are reasonable grounds for suspecting that there are, on any premises, documents: 22.2.1 which have not been produced, although the Commission has required production, either by written notice (paragraph 1 of the Ninth Schedule) or in the course of an inspection without a warrant (paragraph 2 of the Ninth Schedule); 22.2.2 which would be concealed, removed, tampered with or destroyed if required to be produced by written notice (paragraph 1 of the Ninth Schedule); or 22.2.3 which an inspector (or any person assisting him) could have required to be produced in the course of an inspection without a warrant (paragraph 2 of the Ninth Schedule), but was unable to effect entry into the premises. Scope of the power 22.3 The warrant will authorise an inspector (and any other persons he may require to assist him) to do all or any of the following: 22.3.1 enter the premises using such force as is reasonably necessary; 22.3.2 search any person on those premises if there are reasonable grounds for believing that that person has in his possession any document, equipment or article which has a bearing on the investigation; 22.3.3 search the premises and take copies of, or extracts from, any document appearing to be of the kind in respect of which the warrant was

		granted (as described in paragraph 22.2 above); 22.3.4 take possession of any document appearing to be of the kind in respect of which the warrant was granted if such action appears to be necessary for preserving the document or preventing interference with it, or if it is not reasonably practicable to take copies of the document on the premises. Upon request for a copy of the document by the person from whom possession of such document was taken, the inspector may provide such copy. Documents taken may be retained for a period of not more than 3 months; 22.3.5 take any other steps which appear necessary in order to preserve the documents or prevent interference with them including requiring equipment and storage facilities to be sealed if necessary; 22.3.6 require any person to provide an explanation of any document appearing to be of the kind in respect of which the warrant was granted or to state to the best of his knowledge and belief where such document may be found; 22.3.7 require any information, which is stored in any electronic form and is accessible from the premises, and which the investigator considers relates to any matter relevant to the investigation, to be produced in a visible and legible form which can be taken away; and 22.3.8 remove from the premises for examination any equipment or article which relates to any matter relevant to the investigation. Where appropriate, the inspector may, instead of removing from the premises such equipment or articles, allow them to be retained on the premises subject to conditions. 22.4 In addition, where a warrant is granted to enter premises pursuant to a reasonable suspicion that, if prior written notice under paragraph 1 of the Ninth Schedule were given, documents would be concealed, removed, tampered with or destroyed (i.e. in the circumstances described in paragraph 21.2.2 above), then, if the court is satisfied that it is reasonable to suspect that there are also other documents on the premises which relate to the investigation, the warrant will authorise the

		actions mentioned in paragraph 21.4 above to be taken in relation to such other documents. 22.5 The inspector entering the premises (and any other persons he may require to assist him) may take with him any equipment, which appears to him to be necessary. 23. Suspension or conclusion of an investigation 23.1 Section 50(3) of the PDPA lists various situations in which the Commission may suspend or discontinue an investigation. These include the situations described in paragraphs 16.4(a) – (e) above. 23.2 Where the Commission proceeds with an investigation, the Commission will consider the information and evidence it has obtained and determine if an organisation has contravened the PDPA. The Commission's powers where it finds an organisation has contravened the PDPA are set out in the next Part of these Guidelines. 24. Public communications 24.1 Organisations that intend to issue any media releases or public disclosure of matters related to the alleged breach are advised to consider whether the content would hinder the ongoing investigations and to also provide the Commission with a copy of the materials before their release.
24	Joint Advisory on ALTDOS	
25	Advisory Guidelines on the Do Not Call Provisions	
26	Advisory Guidelines on Application of PDPA to Election Activities	
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers	
28	Advisory Guidelines on Requiring Consent for	

	Marketing Purposes	
29	Advisory Guidelines for Management Corporations	
30	Advisory Guidelines for the Education Sector	
31	Advisory Guidelines for the Social Service Sector	
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire	
33	Advisory Guidelines for the Real Estate Agency Sector	
34	Advisory Guidelines for the Healthcare Sector	
35	Advisory Guidelines for the Telecommunication Sector	
36	Joint Technical Advisory on LockBit 3.0	
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act	

Penalties

#	Regulation	Corporate Punishments	Individual Punishments
		Forms of penalties (e.g., recommendations for corrective action, public penalties, fines, confiscation of assets and income, data deletion, data processing, business suspension, etc.)	Penalties (penalties, fines, demotion, etc.)

		Forms of penalties on corporate	Forms of penalties on individual
1	Personal Data Protection Act 2012	Financial penalties 48J.—(1) Subject to subsection (2), the Commission may, if it is satisfied that — (a) an organisation has intentionally or negligently contravened any provision of Part 3, 4, 5, 6, 6A or 6B; or (b) a person has intentionally or negligently contravened — (i) any provision of Part 9; or (ii) section 48B(1), require, by written notice, the organisation or person (as the case may be) to pay a financial penalty. [40/2020] (2) Subsection (1) does not apply in relation to any contravention of a provision of this Act, the breach of which is an offence under this Act. [40/2020] (3) A financial penalty imposed on an organisation under subsection (1)(a) must not exceed the maximum amount to be prescribed, which in no case may be more than the following: (a) in the case of a contravention on or after the date of commencement of section 24 of the Personal Data Protection (Amendment) Act 2020 by an organisation whose annual turnover in Singapore exceeds $10 million — 10% of the annual turnover in Singapore of the organisation; (b) in any other case — $1 million. [Act 40 of 2020 wef 01/10/2022] (4) A financial penalty imposed on a person under subsection (1)(b)(i) must not exceed the maximum amount to be prescribed, which in no case may be more than the	Offences and penalties 51.—(1) A person shall be guilty of an offence if the person — (a) makes a request under section 21(1) to obtain access to personal data about another individual without the authority of that other individual; (b) makes a request under section 22(1) to change personal data about another individual without the authority of that other individual; or (c) subject to subsection (1A), gives a porting organisation a data porting request under section 26H(1) to transmit personal data about another individual to a receiving organisation without the authority of that other individual. [40/2020] (1A) Subsection (1)(c) does not apply to an individual who gives a data porting request under section 26H(1), in the individual's personal or domestic capacity, to transmit any user activity data or user-provided data about the individual even though the user activity data or user-provided data (as the case may be) includes personal data about another individual. [40/2020] (2) A person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 12 months or to both. (3) An organisation or person commits an offence if the organisation or person — (a) with an intent to evade a request under section 21 or 22, disposes of, alters, falsifies, conceals or destroys, or directs another person to dispose of, alter, falsify, conceal or destroy,

		following: (a) in the case of an individual — $200,000; (b) in any other case — $1 million. [40/2020] [Act 40 of 2020 wef 01/10/2022] (4A) A financial penalty imposed on a person under subsection (1)(b)(ii) must not exceed the maximum amount to be prescribed, which in no case may be more than the following: (a) in the case of an individual — $200,000; (b) in the case of a contravention on or after the date of commencement of section 24 of the Personal Data Protection (Amendment) Act 2020 by a person whose annual turnover in Singapore exceeds $20 million — 5% of the annual turnover of the person in Singapore; (c) in any other case — $1 million. [Act 40 of 2020 wef 01/10/2022] (5) For the purposes of subsections (3) and (4), different maximum amounts may be prescribed in respect of contraventions of different provisions of this Act. [40/2020] (5A) For the purposes of subsections (3)(a) and (4A)(b), the annual turnover in Singapore of an organisation or a person (as the case may be) is the amount ascertained from the most recent audited accounts of the organisation or person available at the time the financial penalty is imposed on that organisation or person. [Act 40 of 2020 wef 01/10/2022] (6) The Commission must, in	a record containing — (i) personal data; or (ii) information about the collection, use or disclosure of personal data; (b) obstructs or hinders the Commission, an inspector or an authorised officer in the performance of any function or duty, or the exercise of any power, under this Act; (ba) without reasonable excuse, neglects or refuses to provide any information or produce any document which the organisation or person is required by or under this Act to provide or produce to the Commission or an inspector; (bb) without reasonable excuse, neglects or refuses to attend before the Commission or an inspector as required by or under this Act; or (c) makes a statement, or provides any information or document, to the Commission, an inspector or an authorised officer under this Act, which the organisation or person knows, or ought reasonably to know, to be false or misleading in any material particular. [22/2016; 40/2020] (4) An organisation or person that commits an offence under subsection (3)(a) is liable — (a) in the case of an individual, to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 12 months or to both; and (b) in any other case, to a fine not exceeding $50,000. [40/2020] (5) An organisation or person that commits an offence under subsection (3)(b) or (c) is liable — (a) in the case of an individual, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both;

		determining the amount of a financial penalty imposed under subsection (1), have regard to, and give such weight as the Commission considers appropriate to, all of the following matters: (a) the nature, gravity and duration of the non-compliance by the organisation or person, as the case may be; (b) the type and nature of the personal data affected by the non-compliance by the organisation or person, as the case may be; (c) whether the organisation or person (as the case may be), as a result of the non-compliance, gained any financial benefit or avoided any financial loss; (d) whether the organisation or person (as the case may be) took any action to mitigate the effects and consequences of the non-compliance, and the timeliness and effectiveness of that action; (e) whether the organisation or person (as the case may be) had, despite the non-compliance, implemented adequate and appropriate measures for compliance with the requirements under this Act; (f) whether the organisation or person (as the case may be) had previously failed to comply with this Act; (g) the compliance of the organisation or person (as the case may be) with any direction given under section 48I or 48L(4) in relation to remedying or mitigating the effect of the non-compliance; (h) whether the financial penalty to be imposed is proportionate and effective, having regard to achieving compliance and deterring	and (b) in any other case, to a fine not exceeding $100,000. (6) An organisation or a person that commits an offence under subsection (3)(ba) or (bb) is liable — (a) in the case of an individual — to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 6 months or to both; and (b) in any other case — to a fine not exceeding $10,000. General penalties 56. A person guilty of an offence under this Act for which no penalty is expressly provided shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a continuing offence, to a further fine not exceeding $1,000 for every day or part of a day during which the offence continues after conviction.

		non-compliance with this Act; (i) the likely impact of the imposition of the financial penalty on the organisation or person (as the case may be), including the ability of the organisation or person to continue the usual activities of the organisation or person; (j) any other matter that may be relevant.	
2	Public Sector (Governance) Act 2018		Unauthorised disclosure and improper use of information 7.—(1) If — (a) an individual discloses, or the individual's conduct causes disclosure of, information under the control of a Singapore public sector agency to another person (whether or not a Singapore public sector agency); (b) the disclosure is not authorised by any data sharing direction given to the Singapore public sector agency; (c) the individual is a relevant public official of the Singapore public sector agency at the time of the disclosure; and (d) the individual does so — (i) knowing that the disclosure is not in accordance with that direction; or (ii) reckless as to whether the disclosure is or is not in accordance with that direction, the individual shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both. (2) In proceedings for an offence under subsection (1), it is a defence for the defendant to prove, on a balance of probabilities, that the defendant disclosed, or caused the disclosure of, information under the control of a Singapore public sector agency — (a) as permitted or required by or

			under an Act or other law (apart from this Act); or (b) as authorised or required by an order of court. (3) If an individual — (a) makes use of information under the control of the Singapore public sector agency when he or she is a relevant public official of a Singapore public sector agency or a contractor (or an employee thereof) supplying goods or services to a Singapore public sector agency; and (b) obtains a gain for himself or herself as a result of that use, the individual shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both. (4) In proceedings for an offence under subsection (3), it is a defence for the defendant to prove, on a balance of probabilities, that the information under the control of a Singapore public sector agency was, at the time of its use by the defendant, generally available information. (5) In this section — "disclose", in relation to information, includes provide access to information; "gain" means — (a) a gain in property or a supply of services (whether temporary or permanent); or (b) an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of remuneration; "generally available information" means information that consists of readily observable matter, including information that consists of deductions, conclusions or inferences made

			or drawn from readily observable matter; "relevant public official", for a Singapore public sector agency, means — (a) an officer of the Singapore public sector agency; (b) a member of a Group 1, Group 2 or Group 3 public body which is that Singapore public sector agency, or of the governing body of such a public body; or (c) the chief executive of a Group 1, Group 2 or Group 3 public body which is that Singapore public sector agency. Unauthorised re-identification of anonymised information 8.—(1) If — (a) an individual takes any action to re-identify or cause re-identification of the person to whom anonymised information under the control of a Singapore public sector agency relates; (b) the re-identification is not authorised by any data sharing direction given to the Singapore public sector agency; (c) the individual is a relevant public official of the Singapore public sector agency at the time of taking that action; and (d) the individual does so — (i) knowing that the re-identification is not authorised by that data sharing direction; or (ii) reckless as to whether the re-identification is or is not authorised by that data sharing direction, the individual shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both. (2) In proceedings for an offence under subsection (1), it is a defence to the charge for the

			accused to prove, on a balance of probabilities, that — (a) the information on the identity is publicly available; or (b) the action to re-identify or cause re-identification is — (i) permitted or required by or under an Act or other law (apart from this Act); or (ii) authorised or required by an order of court. (3) In this section — "anonymised information" means any information which is in anonymised or de-identified form; "relevant public official" has the meaning given by section 7(5).
3	Telecommunications Act 1999		
4	CRIMINAL PROCEDURE CODE 2010		
5	Cybersecurity Act 2018		
6	Workplace Safety and Health (Medical Examinations) Regulations 2011		
7	Banking Act 1970		
8	PERSONAL DATA PROTECTION REGULATIONS 2021		
9	Personal Data Protection (Appeal) Regulations 2021		
10	Personal Data Protection (Composition of Offences) Regulations 2021		
11	Personal Data Protection (Do Not Call Registry) Regulations 2013		
12	Personal Data Protection (Enforcement) Regulations 2021	Maximum amount of financial penalties 10A.—(1) The maximum amount prescribed for the	

		purposes of section 48J(3) of the Act is — (a) in the case of a contravention on or after 1 October 2022 by an organisation whose annual turnover in Singapore exceeds $10 million — 10% of the annual turnover in Singapore of the organisation; and (b) in any other case — $1 million. (2) The maximum amount prescribed for the purposes of section 48J(4) of the Act is — (a) in the case of an individual — $200,000; and (b) in any other case — $1 million. (3) The maximum amount prescribed for the purposes of section 48J(4A) of the Act is — (a) in the case of an individual — $200,000; (b) in the case of a contravention on or after 1 October 2022 by a person whose annual turnover in Singapore exceeds $20 million — 5% of the annual turnover of the person in Singapore; and (c) in any other case — $1 million.	
13	Personal Data Protection (Notification of Data Breaches) Regulations 2021		
14	Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015		
15	Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014		
16	Personal Data Protection (Prescribed Law		

	Enforcement Agency) Notification 2020		
17	Personal Data Protection (Statutory Bodies) Notification 2013		
18	Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment		
19	Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		
20	Introduction to the Guidelines		
21	Advisory Guidelines on Key Concepts in the Personal Data Protection Act		
22	Advisory Guidelines on the Personal Data Protection Act for Selected Topics		
23	Advisory Guidelines on Enforcement of Data Protection Provisions	PART VI: DIRECTIONS AND FINANCIAL PENALTIES 26. Power to issue directions to secure compliance 26.1 The Commission's power to issue directions to secure an organisation's compliance with the PDPA is set out in section 48I of the PDPA. In particular: 26.1.1 Section 48I(1) of the PDPA provides that the Commission may, if it is satisfied that an organisation is not complying with any of the Data Protection Provisions or any person has not complied or is not	

		complying with any of the DNC Provisions, give the organisation or person (as the case may be) such directions as the Commission thinks fit in the circumstances to ensure the organisation's compliance with that provision. 26.1.2 Section 48I(2) of the PDPA further provides that the Commission may (without prejudice to section 48I(1) of the PDPA) give an organisation that is not complying with any Data Protection Provisions, any or all of the following directions: (a) to stop collecting, using or disclosing personal data in contravention of the PDPA; (b) to destroy personal data collected in contravention of the PDPA; or (c) to comply with any direction of the Commission under section 48H(2) of the PDPA. 26.2 In general, the directions that the Commission may give under section 48I of the PDPA are likely to fall within the following types: 26.2.1 Directions to remedy the organisation's contravention, that is, by requiring the organisation to take corrective action, for example, by requiring the infringing organisation to cease its use of personal data collected in contravention of the PDPA; 26.2.2 Directions to prevent or reduce the possibility of harm (or further harm) to individuals who are (or may be) affected by the organisation's contravention; and 26.2.3 Directions to rectify an organisation's processes, for	

		example, by requiring the infringing organisation to take certain measures so that it will be brought into compliance with the PDPA. 26.3 In the event an organisation does not comply with a direction under section 48I of the PDPA, the Commission is empowered under section 48M of the PDPA to enforce the direction by registering it in the District Court. Please refer to section 30 of these Guidelines for more information on the enforcement of the Commission's directions. 27. Written notice to pay financial penalties 27.1 Under Section 48J of the PDPA, the Commission may require an organisation to pay a financial penalty of up to S$1 million or 10% of the organisation's annual turnover in Singapore53, whichever is higher, for any intentional or negligent contravention of the Data Protection Provisions. 54 27.2 For any intentional or negligent contravention of the DNC Provisions involving the use of dictionary attacks and address-harvesting software 55 , the Commission may require payment of a financial penalty of up to S$200,000 in the case of an individual and in the case of an organisation, a financial penalty of up to S$1 million or 5% of the organisation's annual turnover in Singapore56, whichever is higher. Contraventions of other DNC provisions57, the Commission may require payment of a financial penalty of up to S$200,000 in the case	

		of an individual and in other cases, a financial penalty of up to S$1 million. 27.3 An organisation's annual turnover in Singapore will be ascertained from the most recent audited accounts of the organisation available at the time the financial penalty is imposed58. 27.4 In determining the amount of financial penalty to be imposed59, the Commission will consider the following, among others: 27.4.1 Assessthe incident based on the principles of harm and culpability, drawn from the factors set out in section 48J of the PDPA: (a) Harm includes the number of affected individuals, categories of affected personal data, duration of the incident etc. The Commission will determine the level of harm in accordance with the above factors, (b) Culpability refers to the organisation's conduct in the incident and the Commission will consider the nature of the specific breach of the PDPA as well as the organisation's overall compliance with the PDPA. 27.4.2 Consider other relevant factors calling for an increase and/or decrease of the financial penalty. Such factors will take into account whether the organisation or person took any action to mitigate the effects and consequences of the noncompliance, and the timeliness and effectiveness of that action, whether the organisation or person had previously failed to comply with the PDPA etc. 27.5 Table 1 below provides	

		some of the past Commission Decisions60 in which the factors from section 48J(6) of the PDPA were considered in the process of determining the financial penalties.	
24	Joint Advisory on ALTDOS		
25	Advisory Guidelines on the Do Not Call Provisions		
26	Advisory Guidelines on Application of PDPA to Election Activities		
27	Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers		
28	Advisory Guidelines on Requiring Consent for Marketing Purposes		
29	Advisory Guidelines for Management Corporations		
30	Advisory Guidelines for the Education Sector		
31	Advisory Guidelines for the Social Service Sector		
32	Advisory Guidelines on In-vehicle Recordings by Transport Services for Hire		
33	Advisory Guidelines for the Real Estate Agency Sector		

34	Advisory Guidelines for the Healthcare Sector		
35	Advisory Guidelines for the Telecommunicatio n Sector		
36	Joint Technical Advisory on LockBit 3.0		
37	LIA Code of Conduct for Tied Agents of Life Insurers on the Singapore Personal Data Protection Act		

l) Thailand

Legal system overview

#		Translation	Purpose
			What purpose does the legal system serve?(e.g. cybersecurity)
		Google translation or Translation by certain organization	
1	Constitution of the Kingdom Of Thailand	Translation by certain organization	Prescribing rights, duties and framework for Thais
2	Personal Data Protection Act 2019	Translation by certain organization	Providing the framework for personal data protection regulations
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)	Google translation	Providing measures to maintain the security of personal data controllers
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)	Google translation	Providing criteria and methods for preparing to make and maintain records of personal data processing activities for personal data processors
5	PDPC Notification on the exemption	Google translation	Providing exemptions from recording records of personal

	from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		data controllers who are small business
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565	Google translation	Providing procedure for data subject to make complaint in case the data handler violates or fails to comply with the law and regulation on personal data
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565	Google translation	Providing rules and methods of personal data breach notification for data handler
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	Google translation	Providing for activites necessary to check personal information or systems regularly
9	Guideline for obtaining consent from data subjects according to the PDPA	Google translation	Providing guideline for requesting consent from the data subject according to the Personal Data Protection Act
10	Guideline for notifying purposes and details for collecting personal data from the data subjects	Google translation	Providing guidelines for notifying objectives and details of collecting personal data from the owner of personal data

	according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562	Google translation	Providing questions and answers on the implementation of the PDPA 2019
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)	Google translation	Providing list of entities that are exempted from some articles of PDPA
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)	Google translation	Providing characteristics, businesses, or organizations which are exempted from some articles of the Personal Data Protection Act B.E. 2562 (2019)
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)	Google translation	Providing responsibility of who is exempt from he Personal Data Protection Act B.E. 2019

16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other	Google translation	Providing measure for the collection of personal data for purpose relating to research or statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	Google translation	Providing the criteria for protecting personal data sent or transferred abroad under Art.28 of the Personal Data Protection Act B.E. 2562 (2019)
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	Google translation	Providing the criteria for protecting personal data sent or transferred abroad under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)
19	Notification of the Personal Data Protection	Google translation	Providing criteria regarding protection measures for the collection of personal

	Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		information regarding criminal history
20	Electronic Transactions Act, B.E. 2544 (2001)	Translation by certain organization	To define principle, regulations, responsible entities, penalties of electronic transaction for business and commercial purpose
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)	Translation by certain organization	
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)	Translation by certain organization	
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)	Translation by certain organization	
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)	Translation by certain organization	To define responsible entities and penalties of misconduct of computer system utilization including import, export, counterfeit of data etc.
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)	Translation by certain organization	
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of	Google translation	To determine the nature and method of sending and the nature and amount of information, frequency, and method of computer or electronic mail transmission. which does not cause annoyance to the recipient

	information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)	Google translation	To specify notification procedures Stopping the spread of computer data and removal of computer data from the service provider's computer system
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)	Google translation	To determine the criteria, time period, and procedures for suspending the conduct of distribute or delete computer data of officials or service providers as the court has ordered to be suppressed.
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)	Google translation	To improve the criteria for maintaining computer traffic data of service providers to be appropriate for the current economic, social, and technological conditions
30	The Special Case Investigation Act B.E. 2547 (2004)	Translation by certain organization	To determine the authority responsible for Special Case Investigation and its principles and power

31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)	Translation by certain organization	
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)	Translation by certain organization	To determine public administration in emergency situations
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	Google translation	To determine the criteria for protecting the rights of telecommunications service users regarding Personal information Right to privacy and freedom to communicate with each other via telecommunications
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications	Google translation	To set a guideline protecting the rights of users of telecommunications services regarding personal data.
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)	Google translation	To prevent and suppress Technology Crimes and to protect people who have been deceived and lost their property through the phone or other methods
36	The Credit Information Business Operation Act B.E. 2545 (2002)	Translation by certain organization	To define principle, regulations, responsibility, penalties of credit business and financial institutions regarding the customer data management, utilization, disclosure
37	The Credit Information Business Operation Act	Translation by certain organization	

	No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)	Translation by certain organization	
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)	Translation by certain organization	
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)	Translation by certain organization	
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)	Translation by certain organization	
42	The Child Protection Act B.E. 2546 (2003)	Translation by certain organization	To give pretection and welfare of the child, and define responsible entities and penalties of any misconduct
43	The National Health Act B.E. 2550 (2007)	Translation by certain organization	To define principle, consumer rights, responsible entities, penalties of national health management and operation
44	The Payment System Act B.E. 2560 (2017)	Translation by certain organization	To define principle, responsibility, penalties of payment system business including business operation, management, personal data security
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules	Google translation	To set out guidelines and standard of market conduct including corporate management, customer management, business operation, data privacy
46	The Notification of the Office of Insurance Commission Re: Rules, Methods	Translation by certain organization	To set out standard, method of offering of life Insurance for sale including sale process, advertiseing, customer data security

	for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)	Translation by certain organization	To set out standard, method of offering of non-life Insurance for sale including sale process, advertiseing, customer data security
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)	Google translation	To set out guideline of personal data protection including data collection, storage, security, utilization, etc. for life insurance
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)	Google translation	To set out guideline of personal data protection including data collection, storage, security, utilization, etc. for non-life insurance
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for	Google translation	To set out guideline of personal data protection including data collection, storage, security, utilization, etc. for loss adjuster business

	Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)	Translation by certain organization	To define definition, protection, responsible entities, penalties of trade secret and information
52	Trade Secret Act (No.2) B.E. 2558 (2015)	Translation by certain organization	

#		Format	Target Business
		Apart from law is there any other type of regulations e.g. guidelines, ordinances issued to ensure lead time before the law is actually enforced?	Does the law target specific industry or in general? Is it clearly stated in the regulations?
		Regulation level	Industry
1	Constitution of the Kingdom Of Thailand	Law	General
2	Personal Data Protection Act 2019	Law	General
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)	Notification	General
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)	Notification	General
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)	Notification	General
6	Rules of the PDPC re: the Filing, Refusal of	Notification	General

	Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565	Notification	General
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	Notification	General
9	Guideline for obtaining consent from data subjects according to the PDPA	Guideline	General
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA	Guideline	General
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal	Guideline	General

	Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)	Royal decree	General
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)	Royal decree	General
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)	Notification	General
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or	Notification	General

	Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	Notification	General
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	Notification	General
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized	Notification	General

	Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)	Laws	General
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)	Laws	General
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)	Laws	General
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)	Laws	General
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)	Laws	General
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)	Laws	General
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)	Notification	General
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of	Notification	General

	the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)	Notification	General
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)	Notification	General
30	The Special Case Investigation Act B.E. 2547 (2004)	Laws	General
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)	Laws	General
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)	Laws	General
33	The Notification of the National Telecommunicati ons Commission Re: Measures to Protect Telecommunicati	Notification	Telecommunication

	ons Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)		
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications	Guideline	Telecommunication
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)	Laws	General
36	The Credit Information Business Operation Act B.E. 2545 (2002)	Laws	Finance
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)	Laws	Finance
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)	Laws	Finance
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)	Laws	Finance
40	The Credit Information Business Operation Act	Laws	Finance

	No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)	Laws	Finance
42	The Child Protection Act B.E. 2546 (2003)	Laws	General
43	The National Health Act B.E. 2550 (2007)	Laws	General
44	The Payment System Act B.E. 2560 (2017)	Laws	Finance
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules	Notification	Finance
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)	Notification	Finance
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent,	Notification	Finance

	Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)	Notification	Finance
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)	Notification	Finance
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)	Notification	Finance
51	Trade Secret Act B.E. 2545 (2002)	Laws	Commerce
52	Trade Secret Act (No.2) B.E. 2558 (2015)	Laws	Commerce

#		Government Authorities	Jurisdiction
		Which regulatory authority has jurisdiction over regulation?	Cyber security, data security, personal information protection, etc.
		Name of ministry/organization	Similar to purpose?
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019	Minister of Digital Economy and Society	Personal Information, Data security
3	PDPC Notification on security	Data Protection Committee	Personal Information, Data security

	measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)	Personal Data Protection Committee	Personal Information, Data security
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)	Personal Data Protection Committee	Personal Information, Data security
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565	Personal Data Protection Committee	Personal Information
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565	Personal Data Protection Committee	Personal Information
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act	Personal Data Protection Committee	Personal Information

	B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA	Personal Data Protection Committee	Personal Information
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA	Personal Data Protection Committee	Personal Information
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562	The Office of Personal Data Protection Committee	Personal Information, Data security
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)	Minister of Digital Economy and Society	Personal Information
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)	Minister of Digital Economy and Society	Personal Information

15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)	Personal Data Protection Committee	Personal Information, Data security
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other	Personal Data Protection Committee	Personal Information, Data security
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	Personal Data Protection Committee	Personal Information, Cross-boarder data transfer
18	Notification of the Personal	Personal Data Protection Committee	Personal Information, Cross-boarder data transfer

	Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566	Personal Data Protection Committee	Personal Information
20	Electronic Transactions Act, B.E. 2544 (2001)	Section 6. The Prime Minister shall have charge and control of the execution of this Act.	Data security, Personal information
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		Data security, Personal information
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		Data security, Personal information
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)	Section 6. The Minister of Digital Economy and Society shall have charge and control of the execution of this Act.	Data security, Personal information
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		Cyber security
25	COMPUTER-RELATED CRIME	Section 4. The Minister of Digital Economy and Society shall have charge and control of the	Cyber security

	ACT (NO. 2), B.E. 2560 (2017)	execution of this Act and shall have the powers to appoint competent officials and issue Ministerial Regulations and Notifications in the execution of this Act.	
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)	The Minister of Digital Economy and Society	Data security
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)	The Minister of Digital Economy and Society	Data security
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service	The Minister of Digital Economy and Society	Data security

	providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)	The Minister of Digital Economy and Society	Data security
30	The Special Case Investigation Act B.E. 2547 (2004)	Section 4. The Minister of Justice shall take charge and control of the execution of this Act and shall have power to issue Ministerial Regulations and Rules for implementing this Act	Special case investigation (not directly related to DFFT)
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)	Section 4. The Minister of Justice shall take charge and control of the execution of this Act and shall have power to issue Ministerial Regulations and Rules for implementing this Act	Special case investigation (not directly related to DFFT)
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)	Section 19. The Prime Minister shall have charge and control of the execution of this Emergency Decree	Public Administration in a State of Emergency (not directly related to DFFT)
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	National Broadcasting and Telecommunication Commission	Personal information
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy	National Broadcasting and Telecommunication Commission	Personal information

	Rights and Freedom of Communications		
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)	Section 14 The Prime Minister and the Minister of Digital Economy and Society Acting in accordance with this Royal Dec	Cyber security
36	The Credit Information Business Operation Act B.E. 2545 (2002)	Section 5 The Minister of Finance shall be in charge of the enforcement of this Act, and shall be empowered to issue notifications for implementation of this Act. Such a notification shall be enforced upon its publication in the Government Gazette.	Data security
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		Data security
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		Data security
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		Data security
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		Data security
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		Data security
42	The Child Protection Act B.E. 2546 (2003)	Section 6. The Minister of Social Development and Human Security, the Minister of Interior,	Child personal information

		the Minister of Education, and the Minister of Justice shall be in charge for the enforcement of this Act, and shall, in relation to their respective Ministers, have the power to appoint Competent Officials and issue Ministerial Regulation or rules to enable the implementation of this Act for matters which relate to such Ministry. Ministerial Regulation or rules shall be enforced from the time of its publication in the Government Gazette.	
43	The National Health Act B.E. 2550 (2007)	Section 4. The Prime Minister and the Minister of Public Health shall have charge and control of the execution of this Act, and shall have power to issue Ministerial Regulation for the implementation of this Act. Such Ministerial Regulations shall come into force upon their publication in the Government Gazette	Personal information
44	The Payment System Act B.E. 2560 (2017)	Section 4 The Minister of Finance shall be in charge of the execution of this Act.	Personal information, Business information
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules	Bank of Thailand	Personal information
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)	Office of Insurance Commission	Personal information
47	The Notification of the Office of	Office of Insurance Commission	Personal information

	Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)	Office of Insurance Commission	Personal information
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)	Office of Insurance Commission	Personal information
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)	Office of Insurance Commission	Personal information
51	Trade Secret Act B.E. 2545 (2002)	Section 4 The Minister of Agriculture and Co-operative, the Minister of Commerce and the Minister Public Health shall take charge of this Act and have the power to appoint officers, issue Ministerial Regulations and Rules for the enforcement of this	Business information

		Act in relation to their responsibilities.	
52	Trade Secret Act (No.2) B.E. 2558 (2015)		Business information

#		Status	Citation
		Bill (Draft)/Published/Passed/Enacted/Enforcement/Amendment etc	
		Status of the regulation: Draft = drafting (new regulation) published = published in the gazzette but not yet enacted Enact = published in the gazzette and already enacted Amendment = enacted regulation being on amending process	URL
1	Constitution of the Kingdom Of Thailand	Enacted	https://cdc.parliament.go.th/draftconstitution2/download/article/article_20180829093502.pdf
2	Personal Data Protection Act 2019	Enacted	https://www.mdes.go.th/uploads/tinymce/source/%E0%B8%AA%E0%B8%84%E0%B8%AA/Personal%20Data%20Protection%20Act%202019.pdf
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)	Enacted	https://www.ratchakitcha.soc.go.th/DATA/PDF/2565/E/140/T_0028.PDF
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)	Enacted	https://www.ratchakitcha.soc.go.th/DATA/PDF/2565/E/140/T_0026.PDF
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small	Enacted	https://www.ratchakitcha.soc.go.th/DATA/PDF/2565/E/140/T_0024.PDF

	organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565	Enacted	https://www.mdes.go.th/uploads/tinymce/source/%E0%B8%AA%E0%B8%84%E0%B8%AA/%E0%B8%A3%E0%B8%B0%E0%B9%80%E0%B8%9A%E0%B8%B5%E0%B8%A2%E0%B8%9A%E0%B8%AF%20%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%A2%E0%B8%B7%E0%B9%88%E0%B8%99%20%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B9%84%E0%B8%A1%E0%B9%88%E0%B8%A3%E0%B8%B1%E0%B8%9A%E0%B9%80%E0%B8%A3%E0%B8%B7%E0%B9%88%E0%B8%AD%E0%B8%87%20%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%A2%E0%B8%B8%E0%B8%95%E0%B8%B4%E0%B9%80%E0%B8%A3%E0%B8%B7%E0%B9%88%E0%B8%AD%E0%B8%87%20%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%9E%E0%B8%B4%E0%B8%88%E0%B8%B2%E0%B8%A3%E0%B8%93%E0%B8%B2%E0%B8%AF%20%E0%B8%84%E0%B8%B3%E0%B8%A3%E0%B9%89%E0%B8%AD%E0%B8%87%E0%B9%80%E0%B8%A3%E0%B8%B5%E0%B8%A2%E0%B8%99%202565.pdf
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565	Enacted	https://www.mdes.go.th/law/detail/6336-%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%81%E0%B8%B2%E0%B8%A8%E0%B8%84%E0%B8%93%E0%B8%B0%E0%B8%81%E0%B8%A3%E0%B8%A3%E0%B8%A1%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%84%E0%B8%B8%E0%B9%89%E0%B8%A1%E0%B8%84%E0%B8%A3%E0%B8%AD%E0%B8%87%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%9A%E0%B8%B8%E0%B8%84%E0%B8%84%E0%B8%A5-%E0%B9%80%E0%B8%A3

			%E0%B8%B7%E0%B9%88%E0%B8%AD%E0%B8%87-%E0%B8%AB%E0%B8%A5%E0%B8%B1%E0%B8%81%E0%B9%80%E0%B8%81%E0%B8%93%E0%B8%91%E0%B9%8C%E0%B9%81%E0%B8%A5%E0%B8%B0%E0%B8%A7%E0%B8%B4%E0%B8%98%E0%B8%B5%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B9%83%E0%B8%99%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B9%81%E0%B8%88%E0%B9%89%E0%B8%87%E0%B9%80%E0%B8%AB%E0%B8%95%E0%B8%B8%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%A5%E0%B8%B0%E0%B9%80%E0%B8%A1%E0%B8%B4%E0%B8%94%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%A1%E0%B8%B9%E0%B8%A5%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%9A%E0%B8%B8%E0%B8%84%E0%B8%84%E0%B8%A5-%E0%B8%9E-%E0%B8%A8--%E0%B9%92%E0%B9%95%E0%B9%96%E0%B9%95
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	Enacted	https://www.mdes.go.th/uploads/tinymce/source/%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%81%E0%B8%B2%E0%B8%A8%20%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%88%E0%B8%B1%E0%B8%94%E0%B9%83%E0%B8%AB%E0%B9%89%E0%B8%A1%E0%B8%B5%20dpo%20%E0%B8%A1%E0%B8%B2%E0%B8%95%E0%B8%A3%E0%B8%B2%2041(2).pdf
9	Guideline for obtaining consent from data subjects according to the PDPA	Enacted	https://www.dataguidance.com/sites/default/files/consent_guidelines.pdf
10	Guideline for notifying purposes and details for collecting personal data	Enacted	https://www.dataguidance.com/sites/default/files/information_provision_guidelines.pdf

	from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562	Enacted	https://www.mdes.go.th/uploads/tinymce/source/%E0%B8%AA%E0%B8%84%E0%B8%AA/%E0%B9%81%E0%B8%99%E0%B8%A7%E0%B8%9B%E0%B8%8F%E0%B8%B4%E0%B8%9A%E0%B8%B1%E0%B8%95%E0%B8%B4%20%E0%B8%81%E0%B8%A3%E0%B8%93%E0%B8%B5%E0%B8%A8%E0%B8%B6%E0%B8%81%E0%B8%A9%E0%B8%B2%E0%B8%88%E0%B8%B2%E0%B8%81%E0%B8%82%E0%B9%89%E0%B8%AD%E0%B8%AB%E0%B8%B2%E0%B8%A3%E0%B8%B7%E0%B8%AD%20pdpa(1).pdf
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)	Amended by Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)	https://www.ratchakitcha.soc.go.th/DATA/PDF/2563/A/037/T_0001.PDF
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)	Enacted	https://www.mdes.go.th/uploads/tinymce/source/%E0%B8%9E%E0%B8%A3%E0%B8%8E-%E0%B8%81%E0%B8%B3%E0%B8%AB%E0%B8%99%E0%B8%94%E0%B8%A5%E0%B8%B1%E0%B8%81%E0%B8%A9%E0%B8%93%E0%B8%B0%E0%B8%81%E0%B8%B4%E0%B8%88%E0%B8%81%E0%B8%B2%E0%B8%A3%20%E0%B8%A2%E0%B8%81%E0%B9%80%E0%B8%A7%E0%B9%89%E0%B8%99%20PDPA%20%E0%B8%A1%E0%B8%B2%E0%B8%9A%E0%B8%B1%E0%B8%87%E0%B8%84%E0%B8%B1%E0%B8%9A.pdf
15	Notification of the Personal Data Protection Committee Re:	Enacted	https://ratchakitcha.soc.go.th/documents/13995.pdf?fbclid=IwAR28qpNv9RDvV4cil8tjiTqhU_XC4jt

	Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		9_tQY2ALaUR4Cq7hEiomA__j7Wzo
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other	Enacted	https://ratchakitcha.soc.go.th/documents/16521.pdf
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	Enacted	https://ratchakitcha.soc.go.th/documents/14915.pdf
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of	Enacted	https://ratchakitcha.soc.go.th/documents/14913.pdf?fbclid=IwAR0GiJdTaa-rjN3MyYRFOoi6gc08J7Uqpi287_YbZHwhXp_iLjbAZRzaZLA

	Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566	Enacted	https://ratchakitcha.soc.go.th/documents/16522.pdf
20	Electronic Transactions Act, B.E. 2544 (2001)	Enact	https://www.etda.or.th/th/Useful-Resource/law/transactionlaws.aspx
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)	Enact	https://www.etda.or.th/th/Useful-Resource/law/transactionlaws.aspx
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)	Enact	https://www.etda.or.th/th/Useful-Resource/law/transactionlaws.aspx
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)	Enact	https://www.etda.or.th/th/Useful-Resource/law/transactionlaws.aspx
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)	Enact	http://www1.ldd.go.th/web_enactment/Law/computer.pdf
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)	Enact	http://sql.ldd.go.th/intraaccount/Information_Law/File/Law-10.pdf

26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)	Enact	http://www1.ldd.go.th/web_enactment/Law/computer.pdf
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)	Enact	https://www.etda.or.th/getattachment/1ea58862-9366-46aa-9e1f-f2d0fbbe1601/Notification-of-MDES-Re-Take-Down-Notice-BE-2560.aspx
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)	Enact	https://www.etda.or.th/getattachment/23af4648-b655-4959-a594-191286082747/%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%81%E0%B8%B2%E0%B8%A8%E0%B8%81%E0%B8%A3%E0%B8%B0%E0%B8%97%E0%B8%A3%E0%B8%A7%E0%B8%87%E0%B8%94%E0%B8%88%E0%B8%97%E0%B8%A5%E0%B9%80%E0%B8%9E%E0%B8%AD%E0%B9%80%E0%B8%A8%E0%B8%A3%E0%B8%A9%E0%B8%90%E0%B8%81%E0%B8%88%E0%B9%81%E0%B8%A5%E0%B8%B0%E0%B8%AA%E0%B8%87%E0%B8%84%E0%B8%A1-%E0%B9%80%E0%B8

			%A3%E0%B8%AD%E0%B8%87-%E0%B8%AB%E0%B8%A5%E0%B8%81%E0%B9%80%E0%B8%81%E0%B8%93%E0%B8%91-%E0%B8%A3%E0%B8%B0.aspx
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)	Enact	https://www.etda.or.th/getattachment/f1456b62-e9ee-4d05-8493-aceef24c718f/%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%81%E0%B8%B2%E0%B8%A8%E0%B8%81%E0%B8%A3%E0%B8%B0%E0%B8%97%E0%B8%A3%E0%B8%A7%E0%B8%87%E0%B8%94%E0%B8%88%E0%B8%97%E0%B8%A5%E0%B9%80%E0%B8%9E%E0%B8%AD%E0%B9%80%E0%B8%A8%E0%B8%A3%E0%B8%A9%E0%B8%90%E0%B8%81%E0%B8%88%E0%B9%81%E0%B8%A5%E0%B8%B0%E0%B8%AA%E0%B8%87%E0%B8%84%E0%B8%A1-%E0%B9%80%E0%B8%A3%E0%B8%AD%E0%B8%87-%E0%B8%AB%E0%B8%A5%E0%B8%81%E0%B9%80%E0%B8%81%E0%B8%93%E0%B8%91%E0%B8%81%E0%B8%B2%E0%B8%A3.aspx
30	The Special Case Investigation Act B.E. 2547 (2004)	Enact	https://www.dsi.go.th/Upload/1138aa4c1a00b5bb18c5beb6a9ce1d0d.pdf
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)	Enact	https://www.dsi.go.th/Upload/71b8bc0b7b18e81af25c823ecc5795a1.pdf
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)	Enact	https://ddc.moph.go.th/viralpneumonia/file/laws/laws_08.pdf
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and	Enact	https://ratchakitcha.soc.go.th/documents/140D215S0000000002700.pdf

	Freedom of Communications B.E.2566 (2023)		
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications	Enact	https://www.nbtc.go.th/law/%E0%B9%81%E0%B8%99%E0%B8%A7%E0%B8%9B%E0%B8%8F%E0%B8%B4%E0%B8%9A%E0%B8%B1%E0%B8%95%E0%B8%B4%E0%B8%95%E0%B8%B2%E0%B8%A1%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%81%E0%B8%B2%E0%B8%A8-%E0%B8%81%E0%B8%AA%E0%B8%97%E0%B8%8A-%E0%B9%80%E0%B8%A3%E0%B8%B7%E0%B9%88%E0%B8%AD%E0%B8%87-%E0%B8%A1%E0%B8%B2%E0%B8%95%E0%B8%A3%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%84%E0%B8%B8%E0%B9%89%E0%B8%A1%E0%B8%84%E0%B8%A3%E0%B8%AD%E0%B8%87%E0%B8%AA%E0%B8%B4/%E0%B9%81%E0%B8%99%E0%B8%A7%E0%B8%9B%E0%B8%8F%E0%B8%B4%E0%B8%9A%E0%B8%B1%E0%B8%95%E0%B8%B4%E0%B8%95%E0%B8%B2%E0%B8%A1%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%81%E0%B8%B2%E0%B8%A8-%E0%B8%81%E0%B8%AA%E0%B8%97%E0%B8%8A-%E0%B9%80%E0%B8%A3%E0%B8%B7%E0%B9%88%E0%B8%AD%E0%B8%87-%E0%B8%A1%E0%B8%B2%E0%B8%95%E0%B8%A3%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%84%E0%B8%B8%E0%B9%89%E0%B8%A1%E0%B8%84%E0%B8%A3%E0%B8%AD%E0%B8%87%E0%B8%AA%E0%B8%B4.aspx
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)	Enact	https://www.mdes.go.th/law/detail/6664-%E0%B8%9E%E0%B8%A3%E0%B8%B0%E0%B8%A3%E0%B8%B2%E0%B8%8A%E0%B8%81%E0%B8%B3%E0%B8%AB%E0%B8%99%E0%B8%94%E0%B8%A1%E0%B8%B2%E0%B8%95%E0%B8%A3%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%9

			B%E0%B9%89%E0%B8%AD%E0%B8%87%E0%B8%81%E0%B8%B1%E0%B8%99%E0%B9%81%E0%B8%A5%E0%B8%B0%E0%B8%9B%E0%B8%A3%E0%B8%B2%E0%B8%9A%E0%B8%9B%E0%B8%A3%E0%B8%B2%E0%B8%A1%E0%B8%AD%E0%B8%B2%E0%B8%8A%E0%B8%8D%E0%B8%B2%E0%B8%81%E0%B8%A3%E0%B8%A3%E0%B8%A1%E0%B8%97%E0%B8%B2%E0%B8%87%E0%B9%80%E0%B8%97%E0%B8%84%E0%B9%82%E0%B8%99%E0%B9%82%E0%B8%A5%E0%B8%A2%E0%B8%B5-%E0%B8%9E-%E0%B8%A8--%E0%B9%92%E0%B9%95%E0%B9%96%E0%B9%96
36	The Credit Information Business Operation Act B.E. 2545 (2002)	Enact	https://www.bot.or.th/th/laws-and-rules/bot-takes-responsibilities-and-other-relevant-laws-and-regulations/law07.html#accordion-eb57fdac92-item-ac4a766ee7
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)	Enact	https://www.bot.or.th/th/laws-and-rules/bot-takes-responsibilities-and-other-relevant-laws-and-regulations/law07.html#accordion-eb57fdac92-item-ac4a766ee7
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)	Enact	https://www.bot.or.th/th/laws-and-rules/bot-takes-responsibilities-and-other-relevant-laws-and-regulations/law07.html#accordion-eb57fdac92-item-ac4a766ee7
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)	Enact	https://www.bot.or.th/th/laws-and-rules/bot-takes-responsibilities-and-other-relevant-laws-and-regulations/law07.html#accordion-eb57fdac92-item-ac4a766ee7
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)	Enact	https://www.bot.or.th/th/laws-and-rules/bot-takes-responsibilities-and-other-relevant-laws-and-regulations/law07.html#accordion-eb57fdac92-item-ac4a766ee7
41	The Credit Information Business	Enact	https://www.bot.or.th/th/laws-and-rules/bot-takes-responsibilities-and-other-

	Operation Act No.6 B.E. 2565 (2022)		relevant-laws-and-regulations/law07.html#accordion-eb57fdac92-item-ac4a766ee7
42	The Child Protection Act B.E. 2546 (2003)	Enact	https://dep.go.th/images/uploads/Downloads/pdf/888_08.pdf
43	The National Health Act B.E. 2550 (2007)	Enact	https://infocenter.nationalhealth.or.th/?lsvr_kba=%E0%B8%9E%E0%B8%A3%E0%B8%B0%E0%B8%A3%E0%B8%B2%E0%B8%8A%E0%B8%9A%E0%B8%B1%E0%B8%8D%E0%B8%8D%E0%B8%B1%E0%B8%95%E0%B8%B4%E0%B8%AA%E0%B8%B8%E0%B8%82%E0%B8%A0%E0%B8%B2%E0%B8%9E%E0%B9%81%E0%B8%AB%E0%B9%88
44	The Payment System Act B.E. 2560 (2017)	Enact	https://www.bot.or.th/th/laws-and-rules/bot-takes-responsibilities-and-other-relevant-laws-and-regulations/law04.html#accordion-f5cdb6776c-item-4ae4a3733e
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules	Enact	https://www.bot.or.th/content/dam/bot/fipcs/documents/FPG/2563/ThaiPDF/25630223.pdf
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)	Enact	https://www.ratchakitcha.soc.go.th/DATA/PDF/2565/E/109/T_0012.PDF
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance	Enact	https://www.ratchakitcha.soc.go.th/DATA/PDF/2565/E/109/T_0026.PDF

	Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)	Enact	https://oiceservice.oic.or.th/document/Law/file/16553/16553_579b7ac02de623d8d0b3774a7534bbf4_1.pdf
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)	Enact	https://oiceservice.oic.or.th/document/Law/file/16552/16552_cfd707e98142e86ed91df360cbceab06_1.pdf
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)	Enact	https://oiceservice.oic.or.th/document/Law/file/16554/16554_1e09397c3fd3e0662c8e4e154fd8a560.pdf
51	Trade Secret Act B.E. 2545 (2002)	Enact	https://www.ipthailand.go.th/th/dip-law-2/category/%E0%B8%9E%E0%B8%A3%E0%B8%B0%E0%B8%A3%E0%B8%B2%E0%B8%8A%E0%B8%9A%E0%B8%B1%E0%B8%8D%E0%B8%8D%E0%B8%B1%E0%B8%95%E0%B8%B4-acts-4.html
52	Trade Secret Act (No.2) B.E. 2558 (2015)	Enact	https://www.jetro.go.jp/ext_images/world/asia/th/ip/pdf/trade_secret_law_2558_20150205th.pdf

Definition BasicTerm

#	Regulation	Type and Scope of Data	Data processing and handling
		Personal data, personal information/sensitive and important data/children and minors' data, etc. Is the scope of data clearly written in the regulations? What are the unclear points?	Processing, handling / disclosure, sharing, provision, transmission, outsourcing / use for advertising, etc.
		Specific type of data required to complied with the regulation	Provision for data processing
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019	6 "Personal Data" means any information relating to a Person, which enables the identification of such Person, whether directly or indirectly, but not including the information of the deceased Persons in particular;	5 This Act applies to the collection, use or disclosure of Personal Data by a Data Controller or a Data Processor that is in the Kingdom of Thailand, regardless of whether such collection, use or disclosure takes place in the Kingdom of Thailand or not.
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		Those who are exempt from taking action according to Section 39, paragraph one (1), (2), (3), (4), (5), (6), and (8) must have one of the following characteristics: (1) Be a small enterprise or medium sized enterprise according to the law on small and medium sized busiiness promoion (2) is a community enterprise or

			community enterprise network according to the law on enterprise promotion. (3) is a social enterprise or social enterprise group according to the law on the promotion of social enterprises; (4) is a cooperative, cooperative assembly, or farmer group according to the law on cooperatives; (5) is a foundation, association, religious organization, or non-profit organization (6) is a household business or other business of the same nature ...
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		"Activities" means any actions of the Personal Data Controller or Personal data processors collect, use or disclose personal data whether related to core activities or auxiliary activities...
9	Guideline for obtaining consent from data subjects	3 Criteria for requesting consent The personal data controller should be aware that the collection, use, or disclosure of	

	according to the PDPA	personal information may be carried out without the consent of the owner of the personal information (exception for complying to PDPA) but exceptions must be met that the Personal Data Protection Act allows to be done ("legal basis or Lawful Basis") according to Section 24 of the Personal Data Protection Act B.E. 2019, including 1) to achieve the objectives related to organize to make historical documents or archives for public benefit or related to research studies or statistics 2) To prevent or stop danger to a person's life, body, or health. 3) It is necessary for the performance of a contract to which the owner of personal data is a party. or for use in carrying out the request of the owner of personal data before entering into the contract 4) it is necessary for the performance of duties in operating Carrying out missions for the public benefit of the personal data controller or performing duties in the use of State authority granted to the personal data controller 5) It is necessary for the legitimate interests of the personal data controller. or of persons or juristic persons other than the Personal Data Controller. 6) It is the personal data controller's compliance with the law. In the case of personal data regarding race, ethnicity, political opinions, beliefs in sects, religions or philosophies. sexual behavior Criminal history, health information, disability, labor	

		union information, genetic information, biological information, or any other information that similarly affects the owner of personal information as specified in the announcement of the Personal Data Protection Committee will be subject to the exceptions as specified. Section 26 of the Personal Data Protection Act B.E. 2019	
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562	1.1 Question: Information on small and medium enterprise entrepreneurs who are natural persons (not a juristic person) considered personal information under the Personal Data Protection Act 2019 or not? How? Answer: Section 6 of the Personal Data Protection Act 2019 stipulates that "personal data" means Information about an individual that enables him or her to be identified, directly or indirectly. But it does not include information about specific deceased persons and "person" means a natural person. Therefore, in the case of information about entrepreneurs who are natural persons which is not information of the deceased person or information of a juristic person If such information makes it possible to identify an individual. whether directly or indirectly Such information is considered personal information. 2.1 Question: Information on	

		small and medium enterprise entrepreneurs who are natural persons (not a juristic person) considered personal information under the Personal Data Protection Act 2019 or not? How? Answer: Section 6 of the Personal Data Protection Act 2019 stipulates that "personal data" means Information about an individual that enables him or her to be identified, directly or indirectly. But it does not include information about specific deceased persons and "person" means a natural person. Therefore, in the case of information about entrepreneurs who are natural persons which is not information of the deceased person or information of a juristic person If such information makes it possible to identify an individual. whether directly or indirectly Such information is considered personal information. 3.1Question: Collection, use, and disclosure of personal information in the reporting process Environmental impact assessment, which is carried out in accordance with the law on promoting and maintaining environmental quality. It is considered to be carried out as required by law for the benefit of the public. which is exempt Is it not subject to the enforcement of the Personal Data Protection Act B.E. 2019 according to Section 4 (3)? Answer: According to Section 4 (3) of the Personal Data Protection Act B.E. 2019...the preparation of the environmental impact assessment report is not personal information that is collected. specifically for media activities, artistic works, or literary works; therefore,	

		enforcement is not exempted according to Section 4 (3) of the said Act.	
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		4 This Royal Decree is aimed that the personal data controllers who collect, use, or disclose personal data as specified in each section in this Royal Decree are exempted from some parts of the Personal Data Protection Act B.E. 2019 under certain conditions specified with principles for important information as follows: (1) Requesting personal information in accordance with this Royal Decree must be for the public benefit as the case may be according to the objectives and scope of the law granting within the authority of government agencies as specified without creating an unreasonable burden to the personal data controller who is responsible for disclosing

			personal data (2) The duty of the Personal Data Controller to disclose personal data without obtaining consent from the owner of personal data when receiving a request for such information from a government agency which has a lawful authority to request that information to perform duties and duties and the authority of the requesting government agency. (3) Certification of the rights of the owner of the personal data or the controller taht is requested for making a complaint to the expert committee or asking the committee for interpretation or decision as the case may be (4) Exemption from offenses and criminal penalties under this Royal Decree does not covere illegal operation by this Royal Decree 6 When the Personal Data Controller receives a request for personal data from National Anti-Corruption Commission or assigned government agency to be carried out by the National Anti-Corruption Commission in accordance with the organic law concerning the prevention and suppression of corruption, the National Anti-Corruption Commission, Office of the National Anti-Corruption Commission, or government agencies specified by the committee, those who are authorized by law to request personal information in order to carry out a purpose or mission according to the law regarding prevention and suppression of corruption, the controller of such personal data will be wxempted from compliance with the

			provisions of Chapter 2 and Chapter 3 of the Data Protection Act 2019. 7 When the Personal Data Controller receives a request for personal data from the Revenue Department, Customs Department, or Excise Department, those who have authority to request personal information for processing according to the objective or mission under the law that is responsible for tax collection, any action related to the enforcement of all tax fees, court fees, including the implementation of international obligations or cooperation in such matters or any duties or taxes, the said personal data controller is exempt from compliance with the provisions of Chapter 2 and Chapter 3 of the Personal Data Protection Act B.E. 2019. ... 8 When the Personal Data Controller receives a request for personal data from local government organizations designated by the committee and those that have the law to authorize them to request information to carry out the legal objectives or missions under its responsibility regarding tax collection according to the law on land and building tax, the controller of such personal data shall be exempt from compliance with the provisions of Chapter 2 and Chapter 3 of the Protection Act 2019 9 When the Personal Data Controller receives a request for personal data from to the Cabinet Secretariat to carry out the objectives or

			missions in accordance with the laws contained responsibilities regarding the establishment of clerical titles Appointment or removal of government officials or group of people which is the king the power of the king or that must be submitted to the Cabinet and requesting royal gifts or restore the royal decorations a petition submitted to the King or a request for royal grace in various matters, the controller of such personal data is exempt from compliance with the provisions of Chapter 2 and Section 3 of the Personal Data Protection Act 2019. 10 When the Personal Data Controller receives a request for personal data from a government agency that has authority to request personal information to carry out objectives or missions according to the law regarding important public benefits Important information which the committee announces, the data controller are exempt from compliance with the provisions of Section 2 and Section 3 of the Personal Data Protection Act 2019 ... 11 Collection, use, and disclosure of personal data of personal data controllers in the process of deportation extradition International cooperation on criminal justice process Preventing and suppressing participation in transnational criminal organizations, cooperation in the courts or international justice process, the controller of such personal data shall be exempt from compliance with the provisions of Chapter 2 and Chapter 3 of the

			Personal Data Protection Act 2019.
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other	1. personal data to achieve research research objectives or statistics according to section 24 (1) and scientific, historical or statistical study or other public benefits according to Section 26 (5) (d) of the Personal Data Protection Act B.E. 2019 B.E. 2566	3. (para 2) "Send or transfer personal data" means sending or transferring personal data by the sender or transfer personal information whether it is sending or transferring information by physical means or through the computer system or network system to the recipient of personal information but it does not include sending and receiving personal information in a way that is just a medium (intermediary) in the transmission of data (data transit) between computer systems or network systems or the storage of data (data storage) in temporary or permanent form that no third party has access to such personal information in addition to the personal data controller or the personal data processor who sends the personal data or its personnel, employees, or employees. The controller of personal data or the processor of that personal data, such as in the case of sending data over a network system abroad or sending data through the cloud computing service provider's system provider)where there is no person other than the personal

			data controller or personal data processor who is The sender of that personal information or the personnel, employees, or employees who access the personal information because there are technical measures or legal conditions to support it.
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		4. "Send or transfer personal data" means sending or transferring personal data by the sender or Transfer personal information whether it is sending or transferring information by physical means or through the computer system or network system to the recipient of personal information but this does not include sending and receiving personal information in a way that is just a medium (intermediary) in the transmission of data(data transit) between computer systems or network systems or the storage of data (data storage) in temporary or permanent form. that no third party has access to such personal information In addition to the personal data controller or The personal data processor who sends the personal data or its personnel, employees, or employees. The controller of personal data or the processor of that personal data, such as in the case of sending data through a network system

			in a foreign country or sending data through the system of a cloud computing service provider where there is no person other than Personal data controller or personal data processor who is The person who sends that personal information or the personnel, employee, or employee who has access to the personal information because there are measures technical or legal conditions support.
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566	3. "Personal information regarding criminal history" means personal information regarding investigation of criminal offenses criminal proceedings or receiving criminal punishment that is official information or certified by a government agency with legal authority regarding such action is taken regardless of whether the action has been finalized or not. 4. This Notification shall apply to the collection of personal information regarding criminal history <u>that is not done under the control of an agency having legal authority under Section 26, paragraph three, of the Personal Data Protection Act B.E. 2019</u>	
20	Electronic Transactions Act, B.E. 2544 (2001)	Section4 ...(shorten).... "information" means an incident or fact, whether expressed in the form of a letter, number, sound or image or in any other form capable of connotation by itself or through any means; "data message" means information generated, sent, received, stored or processed by an electronic means such as electronic data interchange, electronic mail, telegramme, telex or facsimile; "electronic signature" means	Section4 ...(shorten).... "electronic data interchange" means the dispatch or receipt of information by an electronic means from computers to computers using an agreed standard; ...(continue)...

		letters, characters, numbers, sound or any other symbols created in an electronic form and affixed to a data message for establishing the association of a particular person with the data message for the purposes of identifying the signatory in relation to such data message and indicating that such person has approved the information contained in that data message; "information system" means a system for processing with an aid of an electronic device for generating, sending, receiving, storing or processing data messages; ...(continue)...	
		Section 26. An electronic signature that meets the following features shall be deemed to be a reliable electronic signature: (1) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person; (2) the signature creation data were, at the time of creating the electronic signature, under the control of the signatory and of no other person; (3) any alteration to the electronic signature, made as from the time of its creation,is detectable; and *(4) in the case where a purpose of the legal requirement for an electronic signature is to provide assurance as to the integrity of the information, any alteration made to that information as from the time of signing is detectable.* *The provisions of paragraph one does not imply any limitation that no other method exists for establishing the reliability of an electronic signature or does not limit the adducing of any evidence of the non-reliability of an electronic signature. (repealed)*	

21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)	Section 11. The provisions of (4) of paragraph one of section 26 of the Electronic Transactions Act, B.E. 2544 (2001) shall be repealed and replaced by the following: "(4) in the case where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information, any alteration made to that information as from the time of signing is detectable."	Section 3. There shall be added a definition of "automated electronic message system" between the definitions of "information system" and "electronic data interchange" in section 4 of the Electronic Transactions Act, B.E. 2544 (2001): ""automated electronic message system" means a computer program or an electronic means or other automated means used to initiate an action or respond to data messages or any performances against data messages in whole or in part, without review or intervention by a natural person each time an action is initiated or each time a response is generated by the system".
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		Section 3. There shall be added definitions of "identification and authentication" and "digital identification and authentication system" between the definitions of "information system" and "automated electronic message system" in section 4 of the Electronic Transactions Act, B.E. 2544 (2001) as amended by the Electronic Transactions Act (No. 3), B.E. 2562 (2019): ""identification and authentication" means a process for identification and authentication of a person; "digital identification and authentication system" means an electronic network linking information between any persons or State agencies for the purpose of the identification and authentication and the conclusion of other transactions incidental to the identification and authentication."

24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)	"computer data" means information, messages and concepts or instruction, a program or anything else in a form suitable for processing in a computer system and shall include electronic data under the law on electronic transaction. "traffic data" means any data relating to communication by means of a computer system, indicating the communication's origin, destination, route, time, date, size, duration, type of underlying service, or other information relating to communication of such a computer system.	
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)	Section 3 "computer data" means data, messages, commands, sets of commands, or other things. Any of them electronically gives and receives computer data or electronic mail, but does not include persons who are Subject: Characteristics and methods of sending and the nature and quantity of information Frequency and method of transmission that is in the computer system in a condition that the computer system may process and shall include The medium for computer data or electronic mail is which does not cause annoyance to the recipient electronic data According to the law on electronic transactions "Electronic Address" means (1) destination address; (destination) used to receive electronic mail (E-mail address) or (2) destination address on	

		Internet used to receive computer data (IP Address of computer data). Contains username, recipient's name, or mailbox. Electronic (E-mail box) of the recipient of the information, including the telephone number or internet address (IP Address) of the recipient of the information, which address can refer to the destination domain name or destination address of a computer network or computer equipment that can be used to receive computer data Regardless of that address will it be visible or not.	
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)	Section 3 "Computer system" means a device or set of computer equipment that is connected to work together by specifying commands, command sets, or anything else and guidelines for operating equipment or a set of equipment that automatically processes data "Computer data" means data, messages, commands, sets of instructions, or any other things. that is in the computer system in a condition that the computer system may process and shall include Electronic data according to the law on electronic transactions as well. "Message" means a story or fact. Whether it appears in the form of letters, numbers, sounds, images or any other form that can convey meaning by its own nature or through any means.	
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or	Section 3 "Computer system" means a device or set of computer equipment connected to working together by specifying an order, set of instructions, or anything else and work guidelines let the device or set of devices perform the task of automatically	

	delete computer data of officials or service providers, B.E 2560 (2017)	processing data. "Computer data" means data, messages, commands, sets of instructions, or any other things that is in the computer system in a condition that the computer system may process and shall include electronic data according to the law on electronic transactions as well "Location of information" means the location or source of information (Related Online Location), such as URL (Related URL) on the internet (Related IP Address), domain name (Related Domain Name) Web page (Related web page) of the resource or The electronic address (Related Electronic Address) associated with that information.	
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		"Digital identity verification and verification system" means a digital registration system. Internet network or electronic network that links information between any person or information between service users, service providers, various individuals, or government agencies. in computer systems and networks electronic or internet For the benefit of verifying identity and any actions related to verifying and verifying identity, ...(shorten)... "Identity verification and verification" means the process of verification and verification of authenticity of an individual, whether by the individual or arising from computer data processed by the system computer or artificial intelligence "Social Media" means media or communication channels or exchange information between people using information technology or Internet network

			Intermediary) that focuses on creating or distributing content between users (Creation and Exchange of User-generated Content) or support two-way communication or presentation and Publish content widely on your own. This includes, but is not limited to, computer programs, software, applications, message boards, social networks, media for distributing and exchanging content ...(continue)...
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	Section 5 in this announcement: "Personal information of users" means information about users of telecommunications services. which makes it possible to identify the user of that service, whether directly or indirectly, from such information itself or from Such information is combined with other information that the license holder has or can access, such as name, surname, address, national identification number, or any other substitute identification number issued by the government. Telecommunications number Service usage information of service users Including behavior in using telecommunications services that may identify the user of the service. "	"Collection" means any action, whether by one or more ways, to obtain which personal information of service users Whether at the same time or several times.

34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications	1. Scope of application of NBTC announcements 1.1 NBTC Announcement, Section 1, 4, determines the scope of use1 to be enforced in accordance with the established criteria1. In the law regarding the protection of personal information, therefore, the use of NBTC announcements must be considered. The Personal Data Protection Act, B.E. 2019, and secondary laws under the said Act together by considering the 1 Data Protection Act 1 personal information etc. There is additional effect on the matter that the NBTC announcement did not specify. Or specified 1 already but 5 is not 5 is sufficient for protection.	2.4 "Collection" means doing anything in one or more ways to obtain which is the personal information of the user of the service Whether it's the same time or multiple times. And whether you will get 1 from uses1 service directly or from other sources.
		1.2 Personal Data Protection Act, Section 3 stipulates that the following 5 matters must be brought: Personal Information Protection Act come into use1, whether it is mandatory5 whether it will be a repeat of what was specified1 in the NBTC announcement or not5 Anyway (1) Collection, use, or disclosure of personal information of service users, such as notifications. Purpose of collection Lawful Basis of Processing The collection of personal data from sources other than the owner of the personal data ...(continue)...	
		1.3 NBTC announcement No.5 does not apply to the case of disclosure. Exchange, access, and storage Collection or use1k1personal information According to the Royal Decree on measures to prevent and suppress crime 2023, however, the licensee may not disclose it	

		to any other person who does not have a related duty to know.1	
		1.4 In the case where there is a law other than the Personal Information Protection Act, etc. Measures to protect the personal information of users of the service are specific. The person receiving the license must comply with the law.	
		2. Definitions in the NBTC announcement 2.1 “Personal information of users of services” 2.1.1 Definitions according to the NBTC announcement must be considered in conjunction with the Protection Act Personal information, etc., is said to not specifically include information about a person who has passed away and must be information about a natural person. 2.1.2 Personal information of a user of a service means any information that identifies a user of a personal service.Ordinary person who is the owner of the data (Data Subject) (1) Data that can directly distinguish users111 of services from each other1, such as first name, last name. Address 5 National Identification Number or any other identification number that uses 1 instead of 1 issued by the government. Number telecommunications ...(continue)...	
		2.2 “License recipient” means a person who receives a telecommunications business license from the NBTC, including type one, type two, and type three licenses.	
		2.3 "service user” 2.3.1 Telecommunications services are divided into 2 types as follows: (1) Individual users The definition must be considered in conjunction with the Act 5.	

		Protection of personal information which a person means a natural person, therefore, the user of the service who will receive protection According to the NBTC announcement, you must be a natural person only. (2) 1 person uses 1 juristic person service (Organizational customers) will receive data protection according to Business Secrets Act B.E. 2002 2.3.2 In the case where the juristic person is a 6-person, 5-person contract with a licensee. B1 Juristic person information, such as name of juristic person Legal entity registration number No5 is considered personal information5 by nature ...(continue)...	
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)	Section 3 in this Royal Decree: "Technological crime" means committing or attempting to commit an offense according to the law on criminal acts. Committing computer crimes to commit fraud, extortion, or extortion of money any person or in a manner that is likely to cause Cause damage to another person or commit an offense of fraud, extortion, or extortion of property. Using the computer system as a tool	
36	The Credit Information Business Operation Act B.E. 2545 (2002)	"prohibited information" means information of a natural person that is not related to receipt of services, application for credit, or that affects the feelings of, or may cause damage to, or that clearly affects the rights and liberties of, the information subject, as follows: (1) disability description; (2) genetic description; (3) information of a person who is under investigation or criminal case trial; (4) any other information	

		prescribed in the notification of the Committee. ...(shorten)... "information subject" means any natural person or juristic person who is the subject of information or who is the subject of history of a customer applying for use of services from a member, whether it be an application for credit or any other services. ...(shortent)... "service user" means a member or juristic person operating lawful business by granting credit as a normal trade practice. "source of information" means a natural person, body of persons or juristic person who provides information to a credit information company.	
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)	Section 3 In this Act, "information" means something that conveys the meaning of facts of credit information or credit mark, irrespective of whether the said conveyance can be made by the nature of that thing itself or through any means, and whether it be in the form of a document, file, report, letter, diagram, map, drawing, photograph, film, picture or sound recording, recording by computer, or any other method which causes the thing recorded to appear. ...(shorten)... "credit information business" means a business concerning control or processing of credit information so as to provide information to its members or service users.	"information processing" means any act done with information, whether it be a gathering, recording, compilation, storage, amendment, retrieval, usage, disclosure, printing, accessibility, deletion, or destruction of information, including a preparation and disclosure of credit mark and statistical report.
39	The Credit Information		

	Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)	"credit information" means facts concerning a customer applying for credit with a member in the category of financial institutions or applying for credit through a member in the category of credit intermediaries, as follows: (1) Facts that indicate the identity and qualifications of the customer applying for credit: (a) which, in the case of a natural person, mean the name, address, day, month, year of birth, marriage status, occupation, national identification number or public authority identification card number or passport number and taxpayer identification number (if any); (b) which, in the case of a juristic person, mean the name, location, juristic person registration number or taxpayer identification number. (2) History of application for and approval of credit, as well as repayment of credit of the customer applying for credit, including history of payment for goods or services by credit card.	
42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)		
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of	“Customer” means a natural person and juristic person	

	Thailand SorGorSor2. 4/2563 re: Market Conduct Rules	currently using the product. and shall include those who contact to inquire about product information Those who are informed about the product through various media and those who are offered or persuaded by the service provider to purchase the product. "Vulnerable customers" means customers for whom service providers must use caution. To contact and provide special services, such as elderly people aged 60 years and over, people with limited financial knowledge, people with no experience in using products or those who have limitations People with limited ability to communicate or make decisions, such as those with hearing or vision impairments or people with health impairments	
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)	"Customer" means a person being or having been invited, induced, or provided with an indicated opportunity by a Company's employee or staff member, a Life Insurance Agent, a Life Insurance Broker, or a Bank for entering into an insurance contract with a Company, and shall include an insured, a beneficiary, and a person who has the right of claim under an insurance policy, as the case may be;	
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent,	"Customer" means a person being or having been invited, induced, or provided with an indicated opportunity by a Company's employee or staff member, Non-life Insurance Agent, Non-life Insurance Broker, or a Bank for entering into an insurance contract with a Company, and shall include the insured, the beneficiary, and the person who has the right of	

	Broker and Bank B.E. 2563 (2020)	claim under an insurance policy, as the case may be;	
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)	Section 1 Definition In this practice "Personal information" means personal information. In accordance with data protection laws "Sensitive personal information" means personal information according to Section 26 of the Act. Personal Information Protection Act 2019 "Customer" means a person who is an employee or employee of the company. life insurance agent insurance broker Life invites, persuades, or directs people to take out insurance with the company. and including the insured Beneficiary, person who has the right to make a claim according to the insurance policy who is a natural person and owner of personal data	
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)	Section 1 Definition In this practice "Personal information" means personal information. According to the law on personal data protection person "Sensitive personal information" means personal information according to Section 26 of the Act. Personal Information Protection Act 2019 "Customer" means a person who is an employee or employee of the company. life insurance agent insurance broker Life invites, persuades, or directs people to take out insurance with the company. and including the insured Beneficiary, person who has the right to make a claim according to the insurance policy who is a natural person and owner of personal data	
50	The Notification of the Office of Insurance	Section 1 Definition In this practice "Personal information" means personal	

	Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)	information. In accordance with data protection laws personal "Sensitive personal information" means personal information according to Section 26 of the Act. Personal Information Protection Act 2019 "Insured" means the insured and persons involved in casualty inspection and assessment who are natural persons and owners of personal information.	
51	Trade Secret Act B.E. 2545 (2002)	Section 3 Under this Act: "Trade Secrets" means trade information not yet publicly known or not yet accessible by persons who are normally connected with the information. The commercial values of which derive from its secrecy and that the controller of the trade secrets has taken appropriate measures to maintain the secrecy. "Trade information" means any medium that conveys the meaning of a statement, facts, or other information irrespective of its method and forms. It shall also include formulas, patterns, compilations or assembled works, programs, methods, techniques, or processes. ...(shorten)... "Owner of Trade Secrets" means the person who discovered, invented, compiled or created the trade information that is a trade secret without infringing someone else's trade secrets or infringing the rightful holder of the testing result or trade information that is a trade secret. It shall also include the transferee under this Act.	
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation	Data handlers
		Classification/ distinction by responsibility (data processor, data controller)/ size of data, (national security) critical services, complexity of business model, etc.
		Provision on type of data handler
1	Constitution of the Kingdom Of Thailand	
2	Personal Data Protection Act 2019	6 "Data Controller " means a Person or a juristic person having the power and duties to make decisions regarding the collection, use, or disclosure of the Personal Data; "Data Processor " means a Person or a juristic person who operates in relation to the collection, use or disclosure of the Personal Data pursuant to the orders given by or on behalf of a Data Controller, whereby such Person or juristic person is not the Data Controller.
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)	
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)	
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)	
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565	

7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565	
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	
9	Guideline for obtaining consent from data subjects according to the PDPA	
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA	
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562	3.2 Question: Environmental impact assessment report creator who is responsible for studying and collecting data for environmental impact assessment. Are you considered a personal data controller? and in the process of collecting personal information for use in studying and evaluating environmental impacts. Including cases where the person preparing the environmental impact assessment report Use secondary data necessary for studying and evaluating environmental impacts from government agencies. Consent must be obtained from the owner of personal data. Or can it be exempted from requesting consent according to Section 24 (4) or Section 26 (5)? Answer: According to Section 6 of the Personal Data Protection Act B.E. 2019, ... Therefore, the person or juristic person who is the operator or Permission applicants who are responsible for preparing environmental impact assessment reports in accordance with the law on the promotion and preservation of national environmental quality is considered the controller of personal

		information and if another person or legal entity is hired or assigned to prepare an environmental impact assessment report The person or legal entity that is hired or assigned Considered a personal data processor according to the Personal Data Protection Act B.E. 2019 ... 4.1 Question: Condominium juristic persons established in accordance with the Condominium Act B.E. 2522 will be exempt from recording the records of the Personal Data Controller which is a small business in accordance with the announcement of the Personal Data Protection Board regarding exemption from recording the records of the Personal Data Controller. Individuals who are small businesses, B.E. 2565 or not? Answer: ...If the condominium juristic person does not sell goods or provide any services to other persons who are not condominium owners or residents. or carry out any business that has the nature of seeking profit. will have the status of being the controller of personal data which is a non-profit organization who are exempt from recording the details of the Personal Data Controller according to Section 3 (5) of the Personal Data Protection Board announcement regarding... 5.1 Question: Condominium management business operator for condominium juristic persons will be exempt from recording records of personal data controllers who are small businesses in accordance with the announcement of the Personal Data Protection Board on exemptions from recording records of personal data controllers who are small businesses, B.E. 2022 or not? Answer: The condominium juristic person established in accordance with the Condominium Act B.E. 2522 ...will have the status of a non-profit organization as the controller of personal data which is exempt from recording the records of the Personal Data Controller according to section 3 (5) of the Personal Data Protection Board announcement on exemption from recording the records of the Personal Data Controller which is a small business, B.E. 2022 ...
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)	3 The provisions of Chapter 2, Section 3, Section 5, Section 6 and Section 7 and Section 95 of the Personal Data Protection Act B.E. 2019 shall not be applied to the personal data controller who is an agency or business listed in the annex of this Royal Decree. 1. Government agency (2) foreign government agencies and international organizations (3) Foundations, associations, religious organizations, and non-profit organizations. (4) Agricultural businesses (5) Industrial activities (6) Commercial activities (7) Medical and public health affairs (8) Energy, steam, water and waste disposal businesses. Including related businesses (9) Construction business (10) Repair and maintenance businesses

		(11) Business in transportation, transportation and storage of goods. (12) Tourism businesses (13) Communications, telecommunications, computers and digital businesses. (14) Financial, banking and insurance businesses. (15) Real estate business (16) Professional activities (17) Administrative and support service activities (18) Science and technology, academics, social work and science activities. (19) Educational affairs (20) Entertainment and recreation businesses (21) Security business (22) Household businesses and community enterprises which cannot classify activities
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)	3 The provisions of Chapter 2, Section 3, Section 5, Section 6 and Section 7 and Section 95 of the Personal Data Protection Act B.E. 2019 shall not be applied to the personal data controller who is an agency or business listed in the annex of this Royal Decree. 1. Government agency (2) foreign government agencies and international organizations (3) Foundations, associations, religious organizations, and non-profit organizations. (4) Agricultural businesses (5) Industrial activities (6) Commercial activities (7) Medical and public health affairs (8) Energy, steam, water and waste disposal businesses. Including related businesses (9) Construction business (10) Repair and maintenance businesses (11) Business in transportation, transportation and storage of goods. (12) Tourism businesses (13) Communications, telecommunications, computers and digital businesses. (14) Financial, banking and insurance businesses. (15) Real estate business (16) Professional activities (17) Administrative and support service activities (18) Science and technology, academics, social work and science activities. (19) Educational affairs (20) Entertainment and recreation businesses (21) Security business (22) Household businesses and community enterprises which cannot classify activities
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are	

	Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)	
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)	3. (IN this Notification) Personal data controller" means the person controlling personal data who is exempt from The Personal Data Protection Act B.E. 2019
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other	3. (para 1) 'Cloud computing service provider' means a service provider that maintains data or stores data for other parties in a temporary or permanent form. There is a system that manages information on the internet. They may provide services in various forms, such as core infrastructure service providers. (Infrastructure as a Service: laaS), platform service provider (Platform as a Service: PaaS), software service provider (Software as a Service: SaaS), data storage system service provider (Data Storage as a Service: DSaaS) and other Providing serverless computing data management systems or function service providers (Function as a Service: FaaS), etc.
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the	

	Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	4. 'Sender or transfer of personal data' means the personal data controller or processor who sent or transferred Personal data to recipients of personal information located abroad. 'Recipient of personal data' means the data controller or data processor living abroad that receives personal information from the sender or transfer of personal information for the purpose of collecting, using, or disclosing personal information 'Cloud computing service provider' means a service provider that maintains data or stores data for other parties in a temporary or permanent form, with a system that manages data on the Internet. They may provide services in various forms, such as infrastructure as a service (LAAS), platform as a service (PaaS), software as a service (SaaS), etc. Storage service (Data Storage as a Service: DSaaS) and serverless data management system provider Computing or function provider (Function as a Service: FaaS), etc.
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566	
20	Electronic Transactions Act, B.E. 2544 (2001)	Section4 ...(shorten).... 'originator' means a person who is a sender or generator of the data message prior to its storage for transmission in accordance with the method designated by such person, whether the data message is sent or generated by such person or is sent or generated in the name of or on behalf of such person, but does not include an intermediary with respect to that data message; 'addressee' means a person to whom the originator intends to send the data message and who receives such data message, but does not include an intermediary with respect to that data message; 'intermediary' means a person who, on behalf of another person, sends, receives or stores a particular data message as well as

		provides other services with respect to that data message; ...(continue)...
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)	
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)	
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)	
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)	'service provider' means: (1) a person who, either in his own name or in the name or for the benefit of another person, provides to other persons with access to the internet or the ability to communicate by other means through a computer system. (2) a person who stores computer data for the benefit of other persons.
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)	
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)	'Recipient of data' means a person to whom the data sender wishes to send computer data or letters. electronically gives and receives computer data or electronic mail, but does not include persons who are the medium for computer data or electronic mail is 'Information sender' means a person who intends to send computer information or electronic mail. Initially for commercial purposes. Whether it is offering to sell products or services, investments or real estate of any kind, including website providers or application providers. (Application) or Social media service providers that advertise or support the sending of information or such electronic mail, but does not include telecommunications service providers that act as a medium for Transmission of computer data or e-mail That electronics
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of	'Service provider' means (1) a service provider for other people to access the Internet; or to be able to contact each other By any other means through the computer system, whether the service is provided on one's own behalf or for benefit of another person (2) The service provider maintains computer data for the benefit of other persons

	the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)	'Service user' means a user of the service provider. service regardless of whether there is a fee for the service or not
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)	Section 3 'Service provider' means (1) a service provider for other people to access the Internet; or to be able to contact each other by other means Through the computer system, whether the service is provided on one's own behalf or for benefit of another person (2) The service provider maintains computer data for the benefit of other persons. 'Competent official' means a person appointed by the Minister to carry out the duties in accordance with the Act. Concerning computer offenses B.E. 2007 and its amendments
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)	Section4 'Service provider' means (1) a service provider providing services to other persons in accessing the Internet; or to be able to contact each other by other means Through the computer system, whether the service is provided on one's own behalf, on behalf of, or for the benefit of another person. (2) The service provider maintains computer data for the benefit of another person
30	The Special Case Investigation Act B.E. 2547 (2004)	
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)	
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)	
33	The Notification of the National Telecommunicati ons Commission Re: Measures to Protect Telecommunicati	'Licensee' means a person who has received a license to operate a telecommunications business according to law Concerning telecommunications business operations. 'User' means a person who uses telecommunications services from the services provided by the licensee. Telecommunications business but does not include service users who are licensees who of

	ons Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	telecommunications services received As a user who uses the service to conduct another business.
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications	
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)	'Financial institutions' means commercial banks and government financial institutions established by specific laws in accordance with the law on financial institution business. "Business operator" means a business operator according to the law on payment systems
36	The Credit Information Business Operation Act B.E. 2545 (2002)	'information controller' means any natural person, body of persons or juristic person in the private sector, whether it be one single work unit or jointly with another work unit, whose duty is to control information processing or to process information by itself. 'information processor' means an information controller or any person who processes information on behalf of an information controller or credit information company. ...(shorten)... 'company' means a limited company under the Civil and Commercial Code or a public limited company under the law governing public limited companies. 'credit information company' means a company licensed to operate credit information business. 'financial institution' means a juristic person licensed to operate or carry on a business in the Kingdom, as follows: ...(shorten)...
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)	
38	The Credit Information Business Operation Act	

	No.3 B.E. 2551 (2008)	
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)	
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)	
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)	'credit Intermediary' means a juristic person that operates as an intermediary for the provision of electronic system or network services in its ordinary course of business in order to facilitate credit provisions and does not operate as a credit provider by itself, in the category of service intermediaries as prescribed in Notifications issued by the Committee. 'member' means a financial institution or a credit intermediary that a credit information company has admitted as its member.
42	The Child Protection Act B.E. 2546 (2003)	
43	The National Health Act B.E. 2550 (2007)	
44	The Payment System Act B.E. 2560 (2017)	
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules	5. Content 5.1 Definitions 'Financial institution' means a commercial bank. Finance companies and credit foncier companies according to the Financial Institution Business Act 'Specialized financial institution' means a specialized financial institution according to law. Concerning financial institution business 'Financial business group' means a financial business group according to the announcement of the Bank of Thailand. Thailand regarding regulations on to supervise financial and related business groups 'Company in the financial business group' means a company in the financial business group. It does not include payment service business operators. Payment under supervision Regulated in accordance with the law on payment systems and companies that operate only businesses that are under regulation under the supervision of other regulatory agencies such as securities companies Asset Management Company General insurance company life insurance company

		'Payment service business operators supervised payment service provider' means a payment service business operator Payment under supervision Regulated in accordance with the law on payment systems 'Credit card business operator that is not a financial institution' means a credit card business operator according to the announcement of the Ministry of Finance regarding businesses that must apply for permission according to Section 5, Revolutionary Council Announcement No. 58 (regarding credit card business). 'Personal loan business operators under supervision regulated entity that is not a financial institution' means a personal loan business operator under supervision Regulated according to the announcement of the Ministry of Finance Concerning businesses that must request permission according to Section 5 of the Revolutionary Council Announcement No. 58 (Personal loans under supervision) 'Microfinance business operator for occupations under supervision that is not a financial institution' means a microfinance business operator for occupations under supervision in accordance with the announcement of the Ministry of Finance regarding businesses that must apply for Permission in accordance with Section 5 of the Revolutionary Council Announcement No. 58 (Regarding microfinance loans for occupations under supervision) 'Asset management company' means an asset management company according to law About asset management companies ...(shorten)... 'Service provider' means a person who acts as an issuer, advisor, seller, purchaser, or transferee of products, including: financial institution Companies in the financial business group Specialized financial institutions Credit card business operators who are not financial institutions Business operators of personal loans under supervision that are not financial institutions Microfinance business operators for occupations under supervision that are not financial institution and asset management companies ...(shorten)... 'Business facilitator' means another person that a specialized financial institution works with. Enter into a contract to hire, assign, or appoint to perform on behalf of all or part of the work that the Specialized Financial Institutions normally have to perform themselves, which includes Subcontractor (subcontract) and natural persons who provide business support services Under the regulations of the Bank of Thailand
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life	Clause 4 In this Notification: 'Company' means a company that has been granted a life insurance business license under the law on life insurance, and shall also mean a foreign life insurance company's branch that has been granted a license to operate a life insurance business in the Kingdom of Thailand under the law on life insurance; 'Life Insurance Agent' means a life insurance agent under the law on

	Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)	life insurance; 'Life Insurance Broker' means a life insurance broker under the law on life insurance, but excluding Banks; "Bank" means a bank that has been granted a life insurance brokerage license under the law on life insurance; ...(shorten)... "Offeror" means an employee or staff member of a Company, a Life Insurance Agent, a Life Insurance Broker, or a Bank;
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)	'Company' means a company that has been granted a non-life insurance business under the law on non-life insurance, and shall also mean a foreign non-life insurance company's branch that has been granted a license to operate a non-life insurance business in the Kingdom of Thailand under the law on non-life insurance; 'Non-life Insurance Agent' means a non-life insurance agent under the law on nonlife insurance; 'Non-Life Insurance Broker' means a non-life insurance broker under the law on nonlife insurance, but excluding Banks; 'Bank' means a bank that has been granted a life insurance brokerage license under the law on non-life insurance; ...(shorten)... 'Offeror' means an employee or staff member of a Company, a Non-life Insurance Agent, a Non-life Insurance Broker, or a Bank;
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)	'Personal data controller' means the person controlling personal data according to the law Personal information protection 'Personal data processor' means a personal data processor according to the law. Personal information protection ...(shorten)... 'Company' means a company that has received a life insurance business license in accordance with the law on life insurance and includes branches of foreign life insurance companies that have received business licenses Life insurance in the Kingdom according to the law on life insurance 'Seller' means life insurance agent. life insurance broker 'Life insurance agent' means a life insurance agent according to the law on life insurance. 'Life insurance broker' means a life insurance broker according to the law on life insurance. 'Personal Data Protection Officer' means the Personal Data Protection Officer according to Personal data protection law
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)	'Personal data controller' means the person controlling personal data according to the law on personal data. Personal information protection 'Personal data processor' means a person who processes personal data according to the law. With personal information protection ...(shorten)... 'Company' means a company that has received a license to operate a casualty insurance business according to law. Regarding casualty insurance and includes Branches of licensed foreign general insurance companies Conducting a casualty insurance business in the Kingdom in accordance with the law on casualty insurance. 'Seller' means a non-life insurance agent. General insurance broker

		'Non-life insurance agent' means a non-life insurance agent according to the law on General insurance 'Non-life insurance broker' means a non-life insurance broker according to the law on General insurance 'Personal Data Protection Officer' means the Personal Data Protection Officer according to Personal data protection law
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)	'Personal data controller' means the person controlling personal data according to the law. Personal information protection 'Personal data processor' means a person who processes personal data according to law. Concerning the protection of personal information ...(shorten)... 'Company' means a company that has received a license to operate a casualty insurance business according to law. Regarding casualty insurance and includes Branches of licensed foreign general insurance companies Conducting a casualty insurance business in the Kingdom in accordance with the law on casualty insurance. 'Casualty assessor' means a casualty assessor according to the law on casualty insurance. 'Personal Data Protection Officer' means the Personal Data Protection Officer according to Personal data protection law
51	Trade Secret Act B.E. 2545 (2002)	'Controller of Trade Secrets' means the owner of trade secrets. It shall also include the possessor, controller, or caretaker of the trade secrets. 'Court' means intellectual property and international trade court under the legislation governing the establishment of the intellectual property and international trade court and its procedure.
52	Trade Secret Act (No.2) B.E. 2558 (2015)	

Legal Basis

#	Regulation		
		consent	necessary for the performance of a contract
1	Constitution of the Kingdom of Thailand		
2	Personal Data Protection Act 2019	19 The Data Controller shall not collect, use, or disclose Personal Data, unless the data subject has given consent prior to or at the time of such collection, use, or disclosure, except the case where it is permitted to do so by the provisions of this Act or any other laws. .... 20 In the event that the data subject is a minor who is not sui	Section 24 The Data Controller shall not collect Personal Data without the consent of the data subject, unless: (3) it is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;

		juris by marriage or has no capacity as a sui juris person under Section 27 of the Civil and Commercial Code, the request for the consent from such data subject shall be made as follows: .... 23 In collecting the Personal Data, the Data Controller shall inform the data subject, prior to or at the time of such collection, of the following details, except the case where the data subject already knows of such details: ... Section 24 The Data Controller shall not collect Personal Data without the consent of the data subject, unless: (1) it is for the achievement of the purpose relating to the preparation of the historical documents or the archives for public interest, or for the purpose relating to research or statistics, in which the suitable measures to safeguard the data subject's rights and freedoms are put in place and in accordance with the notification as prescribed by the Committee; (2) it is for preventing or suppressing a danger to a Person's life, body or health; (3) it is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract; (4) it is necessary for the performance of a task carried out in the public interest by the Data Controller, or it is necessary for the exercising of official authority vested in the Data Controller; (5) it is necessary for legitimate interests of the Data Controller or any other Persons or juristic persons other than the Data Controller, except where such	

		interests are overridden by the fundamental rights of the data subject of his or her Personal Data; (6) it is necessary for compliance with a law to which the Data Controller is subjected. ... 27 The Data Controller shall not use or disclose Personal Data without the consent of the data subject, unless it is the Personal Data which is collected without requirement of consent under Section 24 or Section ... Section 26 Any collection of Personal Data pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner, as prescribed by the Committee, is prohibited, without the explicit consent from the data subject, except where: it is to prevent or suppress a danger to life, body or health of the Person, where the data subject is incapable of giving consent by whatever reason; it is carried out in the course of legitimate activities with appropriate safeguards by the foundations, associations or any other not-for-profit bodies with a political, religious, philosophical, or trade union purposes for their members, former members of the bodies, or persons having regular contact with such foundations, associations or not-for-profit bodies in connection with their purposes, without disclosing the Personal Data outside of such foundations, associations or not-for-profit bodies;	

		(1) it is information that is disclosed to the public with the explicit consent of the data subject; (2) it is necessary for the establishment, compliance, exercise or defense of legal claims; (3) it is necessary for compliance with a law to achieve the purposes with respect to: ...	
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of		

	personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA	2 Type and manner of requesting consent Requesting consent from the owner of personal data can be divided into 2 types: 2.1 In cases where there is a specific law or there is a control or supervisory agency that specifies the form or a message in requesting specific consent ... 2.2 In the case where there is no specific law or there is a control or supervision agency that specifically specifies the form or message for requesting consent that is mandatory. ... 3 Criteria for requesting consent 3.1 Requesting complete consent from the owner of personal data according to Section 19 is in accordance with the following criteria: (1) Timing for requesting consent must be obtained before or during collect, use, or disclose personal information. (2) in requesting consent from the owner of personal data Personal data controller, the purpose and details of the request for consent must be informed to the owner of personal data (informed) before giving consent	

		(3) Requesting consent must specify specific objectives for giving consent, not broad general objectives. (4) Requesting consent must be clearly separated from other messages and have a form or message easy to access and understand including using language that is easy to read and is not deceptive or misleading to the owner of the information Individuals misunderstand the purpose. (5) The request for consent is lawful only when the owner of personal data voluntary and freely given consent (freely given) from the owner of personal data without fraud, deception, threats, or misunderstandings (6) givingconsent must not be a condition that is forced or binding, or a condition that forces the owner of personal data to give consent before entering into the transaction which includes providing any service to collect, use or disclose personal information that is no longer necessary necessary or relevant for for entering into a contract, including providing that service 3.2 Requesting consent must not be part of the agreement, legal contracts or conditions for purchasing goods, providing services, or making transactions by requesting consent must be clearly separated from other messages such as contracts. They cannot be used as any part of the contract. 3.3 Requesting consent must inform the purpose of collection, use or disclose personal information in a specific manner to the owner of personal	

		information and it is prohibited to specify the purpose for collecting, using, or disclosing personal information of many types or subjects or in general terms in one request for consent 3.4 In requesting consent The personal data controller must notify the data owner personal note The following details before or while collecting, using, or disclosing personal data:... 3.5 Notification of the purpose and details of collection, use, and disclosure of personal data can be done in many ways, such as notification in writing. verbal notification, text notifications in the form of SMS, email, MMS or telephone. or any other electronic means, such as specifying details in a URL or QR code, etc. 3.6 Requesting consent must require the owner of personal data to express his intention clearly (clear affirmative act) to show clearly that consent has been given, such as submitting a consent letter prepared by the owner of personal data, signing to consent in the consent form prepared by the Personal Data Controller, clicking in the checkbox to indicate "consent" by the data owner himself, pressing the button on your mobile phone 2 times in a row shows your intention to confirm or sliding the screen (swipe), etc.,... 4. Characteristics of consent required by law Requesting consent must be made clearly (explicit) which may be in writing or through the system electronically, unless consent cannot be obtained by	

		such means. ... 5 Withdrawal of consent Owners of personal data must be able to withdraw their consent at any time unless there are restrictions, limiting the right to withdraw consent by laws or contracts that benefit the owner of personal data. The personal data controller must show details of the method, conditions, or form for withdrawing consent must be prominently displayed in a conspicuous area of the request for consent, whether in written or electronic form. ... 6. Giving consent and withdrawing consent in the case of minors (Children) In giving the consent of minors who are the owners of personal data, personal data controllers should be aware that personal data controllers must use caution and standards in requesting consent from minors who are above legal age in order to protect minors from being deceived, scammed, intimidated, wrongful or illegal actions 6.1 Conditions regarding age and nature of consent ... 6.2 Withdrawal of consent of minors ... 7. In the case where the owner of personal data is an incompetent or quasi-incompetent person In the case where the owner of personal data is an incompetent person or a quasi-incompetent person, ask for consent from the guardian who has authority to act on behalf of the incapacitated person or a powerful guardian acting on	

		behalf of a quasi-incompetent person, as the case may be, by applying the criteria for requesting consent according to the guidelines. This operation is applied mutatis mutandis	
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA	2 Type and manner of notifying the purpose and details of data collection Notification of the purpose and details of collecting, using, and disclosing personal information are divided into 2 types: 2.1 In cases where there is a specific law or a control and supervision agency including setting criteria. ... 2.2 In the case where there is no specific law or control and supervision agency, including specific criteria, methods, or guidelines for operations in informing the purpose and details of personal data collection in cases where there is no specific law or specific agency to supervise, the personal data controller should and proceed according to this guidelines. 3. Principles for notifying the purpose and details to the owner of personal data The personal data controller must notify the purpose and details of data collection. personal information to the owner of personal information before or while collecting personal information by informing the objective Such information must be subject to the following: 3.1 Fairness ... 3.2 Limiting the purposes for collecting, using, and disclosing personal information (Purpose	

		Limitation) ... 3.3 Consent ... 3.4 Claim of Legitimate Interest ... 4. Types of personal data collection Collection can be used or disclosed in 2 methods: 4.1 Collection of personal data directly from the owner of personal data Data Controllermust notify the owner of personal data before or while collecting personal data with details as follows unless the owner of personal data is already aware of the details: ... 4.2 Collection of personal data from other sources that are not the data owner. Collection of personal data from other sources that are not the data owner cannot be done according to Section 25 of the Personal Data Protection Act B.E. 2019, except in the following cases: ... 5. Exceptions to notification of the purpose and details of collecting personal information for collecting personal data from sources other than the direct owner of the personal data For the collection of personal data from sources other than the direct owner of the personal data, according to Section 25, the Personal Data Controller may not have to inform the owner of the personal data of the new purpose for collecting personal data in accordance with Section 21 and inform the purpose and details of the collection according to Section 23 as specified in 4.2, when requesting consent from the data owner in	

		the following cases: 5.1 The owner of personal data already knows the new purpose or details. ... 5.2 The Personal Data Controller can prove that notification of the new purpose or details is not possible or will hinder use or disclosure... 5.3 Use or disclosure of information for such personal information must be done urgently as required by law specified, which has provided appropriate measures to protect the interests of the owners of personal data. 5.4 When the Personal Data Controller is a person who knows or obtains personal data from his duties or from the occupation or profession and must keep the new objectives or certain details under Section 23 secret as required by law. ... 6. Notification of the purpose and details of personal data collection to the owner must be made clearly, which may be done in many ways, such as notification in writing, verbal notification, notification via message in the form of SMS, email, MMS or by telephone or by other electronic means, such as specifying details in a URL or QR code, etc ...	
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562	2.2 Question: Appointing a personal data protection officer from outsiders or personnel within the organization. What are the different advantages and disadvantages? and the organization needs to set up a department with duties specific responsibility To perform such work or not? How? Answer: Section 41, paragraph seven, of the Personal Data	2.2 Question: Appointing a personal data protection officer from outsiders or personnel within the organization. What are the different advantages and disadvantages? and the organization needs to set up a department with duties specific responsibility To perform such work or not? How? Answer: Section 41, paragraph seven, of the Personal Data

		Protection Act 2019 stipulates that the Personal Data Protection Officer may be an employee of the Personal Data Controller or Data Processor. Personally or as a contractor providing services according to a contract with the personal data controller or data processor. Therefore, it is important to consider, according to the appropriateness and necessity of the organization, how it can arrange for personal data protection officers.... 2.3 Question: Personal Data Controller (Data Controller) means a juristic person or organization, right? And is it necessary to appoint a natural person to act on behalf of the juristic person or organization in performing the duties as a personal data controller? If it is necessary to appoint a natural person to act on behalf of the juristic person or organization? Performing such duties What qualities should that person have? And does it have to be the owner of personal data or the owner of the data (Data Owner) or not? How? And should it be an outside person or within the organization? Answer: If an organization that is a juristic person has the authority to decide or take action regarding the collection, use, or disclosure of personal information. The said organization will be considered the personal data controller according to Section 6 of the Personal Data Protection Act B.E. 2019 without having to appoint any other person to act as the personal data controller. The division, agency, as well as The organization's employees and personnel will not have separate personal data controller or	Protection Act 2019 stipulates that the Personal Data Protection Officer may be an employee of the Personal Data Controller or Data Processor. Personally or as a contractor providing services according to a contract with the personal data controller or data processor. Therefore, it is important to consider, according to the appropriateness and necessity of the organization, how it can arrange for personal data protection officers.... 2.3 Question: Personal Data Controller (Data Controller) means a juristic person or organization, right? And is it necessary to appoint a natural person to act on behalf of the juristic person or organization in performing the duties as a personal data controller? If it is necessary to appoint a natural person to act on behalf of the juristic person or organization? Performing such duties What qualities should that person have? And does it have to be the owner of personal data or the owner of the data (Data Owner) or not? How? And should it be an outside person or within the organization? Answer: If an organization that is a juristic person has the authority to decide or take action regarding the collection, use, or disclosure of personal information. The said organization will be considered the personal data controller according to Section 6 of the Personal Data Protection Act B.E. 2019 without having to appoint any other person to act as the personal data controller. The division, agency, as well as The organization's employees and personnel will not have separate personal data controller or

		personal data processor status from the organization. 6.1 Question: In the case of opening an account or making a transaction via Mobile Banking and collecting and using the facial recognition of a minor (ages 7 to 20 years of age) to verify and verify the identity of the minor, must the bank request consent or not? And how? If consent is required from the minor? Can the minor give their own consent? Answer: The collection of personal data of minors in opening a bank account may be considered a legal basis according to Section 24 (3) of the Personal Data Protection Act B.E. 2019, and if it is not required. Requesting consent to collect personal data does not require compliance with Section 19 and Section 20. For activities aimed at verifying and verifying the identity of minors by using facial recognition technology, ... is a collection of biological data according to Section 26, paragraph two. The Bank must therefore consider the legal basis according to Section 26, paragraph one (1) to (5) in collecting personal information for activities with the purpose of verifying identity. When there is no such reason In this case, explicit consent must be sought from the owner of personal data. The criteria for requesting consent of minors must be in accordance with Section 19 and Section 20. 6.2 Question: In the case of opening an account or making a transaction through a Virtual Teller Machine (VTM) and Mobile Banking, the bank collects and	personal data processor status from the organization. 6.1 Question: In the case of opening an account or making a transaction via Mobile Banking and collecting and using the facial recognition of a minor (ages 7 to 20 years of age) to verify and verify the identity of the minor, must the bank request consent or not? And how? If consent is required from the minor? Can the minor give their own consent? Answer: The collection of personal data of minors in opening a bank account may be considered a legal basis according to Section 24 (3) of the Personal Data Protection Act B.E. 2019, and if it is not required. Requesting consent to collect personal data does not require compliance with Section 19 and Section 20. For activities aimed at verifying and verifying the identity of minors by using facial recognition technology, ... is a collection of biological data according to Section 26, paragraph two. The Bank must therefore consider the legal basis according to Section 26, paragraph one (1) to (5) in collecting personal information for activities with the purpose of verifying identity. When there is no such reason In this case, explicit consent must be sought from the owner of personal data. The criteria for requesting consent of minors must be in accordance with Section 19 and Section 20. 6.2 Question: In the case of opening an account or making a transaction through a Virtual Teller Machine (VTM) and Mobile Banking, the bank collects and

		uses the customer's facial recognition to verify and confirm their identity. Will the bank have to ask for consent or not? Answer: Because the collection of personal data by using facial recognition technology is a collection of biological data in accordance with Section 26, paragraph two, of the Personal Data Protection Act 2019, the Bank must consider the legal basis under Section 26. Paragraph one (1) to (5) in collecting personal information for activities with the purpose of verifying identity. When there is no such reason must request explicit consent from the owner of personal data The criteria for requesting consent must be in accordance with Section 19 and Section 20. 6.3 Question: In the case where the bank introduces new products In order to market to minor customers, must the bank seek consent from minors? And how? If consent is required, can minors give such consent? Can you do it yourself? How? Answer: Opening a bank account is a collection of personal data by virtue of Section 24 (3). It is necessary to perform a contract to which the owner of personal data is a party or for use in operations at the request of the owner of personal data before entering into the contract However, if the use of personal information for marketing purposes is an activity that is not related and is not necessary to perform the contract, it will not be able to claim legal bases according to Section 24 (3). Therefore, the Bank must consider other legal bases according to Section 24. It is considered inconsistent with	uses the customer's facial recognition to verify and confirm their identity. Will the bank have to ask for consent or not? Answer: Because the collection of personal data by using facial recognition technology is a collection of biological data in accordance with Section 26, paragraph two, of the Personal Data Protection Act 2019, the Bank must consider the legal basis under Section 26. Paragraph one (1) to (5) in collecting personal information for activities with the purpose of verifying identity. When there is no such reason must request explicit consent from the owner of personal data The criteria for requesting consent must be in accordance with Section 19 and Section 20. 6.3 Question: In the case where the bank introduces new products In order to market to minor customers, must the bank seek consent from minors? And how? If consent is required, can minors give such consent? Can you do it yourself? How? Answer: Opening a bank account is a collection of personal data by virtue of Section 24 (3). It is necessary to perform a contract to which the owner of personal data is a party or for use in operations at the request of the owner of personal data before entering into the contract However, if the use of personal information for marketing purposes is an activity that is not related and is not necessary to perform the contract, it will not be able to claim legal bases according to Section 24 (3). Therefore, the Bank must consider other legal bases according to Section 24. It is considered inconsistent with

		other legal bases according to Section 24 (1) to (6). Therefore, consent from the owner of personal data should be sought. The criteria for requesting consent from the owner of personal data must be in accordance with Section 19 and Section 20. In this regard, consent is sought from the owners of personal data who are minors who are not yet of legal age and when taking into account the appropriateness of the minor's maturity and the impact of the decision. requesting consent In marketing to minor customers There should also be consent from the person with parental authority who has the authority to act on behalf of the minor. 6.4 Question: In the case where the bank offers the same product, such as offering other types of deposit products to minor customers using deposit products or offer products that are related to existing products to minor customers, such as offering ATM cards or mobile banking. Does the bank have to ask for consent from minors or not? If so, how? Can minors give such consent themselves? How? Answer: The bank must consider the legal basis for collecting, using, or disclosing personal data in accordance with Section 24 of the Personal Data Protection Act B.E. 2019 if presenting the original product or offering products related to the original product is not relevant and is not necessary for the performance of the contract under section 24 (3) and is not consistent with other legal bases under section 24 (1), (2), (4), (5) and (6), consent must be obtained. From the owner of	other legal bases according to Section 24 (1) to (6). Therefore, consent from the owner of personal data should be sought. The criteria for requesting consent from the owner of personal data must be in accordance with Section 19 and Section 20. In this regard, consent is sought from the owners of personal data who are minors who are not yet of legal age and when taking into account the appropriateness of the minor's maturity and the impact of the decision. requesting consent In marketing to minor customers There should also be consent from the person with parental authority who has the authority to act on behalf of the minor. 6.4 Question: In the case where the bank offers the same product, such as offering other types of deposit products to minor customers using deposit products or offer products that are related to existing products to minor customers, such as offering ATM cards or mobile banking. Does the bank have to ask for consent from minors or not? If so, how? Can minors give such consent themselves? How? Answer: The bank must consider the legal basis for collecting, using, or disclosing personal data in accordance with Section 24 of the Personal Data Protection Act B.E. 2019 if presenting the original product or offering products related to the original product is not relevant and is not necessary for the performance of the contract under section 24 (3) and is not consistent with other legal bases under section 24 (1), (2), (4), (5) and (6), consent must be obtained. From the owner of

		personal data By the criteria for requesting consent from the owner of personal data. Must be in accordance with Section 19 and Section 20. In this regard, consent is sought from the owners of personal data who are minors who are not yet of legal age and when taking into account the appropriateness of the minor's maturity and the impact of the decision. requesting consent To offer the original product or offer products related to the original product to minor customers. There should also be consent from the person with parental authority who has the authority to act on behalf of the minor. 7 Question: Can withdrawing consent to process personal data from a customer through a Virtual Teller Machine (VTM) or through the Mobile Banking system, where the customer can change their consent from "consent" to "not consent", be considered a withdrawal of consent? no Or must there be a channel or menu? Allow customers to withdraw additional consent? Answer:...In this case, if the bank has clearly informed the details according to Section 23 in the Privacy Notice to the owner of personal data that the customer has pressed the “not consent” button via the Virtual Teller Machine (VTM)) or through the Mobile Banking system, which is pressing the button after pressing the button Consent has been given. It is considered to be a withdrawal of consent from providing services.... 8.1 Question: In the case where the customer has not yet filled out the consent form and has	personal data By the criteria for requesting consent from the owner of personal data. Must be in accordance with Section 19 and Section 20. In this regard, consent is sought from the owners of personal data who are minors who are not yet of legal age and when taking into account the appropriateness of the minor's maturity and the impact of the decision. requesting consent To offer the original product or offer products related to the original product to minor customers. There should also be consent from the person with parental authority who has the authority to act on behalf of the minor. 7 Question: Can withdrawing consent to process personal data from a customer through a Virtual Teller Machine (VTM) or through the Mobile Banking system, where the customer can change their consent from "consent" to "not consent", be considered a withdrawal of consent? no Or must there be a channel or menu? Allow customers to withdraw additional consent? Answer:...In this case, if the bank has clearly informed the details according to Section 23 in the Privacy Notice to the owner of personal data that the customer has pressed the “not consent” button via the Virtual Teller Machine (VTM)) or through the Mobile Banking system, which is pressing the button after pressing the button Consent has been given. It is considered to be a withdrawal of consent from providing services.... 8.1 Question: In the case where the customer has not yet filled out the consent form and has

		never given Consent for marketing purposes But the bank wishes to promote the bank's financial products and services to customers who use the bank's products. 1.1 In the case where the bank introduces new products To market to bank customers, such as offering loan products to deposit customers Do I have to ask for consent from the customer or not? 1.2 In the case where the bank offers the same product, such as offering other types of deposit products to customers who use deposit products. or offer products related to existing products to customers, such as offering ATM cards or mobile banking to bank deposit customers Do I have to ask for consent from the customer or not? Answer: Introducing new products for marketing purposes is a non-practical activity according to the original product contract. Therefore, it cannot be claimed as a base for contract performance under Section 24 (3) of the Personal Data Protection Act 2019. Therefore, it is necessary to consider other legal bases. When there is no legal basis according to Section 24 (1) to (6) to collect, use, or disclose personal information in order to present new products, consent must be sought from the owner of personal data using the criteria for consent requesting Section 19 and Section 20. ... 8.2 Question: In the case where the customer comes to fill out the consent form and opt out of consent regarding marketing purposes. 2.1 In the case where the bank	never given Consent for marketing purposes But the bank wishes to promote the bank's financial products and services to customers who use the bank's products. 1.1 In the case where the bank introduces new products To market to bank customers, such as offering loan products to deposit customers Do I have to ask for consent from the customer or not? 1.2 In the case where the bank offers the same product, such as offering other types of deposit products to customers who use deposit products. or offer products related to existing products to customers, such as offering ATM cards or mobile banking to bank deposit customers Do I have to ask for consent from the customer or not? Answer: Introducing new products for marketing purposes is a non-practical activity according to the original product contract. Therefore, it cannot be claimed as a base for contract performance under Section 24 (3) of the Personal Data Protection Act 2019. Therefore, it is necessary to consider other legal bases. When there is no legal basis according to Section 24 (1) to (6) to collect, use, or disclose personal information in order to present new products, consent must be sought from the owner of personal data using the criteria for consent requesting Section 19 and Section 20. ... 8.2 Question: In the case where the customer comes to fill out the consent form and opt out of consent regarding marketing purposes. 2.1 In the case where the bank

		offers new products, such as offering loan products to deposit customers Can the bank offer this or not? 2.2 In the case where the bank offers the same product, such as offering other types of deposit products to customers who use deposit products. or offer products related to existing products to customers, such as offering ATM cards or mobile banking to deposit customers Can the bank offer this or not? Answer: In the event that the customer does not give consent ...the Bank has no legal basis for collecting, using, or disclosing personal information. Therefore, the Bank cannot collect, use, or disclose personal information for marketing purposes for such activities. In the case of offering products related to existing products to deposit customers, such as ATM cards or Mobile Banking, the bank may consider using one of the bases for collecting, using, or disclosing personal information, such as... 9.1 Question: In the case where the company trades goods and services between natural persons and juristic persons, but the company must coordinate with natural persons who are employees or representatives of the contracting parties. So the company has a name. Telephone number and other information that is personal information of such person or not. Must the company request consent from the representative of the contracting party? Due to the exemption under Section 24 (3) of the Personal Data Protection Act 2019, the owner of personal data must enter into a contract with the Personal Data	offers new products, such as offering loan products to deposit customers Can the bank offer this or not? 2.2 In the case where the bank offers the same product, such as offering other types of deposit products to customers who use deposit products. or offer products related to existing products to customers, such as offering ATM cards or mobile banking to deposit customers Can the bank offer this or not? Answer: In the event that the customer does not give consent ...the Bank has no legal basis for collecting, using, or disclosing personal information. Therefore, the Bank cannot collect, use, or disclose personal information for marketing purposes for such activities. In the case of offering products related to existing products to deposit customers, such as ATM cards or Mobile Banking, the bank may consider using one of the bases for collecting, using, or disclosing personal information, such as... 9.1 Question: In the case where the company trades goods and services between natural persons and juristic persons, but the company must coordinate with natural persons who are employees or representatives of the contracting parties. So the company has a name. Telephone number and other information that is personal information of such person or not. Must the company request consent from the representative of the contracting party? Due to the exemption under Section 24 (3) of the Personal Data Protection Act 2019, the owner of personal data must enter into a contract with the Personal Data

		Controller. Asnwer: Consideration of the legal basis for collecting personal data in the cases discussed can be divided into two cases, namely: Case 1: In the case where the business partner or contract is a natural person who is the owner of personal data, in this case the company may use a legal base according to Section 24 (3) of the Personal Data Protection Act B.E. 2019 "Performance of the contract" This is an exception to the need for consent to collect personal data.... Case 2: The company keeps a list of names telephone number and other relevant personal information of employees or representatives of legal entities that are contracting parties for coordination purposes, deliver quotations and various documents as requested by employees or representatives of that legal entity in which case the above mentioned persons are not contracting parties of the Company, therefore, the Company cannot claim the basis of "contract performance" in collecting personal information.... 9.2 Question: In the case where the company is hired to be the manager of the condominium/village juristic person, or in the case that the company is not the juristic person manager but is hired to manage the building/village. The company needs to collect Use and disclose personal information of residents/residents for issuing invoices security Specifying personal information on parking stickers Registration of residents And providing other services, does the company have to ask	Controller. Asnwer: Consideration of the legal basis for collecting personal data in the cases discussed can be divided into two cases, namely: Case 1: In the case where the business partner or contract is a natural person who is the owner of personal data, in this case the company may use a legal base according to Section 24 (3) of the Personal Data Protection Act B.E. 2019 "Performance of the contract" This is an exception to the need for consent to collect personal data.... Case 2: The company keeps a list of names telephone number and other relevant personal information of employees or representatives of legal entities that are contracting parties for coordination purposes, deliver quotations and various documents as requested by employees or representatives of that legal entity in which case the above mentioned persons are not contracting parties of the Company, therefore, the Company cannot claim the basis of "contract performance" in collecting personal information.... 9.2 Question: In the case where the company is hired to be the manager of the condominium/village juristic person, or in the case that the company is not the juristic person manager but is hired to manage the building/village. The company needs to collect Use and disclose personal information of residents/residents for issuing invoices security Specifying personal information on parking stickers Registration of residents And providing other services, does the company have to ask

		for consent from all residents/residents? or is subject to an exception under any subsection? Answer: ...In this case, the Company is not a natural person or legal entity who has the authority to make decisions regarding the collection, use, or disclosure of personal information. The company therefore has no status. "Personal Data Controller" but has the status of "Personal data processor"….	for consent from all residents/residents? or is subject to an exception under any subsection? Answer: ...In this case, the Company is not a natural person or legal entity who has the authority to make decisions regarding the collection, use, or disclosure of personal information. The company therefore has no status. "Personal Data Controller" but has the status of "Personal data processor"….
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		

15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal		

	Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566	5. The Personal Data Controller will collect personal information regarding criminal history only when there is a provision of law that requires a criminal history check or inspection, qualifications or prohibited characteristics related to committing a criminal offense or receiving a criminal penalty or having received the express consent of the owner of personal data only. For cases where it is for the following purposes: (1) Consideration of accepting persons to work. or qualification verification prohibited characteristics or consider the suitability of the person to hold any position. (2) Inspection of qualifications or prohibited characteristics of persons in granting permission, issuing licenses, approving, registering, ... or provide other services to individuals by government agencies or designated personal data controllers to perform duties in exercising authority on behalf of government agencies. (3) Inspection of qualifications or prohibited characteristics of persons in permitting, approving, certifying, ... or provide other services to individuals by the person controlling personal data other than what is specified in (2).	

		7. The Personal Data Controller must provide appropriate organizational measures and technical measures, which may include necessary physical measures to control the collection, use, and disclosure of personal data according to this announcement to the extent necessary under the legitimate purposes of the personal data controller. 8. In collecting personal information according to this Notification, he personal data controller must provide security measures appropriate to the risks to individual rights and freedoms which must be in accordance with the minimum standards announced by the Personal Data Protection Board in accordance with Section 37 (1). 9. In the case where there is no specific provision of law and there is no necessity according to the law on personal data protection in collecting personal information about Criminal history for proceeding according to Section 5, paragraph one, when such proceeding is completed, the Personal Data Controller shall collect personal data relating to criminal history for no longer than six months from the date such processing is completed for each personal data subject according to the purpose and necessity of collecting, using, or disclosing personal information unless received the express consent of the owner of personal data is otherwise. ...	
20	Electronic Transactions Act, B.E. 2544 (2001)		

21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)	Section 5: In the case of sending computer data or electronic mail for commercial purposes other than those specified in Section 4, to an electronic address in the following manner: When consent is received from the recipient of the information and will not cause any distress or annoyance to the recipient of the information. (1) The sender of information must specify the following information in the computer data or electronic mail that is sent to each recipient of information: (a)) specify or display symbols or details and any means by which the recipient of information can Terminate or expressly request to refuse to receive computer information or letters electronic (Opt-Out) from the data sender easily ...(continue)...	Section 4: Sending computer data or electronic mail to other persons in the form The following is not considered to be sending information that causes annoyance to the recipient of the information. (1) Transmission of computer data e-mail for contact or as evidence for doing legal contract (transactional) that the parties have already agreed upon or sending information to the recipient. Information and data senders submit it to comply with the law. or to show the relationship or legal relationship that exists between them (relationship) in legal terms includes actions that have the following characteristics: ...(continue)...
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of	Section 4 4 If the following service providers can prove that they have complied with the following announcements, that service provider You will not be punished for cooperating. give consent or	

	the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)	know and understand, which Committing an offense according to Section 15 *(of the COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560)* (1) service provider as an intermediary (Intermediary) which provides computer data transmission services Through the network or computer system of the service provider or service facilitating transmission computer data through computer traffic routes on the Internet (routing) or providing computer services Computer equipment or computer network systems to cause the transmission of computer data ...(continue)...	
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		

32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)		
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications	4. Use or disclosure of personal information of service users for purposes other than operation Telecommunications business ...(shorten)... Requesting and giving consent 4.1 Requesting consent must be done clearly. Have a format or use text that is easy to understand and understand ...(shorten)... 4.2 Requesting consent must specify ...(shorten)... Withdrawal of consent 4.8 The license holder must provide 5 channels for revoking consent ...(continue)... 5. Sensitive Personal Data 5.1 is information that the license holder is required to collect, use, or disclose. Be careful. 5.2 Collection, use1 or disclosure of sensitive personal information Mai 5 can rely on the contract basis Providing telecommunication services1 But 5 must get 1 get "Explicit consent" from users of the service	3. Collection Use or disclose personal information of service users for telecommunications business operations According to the telecommunications service contract entered into with the service user 3.1 The collection, use, or disclosure of personal information of service users in this case is done by Relying on a contract basis (contract basis), which is a contract to provide telecommunications services. which does not require consent from user ...(continue)... 21. Measures to control the person assigned to collect the data. Use! Reveal and preserve information Personal information of the user of the service 21.1 Persons assigned to collect, use, disclose, and preserve personal information. of 1 user using 1 service (The assigned person) has the characteristics of a "personal data processor" according to Personal Information Protection Act This may be either a natural person

		5.3 Explicit consent must include (1) complete general consent and (2) additional conditions, namely, there must be a clear expression from the user of the service. ...(continue)... 18. Providing information about users of telecommunications numbers to the person requesting to use it to prepare a list of users of the service. 18.1 The license holder must provide user information and telecommunications number to 5 persons requesting to prepare a list. Users of the service according to Section 12, paragraph 1, of the Telecommunications Business Act B.E. 2001, which has received consent from the user. And because the information of the user1 user1 telecommunications number is considered 61 personal information, also giving the information of the user11 user1 telecommunications number to the 5 persons who request to use it to prepare a list of names 1 use 1 service It is the use1 or disclosure of personal information of users1 who use services for purposes other than business operations ...(continue)...	or a juristic person. By person 1 receiving a license 21.2 In the event that the assigned person collects, uses, discloses, and maintains personal information, of the user who uses the service to the licensee which is necessary for the performance of the telecommunications service contract It is considered to be processed on a contract basis. Therefore, the assigned person No.5 It is not necessary to obtain consent from 1 person uses 1 additional service in any way. ...(continue)...
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)		
37	The Credit Information	Section 20 A credit information company shall disclose or	

	Business Operation Act No.2 B.E. 2549 (2006)	provide information to its member or the service user who wishes to use the information for the purposes of credit analysis and issuance of credit card. In disclosing or providing such information, the prior consent must be obtained from the information subject every time, unless the information subject has already otherwise given consent, in accordance with the rules, procedures and conditions prescribed by the Committee ...(continue)... *Upon having disclosed or provided information under paragraph two, the credit information company shall notify the information subject in writing thereof within thirty days from the date of disclosure or provision of information. In case it is overall information of any member, the said member shall be informed accordingly.(repealed by The Credit Information Business Operation Act No.6 B.E. 2565 (2022)*	
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)	Section 20/1 A member may consider the information of its customers obtained from credit information company under Section 20, only in part of the information without personally identifying an information subject, to be used as one of the factors for preparing the credit scoring model, but the prior consent must be obtained from	

		the information subject. ...(continue)...	
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)	Section 20 A credit information company shall disclose or provide information ...(shorten)... Upon having disclosed or provided information under paragraph two, the credit information company shall notify the information subject in writing thereof within thirty days from the date of disclosure or provision of information. In case it is overall information of any member, the said member shall be informed accordingly. CHAPTER 3/1 Additional Provisions for Members in the Category of Credit Intermediaries Section 24/1 A credit information company shall disclose or provide information to its member in the category of credit intermediaries that wishes to use the information for the purposes of credit analysis on behalf of the persons who will grant credit. In disclosing or providing such information, prior consent must be obtained from the information subject every time, unless the information subject has already otherwise given consent, in accordance with the rules, procedures and conditions prescribed in Notifications issued by the Committee. Section 24/2 A member in the category of credit intermediaries may disclose the information of the customer applying for credit obtained from a credit information company under Section 24/1 to the persons who will grant credit, provided that such disclosure is made only to the extent necessary for the purpose of credit granting and	

		prior consent is obtained from the information subject, in accordance with the rules, procedures and conditions prescribed in Notifications issued by the Committee. Section 24/3 A member in the category of credit intermediaries may use the information of its customer obtained from a credit information company under Section 24/1 only in the parts not containing the information identifiable to the information subject as a factor for creating a credit scoring model, provided that consent from the information subject is obtained. ...(continue)...	
42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)	Section 7. Personal health information shall be kept confidential. No person shall disclose it in such a manner as to cause damage to him or her, unless it is done according to his or her will, or is required by a specific law to do so. Provided that, in any case whatsoever, no person shall have the power or right under the law on official information or other laws to request for a document related to personal health information of any person other than himself or herself.	
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules	4.2 Process for selling and providing services There is a sales and service process as appropriate. The service provider can specify specified in accordance with Business operation model and suitability for each type of product, taking into account the	

		following matters: 4.2.1 Collecting information and analyzing customers before presenting products to customers. The service provider must provide the following process: Customer grouping and customer analysis (1) Determine how to classify customers, such as retail customers who are vulnerable customers. To be able to present products that are consistent with the type of customers. Including providing information and warnings about various precautions appropriate to each type of customer. (2) There are work procedures. System for inquiring and collecting information about customers that will be to ensure that The service provider knows the information and details of the customer, such as wishes, financial ability, and ability to understand the customer. ...(shorten)... Having a system for checking customer information There is a system, process , or verification method to ensure that customers provide information themselves. Including all related documents must be signed or consented to by the customer or the person authorized to sign on behalf of the customer only. and regularly review and update information to be current 6. Minimum standards for maintaining customer data (data privacy) ...(shorten)... 6.1 Maintaining the security of customer data 6.1.1 Having policies,	

		procedures , and work systems for maintaining the security of customer data in accordance with generally accepted international standards Under the framework of 3 important principles: confidentiality of the system and information (confidentiality), the accuracy and reliability of systems and data (integrity), and the availability of information technology. (availability) which is consistent with the business plan and ready to accept changes in both information technology and business by taking into account the following issues. ...(shorten)... 6.2 Disclosing customer information to other parties 6.2.1 There is a process that to ensure that the recipient of the information This includes business partners who release products together in a co-brand manner, able to maintain tight security of customer data. Collect customer information as necessary and use the information according to the purposes notified to the customer. without disturbing customer privacy continuously and taking into account the ability of the recipient to take care of customer data and the ability of the service provider In controlling the care of the recipient's information, it is an important factor. 6.2.2 Disclosing customer information to other parties for marketing purposes It is a disclosure of information for Promotion or public relations of various products and services which customers have the right to choose in providing Consent to disclose information is optional.	

		This does not affect the consideration of using the product. Please allow the service provider to request Consent to disclose information for marketing purposes from customers by proceeding as follows: 6.2.3 Disclosing customer information to other persons for purposes other than marketing, proceed as follows. ...(continue)...	
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)	Clause 17 If, due to certain necessity, a usual Offering-for-sale of Insurance Policies through meetings with a Company's Staff Members or Employees, Life Insurance Agents, or Life Insurance Brokers pursuant to Clause 16 above, is unfeasible, the Offering-for-sale of Insurance Policies may be conducted by communication through electronic devices carrying voice, or voice and images of the intended Offering-for-sale of Insurance Policies; provided that a target Customer's consent is obtained and a Company or an Offeror undertakes the following acts at a minimum: (1) ensuring readiness of the following systems or processes at a minimum: (a) Recording and storing of conversations; (b) Acquisition, retention, and protection of Customer data in due compliance with the law; (c) Auditing of sales quality and appropriate risk management; (d) An information system that is stable and secured in due compliance with the law; (e) A business continuity plan.	
47	The Notification of the Office of Insurance Commission Re: Rules, Methods	Clause 17 If, due to certain necessity, a usual Offering-for-sale of Insurance Policies through meetings with a Company's Staff Members or	

	for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)	Employees, Non-life Insurance Agents, or Non-life Insurance Brokers pursuant to Clause 16 above, is unfeasible, the Insurance Policies Sales Offering may be conducted by communication through electronic devices carrying voice, or voice and images of the intended Sales Offering of Insurance Policies; provided that a target Customer's consent is obtained and a Company or an Offeror undertakes the following acts at a minimum: (1) ensuring readiness of the following systems or processes at a minimum: (a) Recording and storing of conversations; (b) Acquisition, retention, and protection of Customer data in due compliance with the law; (c) Auditing of sales quality and appropriate risk management; ...(continue)...	
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)	Category 1 company Section 3: The company must collect, use, or disclose personal information according to the purposes that have been informed to customers. Before or while collecting personal information If the company finds or knows that there is a purpose for collecting, using, or disclosing personal information in addition to the original purpose. which is in addition to what is specified in the protection policy Personal information (privacy notice) at present or in the event that there is a change in the purpose of collecting, using, or disclosing personal information. The company will add or change the purposes for collecting, using or disclosing information. Personal is fine.	

		Where the new purpose requires a consent basis The company must ask for consent. from customers for additional collection, use, or disclosure of personal information for new purposes. In this regard, the company must improve the personal data protection policy to cover the objectives. Such new purpose and inform the customer of the new purpose as well. This may be reported in various channels that the company can prove. that it is appropriate to communicate to customers This may be considered from the channels through which the company normally interacts with customers. Or channels through which customers can easily access or know the personal data protection policy, such as sending via post, e-mail, telephone communication (SMS), which may be the same channel as the one in which the policy was previously communicated. Protection of personal information has been previously possible. and in the case where the company uses the website to interact with customers Let the company announce it on the company's website as well. Section 5 allows the company to request consent to collect, use, or disclose personal information in the case that cannot rely on the basis for processing personal data according to Section 24, Section 25, and Section 26 of the Personal Data Protection Act B.E. 2019, considering the type of personal data according to Section 4. The company may rely on the basis for processing. Personal data for various operations according to the following guidelines	

		...(continue)... Article 6 In the case where the company must request consent In collecting, using, or disclosing personal information, the company should consider determining methods for requesting consent that are appropriate for collecting, using, or disclosing information. their personal This is in line with the criteria for requesting consent according to the law on personal data protection. The company may proceed with the following guidelines. ...(continue)... Article 7: The company must provide customers with the ability to withdraw their consent to collect, use, or disclose personal data as required by the law on personal data protection. The customer can withdraw their consent at any time and it must be done as easily as giving consent. Unless there is a restriction on the right to withdraw consent. By law or contract that benefits customers As required by the Personal Data Protection Act, for example, customers must be able to withdraw their consent through the same channel used to give their consent. without having steps additional information that is established as an obstacle to requesting the withdrawal of such consent. and the company must provide a system for recording Withdraw said consent as evidence. Article 14 In the case where the company is the controller of personal data Personal information that the company has collected before June 1, 2022, the company can continue	

		to collect and use that personal information for the original purpose. The method must be specified to revoke consent and disseminate information to customers who do not wish to be collected by the company. and continue to use such personal information, you can easily withdraw your consent. ...(continue)... Category 2 life insurance agent Article 15 In the case where a life insurance agent is a personal data processor of any company, the life insurance agent must collect, use or disclose general personal data or sensitive personal data as instructed or The agreement exists only with that company. Therefore, it is considered data processing based on the same legal base as that company. However, in the case where the life insurance agent is the controller of personal information The legal basis must be considered. For each purpose, it is done on a case-by-case basis in accordance with the law on personal data protection. Article 16 In the case where the company cannot rely on the basis for processing personal data according to Section 24, Section 25 and Section 26 of the Personal Data Protection Act B.E. 2019 and is required to request consent. In collecting, using or disclosing personal information to life insurance agents who process personal data The Company requests consent from customers in accordance with the Personal Data Protection Act on behalf of the Company, which includes collecting, using, or	

		disclosing personal data of minors. incompetent person or a person who is also quasi-incompetent The life insurance agent may proceed according to the following guidelines. ...(continue)... Article 17 In the case where a life insurance agent is assigned by the company to receive a request to withdraw consent. In collecting, using, or disclosing personal information from customers Let the life insurance agent proceed according to the guidelines. Withdraw consent given by the company according to Section 7. Section 3 life insurance broker Article 24 Life insurance brokers must collect, use, or disclose personal information according to the purposes for which they were obtained. Inform customers before or at the time of collecting personal information. If the life insurance broker finds or knows that there is a purpose In collecting, using or disclosing personal information in addition to the original purpose. which is in addition to what has been Specified in the current Personal Data Protection Policy (Privacy Notice) or in the event of changes. Purpose for collecting, using, or disclosing personal information Life insurance brokers will add or change The purpose of collecting, using, or disclosing personal information can be Where the new purpose requires a consent basis Life insurance brokers must request Consent from customers for collecting, using, or disclosing personal information for new purposes is additionally	

		...(continue)... Article 26: Life insurance brokers must request consent to collect, use, or disclose information. Personal data of customers for cases where personal data processing cannot be based on Section 24, Section 25, and Section 26 of the Personal Data Protection Act B.E. 2019, considering the type of data. Personal data according to Section 4. However, life insurance brokers may rely on the processing of personal data for Take various actions according to the following guidelines. ...(continue)... Article 27 In the case where the life insurance broker must request consent. In collecting, using or disclosing, life insurance brokers should consider determining methods for requesting consent that are appropriate for the collection. Personal Information: Use or disclose your personal information. This is consistent with the criteria for requesting consent according to the law on Protection of personal information. Life insurance brokers may operate according to the following guidelines. ...(continue)... Article 28 Life insurance brokers must provide customers with the ability to withdraw their consent to collect, use, or disclose personal information as required by the Personal Data Protection Act. The customer will withdraw the complaint. Consent at any time It must be as easy as giving consent. Unless there is a restriction on the right to withdraw. Consent by law or	

		contract that benefits the customer As required by the Personal Data Protection Act, for example, customers must be able to withdraw consent through the same channel used to give consent. There are no additional steps established to act as an obstacle to withdrawing such consent. and insurance brokers Life must provide a system for recording such withdrawals of consent as evidence, in accordance with the law. Concerning the protection of personal information Article 35 In the case where the life insurance broker is the controller of personal information. Personal information provided by the broker Life insurance was collected before June 1, 2022. Life insurance brokers can collect and use Personal information can be continued for the original purpose. The method for revoking consent must be specified and published. Publicize to customers who do not wish for life insurance brokers to continue collecting and using such personal information. Can easily withdraw consent ...(continue)...	
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)	Section 5 allows the company to request consent to collect, use, or disclose personal information in the case that cannot rely on the basis for processing personal data according to Section 24, Section 25, and Section 26 of the Personal Data Protection Act B.E. 2019, considering the type of personal data according to Section 4. The company may rely on the basis for processing. Personal data for various operations according to the following guidelines	Article 10 Status of the company Companies that collect, use, or disclose personal information related to insurance business operations As an insurer or reinsurer Have the authority to make decisions regarding the collection, use, or disclosure of information. personal data for various purposes, as well as the period of personal data retention itself, such as collecting data Personal information of customers and related persons for consideration of insurance

		...(continue)... Article 6 In the case where the company must request consent In collecting, using, or disclosing personal information, the company should consider determining methods for requesting consent that are appropriate for collecting, using, or disclosing information. their personal This is in line with the criteria for requesting consent according to the law on personal data protection. The company may proceed with the following guidelines. ...(continue)... Article 7: The company must provide customers with the ability to withdraw their consent to collect, use, or disclose personal data as required by the law on personal data protection. The customer can withdraw their consent at any time and it must be done as easily as giving consent. Unless there is a restriction on the right to withdraw consent. By law or contract that benefits customers As required by the Personal Data Protection Act, for example, customers must be able to withdraw their consent through the same channel used to give their consent. without having steps additional information that is established as an obstacle to requesting the withdrawal of such consent. and the company must provide a system for recording Withdraw said consent as evidence. as follows Article 14 In the case where the company is the controller of personal data Personal information that the company has collected before June 1, 2022, the company can continue	reinsurance Consider accepting reinsurance and comply with insurance contracts. Consider and perform actions related to compensation payment, prepare legal registers. as evidence in fighting legal cases or to offer for sale or carry out business activities Direct marketing, etc., has the characteristics of being a controller of personal information. However, the company as an insurer or reinsurer may be characterized as a processor. Personal information If the collection, use, or disclosure of personal information has been carried out on behalf of or under the order of Other specific data controllers

		to collect and use that personal information for the original purpose. The method must be specified to revoke consent and disseminate information to customers who do not wish to be collected by the company. and continue to use such personal information, you can easily withdraw your consent. ...(continue)... Article 16 In the case that the company cannot rely on the basis for processing personal data according to Section 24, Section 25 and Section 26 of the Personal Data Protection Act B.E. 2019 and is required to request assistance. Consent to collect, use, or disclose personal information to the insurance agent who processes the data The Company requests consent from customers in accordance with the Personal Data Protection Act on behalf of the Company. This includes collecting, using, or disclosing the personal information of minors. incompetent person or a virtual person without ability too The insurance agent may proceed according to the following guidelines. ...(continue)... Article 17 In the case where a non-life insurance agent is assigned by the company to receive a withdrawal request. Consent for collecting, using, or disclosing personal information from customers Let the insurance agent handle it. According to the guidelines for withdrawing consent set by the company according to Section 7. Article 23 In the case where a general insurance agent is a processor of personal data,	

		manage the data. Personal information collected, used or disclosed before 1 June 2022 according to the guidelines set by the company. In the case where the general insurance agent is the controller of personal information Insurance agents can Continue to collect and use that personal information according to the original purpose. The method for revoking consent must be specified. and distribute public relations information to customers who do not wish for non-life insurance agents to collect and use such personal information. Next, you can easily cancel your consent. ...(continue)... Article 26: General insurance brokers must request consent to collect, use, or disclose information. Personal data of customers for cases where personal data processing cannot be based on Section 24, Section 25, and Section 26 of the Personal Data Protection Act B.E. 2019, considering the type of data. Personal data according to Section 4. However, the insurance broker may rely on the processing of personal data for Take various actions according to the following guidelines. ...(continue)... Article 27 In the case where the non-life insurance broker must request consent. To collect, use or Reveal personal information General insurance brokers should consider determining methods for requesting consent that are appropriate for the collection, use, or disclosure of their personal information. in accordance with the criteria for	

		requesting consent according to Personal data protection laws. Non-life insurance brokers may operate according to the following guidelines. (1) Requesting consent This must be done clearly in writing or through an electronic system, except where consent cannot be obtained by such means, consent may be obtained by other means, ...(continue)... Article 28: Non-life insurance brokers must provide customers with the ability to withdraw their consent to the collection, use, or disclosure of personal information as required by the Personal Data Protection Act. The customer may withdraw consent at any time. It must be as easy as giving consent. Unless there are rights restrictions. To withdraw consent by law or contract that benefits the customer. According to the law on data protection For example, customers must be able to request withdrawal of consent through the same channels used to give consent without additional steps being established to hinder such withdrawal of consent, and general insurance brokers must Provide a system for recording such withdrawals of consent as evidence, in accordance with the law on personal data protection. Article 35 In the case where the general insurance broker is the controller of personal information. Personal information provided by the broker Non-life insurance was collected before 1 June 2022. Non-life insurance brokers can collect Collect and use that personal information further for the original purpose. The method	

		for revoking consent must be specified and Publish public relations to customers who do not wish to have their personal information collected and used by insurance brokers. As mentioned above, you can easily cancel your consent. ...(continue)...	
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)	Section 5: The casualty assessor shall request consent from the insured to collect, use, or disclose personal information of the insured in cases where personal data processing cannot be relied upon in accordance with Section 24, Section 25, and Section 26 of the Personal Data Protection Act. Persons Act 2019, considering the type of personal information according to section 4. Clause 6 In the case where the casualty assessor must request consent from the insured. In collecting, using or disclosing personal information Let the casualty assessor consider determining methods for requesting consent that are appropriate for the collection, use, or disclosure of his or her personal information. This is in line with the criteria for requesting consent. According to the law on personal data protection, the casualty assessor may proceed according to the following guidelines. (1) Requesting consent from the insured. This must be done clearly in writing or through the system. electronics Except where consent cannot be obtained by such means, consent may be obtained by other means. ...(continue)... Article 7 The casualty assessor must arrange for the insured to withdraw consent for the	

		collection, use, or disclosure of personal information as required by the Personal Data Protection Act. The insured may withdraw consent at any time. And it must be as easy as giving consent. Unless there is a restriction on the right to withdraw consent by law or contract that benefits the insured. As required by the Personal Data Protection Act, for example, the insured must be able to request a withdrawal. Consent was obtained through the same channels used to give consent. There are no additional steps required. It is an obstacle to withdrawing consent, for example. It is an obstacle to withdrawing such consent. and the casualty assessor must provide a system for recording withdrawals. Alternatives to requesting withdrawal of consent Such consent must also be kept as evidence. Article 14 In the case where the casualty assessor is the controller of personal information. Personal information that the evaluator Casualty data was collected before June 1, 2022. Casualty assessors can collect and use the data. That personal can continue according to its original purpose. The method for revoking consent must be specified and publicized. The insured person who does not wish for the casualty assessor to continue collecting and using such personal information can notify Easily revoke consent ...(continue)...	
51	Trade Secret Act B.E. 2545 (2002)	Section 6 The infringement of trade secret rights under this Act are the act of disclosure, deprivation or usage of trade secrets without the consent of the owner in a manner contrary	Section 5 Trade secrets are transferable. The trade secrets owner is entitled to disclose, deprive of, or use the trade secrets, or license someone else to disclose, deprive of, or use the

		to honest trade practices. In so doing, the infringer must be aware of or has reasonable cause to be aware that such act is contrary to honest trade practices. Acts contrary to honest trade practices under paragraph one shall include breach of contract, infringement or inducement to infringe confidentiality, bribery, coercion, fraud, theft, receiving of stolen property or espionage through electronics or other means.	trade secrets. He may also stipulate any terms and conditions for the maintenance of the secrecy. The transfer of trade secrets under paragraph one, except by way of inheritance, shall be made in writing signed by the transferor and transferee. If no time period is specified in the contract, it shall be deemed to cover a period of ten years.
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation		
		necessary for compliance with a legal obligation	necessary in order to protect the vital interests
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019	Section 24 The Data Controller shall not collect Personal Data without the consent of the data subject, unless: (4) it is necessary for the performance of a task carried out in the public interest by the Data Controller, or it is necessary for the exercising of official authority vested in the Data Controller;	Section 24 The Data Controller shall not collect Personal Data without the consent of the data subject, unless: (2) it is for preventing or suppressing a danger to a Person's life, body or health;
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the		

	data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for		

	collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562		

	(2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		

18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566	5. The Personal Data Controller will collect personal information regarding criminal history only when there is a provision of law that requires a criminal history check or inspection, qualifications or prohibited characteristics related to committing a criminal offense or receiving a criminal penalty or having received the express consent of the owner of personal data only. For cases where it is for the following purposes: (1) Consideration of accepting persons to work. or qualification verification prohibited characteristics or consider the suitability of the person to hold any position. (2) Inspection of qualifications or prohibited characteristics of persons in granting permission, issuing licenses, approving, registering, ... or provide other services to individuals by government agencies or designated personal data controllers to perform duties in exercising authority on behalf of government agencies. (3) Inspection of qualifications or prohibited characteristics of persons in permitting, approving, certifying, ... or provide other services to individuals by the person controlling personal data other than what is specified in	

		(2). 7. The Personal Data Controller must provide appropriate organizational measures and technical measures, which may include necessary physical measures to control the collection, use, and disclosure of personal data according to this announcement to the extent necessary under the legitimate purposes of the personal data controller. 8. In collecting personal information according to this Notification, he personal data controller must provide security measures appropriate to the risks to individual rights and freedoms which must be in accordance with the minimum standards announced by the Personal Data Protection Board in accordance with Section 37 (1). 9. In the case where there is no specific provision of law and there is no necessity according to the law on personal data protection in collecting personal information about Criminal history for proceeding according to Section 5, paragraph one, when such proceeding is completed, the Personal Data Controller shall collect personal data relating to criminal history for no longer than six months from the date such processing is completed for each personal data subject according to the purpose and necessity of collecting, using, or disclosing personal information unless received the express consent of the owner of personal data is otherwise. ...	

20	Electronic Transactions Act, B.E. 2544 (2001)		
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and		

	removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and		

	Freedom of Communications B.E.2566 (2023)		
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications	6. Exemption from collection. Yes! or disclose personal information of users of the service. NBTC Announcement, 6.1 Item 1, except as specified in the announcement. NCPO Section 8 (1) together with Section 19 are responsible for sending personal information of the user of the service that the license holder provides to the NBTC or the NBTC Office upon receipt of the request. For the benefit of regulating telecommunications business operations according to the law, for consideration. ...(continue)...	
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)	CHAPTER 2 Credit Information Business Operation Section 9 No one other than a credit information company shall operate credit information business. Section 10 No credit information company, information controller and information processor shall store prohibited information. Section 11 No one other than a credit information company shall use the prefix of its name or words showing the name in business as "**บริษัทข้อมูลเครดิต** (credit information company)" or any other words of the same meaning. Section 12 No credit information company or information controller or information processor carrying on or operating business in the Kingdom shall operate, control	

		or process information outside the Kingdom. Section 13 No credit information company, information controller or information processor shall process information that is older than that prescribed in the notification of the Committee. Section 14 No one shall announce or advertise that he can revise information to be different from that stored by a credit information company. Section 15 No person or juristic person shall enter into an agreement or do any act which obstructs or impedes the provision of credit information to, or the use of information by, any credit information company, or monopolize the credit information business operation, without the approval of the Committee. CHAPTER 3 Rights and Duties of Credit Information Company, Member and Service User Section 16 A credit information company must process information from the members or from reliable sources of information in accordance with the rules, procedures and conditions prescribed in the notification of the Committee. Section 21 A service user of the same category is entitled to receive information equally from the credit information company. Section 23 The person who has obtained the information under paragraph two of Section 20 shall use the said information for such purposes specifically, and shall maintain the confidentiality of the said information by keeping it in a safe place so as to prevent others from reaching such information.	

37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)	Section 7. Personal health information shall be kept confidential. No person shall disclose it in such a manner as to cause damage to him or her, unless it is done according to his or her will, or is required by a specific law to do so. Provided that, in any case whatsoever, no person shall have the power or right under the law on official information or other laws to request for a document related to personal health information of any person other than himself or herself.	Section 10. In the case where there exists an incident affecting health of the public, a State agency having information related to such incident shall expeditiously provide and disclose such information and the protection thereof to the public. The disclosure under paragraph one shall not be done in such a manner as to infringe personal right of any specific person.

44	The Payment System Act B.E. 2560 (2017)	Section 25. Business providers shall keep data, accounts, documents, seals or other evidence pertaining to its business, assets and liabilities for the purpose of examination in accordance with the rules as prescribed in the notification of the BOT.	
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life	Article 13 In the case where the company is the controller of personal data Create a personal information retention policy. within the organization to determine the retention period for personal information which	

	Insurance Business B.E. 2564 (2021)	must determine the appropriate and necessary time period For each type of personal data and the purpose that is notified to the customer, the Company may specify a period of time. Minimum retention of personal data for the duration of the insurance contract or until the relationship with the company ends, such as in the case where the company refuses to accept insurance. or the insured requests to cancel or surrender the insurance policy. However, if the company has a need to continue collecting that personal information. The company may also collect information. That personal information can be stored, for example, by collecting personal information of a prospect who has been refused insurance. For the benefit of preventing fraud or to comply with other related laws ...(continue)... Article 34 In the case where the life insurance broker is the controller of personal information. Create a retention policy. Personal information within the organization to determine the retention period for personal information which must be specified for a period of time That is appropriate and necessary for each type of personal information and the purpose that has been informed to the customer. However, if the life insurance broker has a need to continue collecting that personal information. Life insurance brokers may also collect it. Personal information can be stored, for example, to comply with other relevant laws. ...(continue)...	

49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		Article 13 In the case where the company is the controller of personal data Create a data retention policy. Personal information within the organization to determine the retention period for personal information which must be specified for an appropriate period of time and is necessary for each type of personal data and the purpose that has been informed to the customer, the company may specify Minimum period of retention of personal data according to the expiration of the insurance contract or until the end Relationship with the company, such as in the case where the company refuses to accept insurance or the insured requests cancellation or surrender insurance policy. However, if the company has a need to continue collecting that personal information, the company may collect that personal information, such as collecting personal information of a prospect who is rejected from accepting insurance for the benefit of Fraud protection or to comply with other related laws ...(continue)...
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)	Article 13 In the case where the casualty assessor is the controller of personal information. Create a retention policy. Personal information within the organization to determine the retention period for personal information which must be specified for a period of time Appropriate and necessary for each type of personal information and the purpose notified to the insured. However, if the casualty assessor has a need to collect that personal information further. The casualty assessor may Collect that personal information, for	

		example to comply with other relevant laws. ...(continue)...	
51	Trade Secret Act B.E. 2545 (2002)	Section 7 Any of the following acts against trade secrets shall not be considered an infringement: (1) Disclosure or use of trade secrets by a person who has obtained the trade secrets through a transaction without knowing or having reasonable cause to know that the other party to the transaction obtained the trade secrets through the infringement thereof. (2) Disclosure or use of trade secrets by state agency which is responsible for their maintenance in the following circumstances: ...(continue)...	
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation		
		necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	necessary for the purposes of the legitimate interests pursued by the controller or by a third party
1	Constitution of the Kingdom Of Thailand	4. Human dignity, rights, liberties and equality of the people shall be protected 32. Human dignity, rights, liberties and equality of the people shall be protected. An act violating or affecting the right of a person under paragraph one, or an exploitation of personal information in any manner whatsoever shall not be permitted, except by virtue of a provision of law enacted only to the extent of necessity of public interest.	

2	Personal Data Protection Act 2019	Section 24 The Data Controller shall not collect Personal Data without the consent of the data subject, unless: (1) it is for the achievement of the purpose relating to the preparation of the historical documents or the archives for public interest, or for the purpose relating to research or statistics, in which the suitable measures to safeguard the data subject's rights and freedoms are put in place and in accordance with the notification as prescribed by the Committee;	Section 24 The Data Controller shall not collect Personal Data without the consent of the data subject, unless: (5) it is necessary for legitimate interests of the Data Controller or any other Persons or juristic persons other than the Data Controller, except where such interests are overridden by the fundamental rights of the data subject of his or her Personal Data;
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of		

	the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses		

	that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re:	4. In collecting personal data without the consent of the owner of the personal data to achieve the objectives related to	

	Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other	research studies or statistics according to Section 24 (1) of the Personal Data Protection Act 2019, the Personal Data Controller must provide appropriate protection measures to protect the rights and freedoms of personal data owners as follows: (1) The Personal Data Controller must provide organizational measures. appropriate organizational measures and technical measures, which may include necessary physical measures.... (2) The Personal Data Controller must provide appropriate security measures for risks to individual rights and freedoms which must meet the minimum standards set by the Personal Data Protection Committee... (3) The Personal Data Controller must provide appropriate measures to control and supervise the collection of personal data to achieve the objectives related to such research studies or statistics in compliance with relevant ethical standards without violating the law... 5. In collecting personal information regarding race, ethnicity, political opinions, creed, religion or philosophy, sexual behavior, criminal history, health information, disability, union information, genetic information, biological information, or any other information that affects the data owner in the same manner as specified in the announcement of the Personal Data Protection Committee without the express consent of the owner of personal data that is necessary to comply with the law in order to achieve objectives regarding scientific	

		research studies. history or statistics or other public benefits according to Section 26 (5) (d) of the Personal Data Protection Act B.E. 2019, the Personal Data Controller must provide appropriate measures to protect basic rights and interests of the owner of personal data as follows: (1) The Personal Data Controller must consider the reasons for necessity and consider that collection of personal data to achieve purposes related to scientific research studies history or statistics or other such public benefits is a case where it is necessary as provided by law, necessary for the performance of duties in carrying out missions in the public interest... (2) The Personal Data Controller must provide organizational measures and technical measures, which may include necessary physical measures to control the collection of such personal data to the extent necessary for purposes related to scientific research, history or statistics or other public benefits taking into account relevant academic principles, including... (3) The personal data controller must provide appropriate security measures with risks to individual rights and freedoms which must meet the minimum standards set by the Personal Data Protection Committee... (4) The Personal Data Controller must provide appropriate measures to control and supervise the collection of personal data to achieve purposes related to scientific research studies, history or statistics are in accordance with relevant and accepted ethical standards and do not violate the law...Such relevant and accepted	

		ethical standards shall include the contents of the following documents: (a) The Belmont Report:... (b) Good Clinical Practice (GCP) by... (c) International Ethical Guidelines for Health-related Research Involving Humans by ... . 6. Subject to Articles 4 and 5 in collecting personal data to achieve objectives related to research studies or statistics according to section 24(1) or to achieve the objectives about scientific research history or statistics according to Section 26 (5) (Ngor) of the Personal Data Protection Act B.E. 2019, the Personal Data Controller shall also provide the following measures: (1) Even though the collection, use, or disclosure of personal data to achieve the said purpose will be exempt from requesting consent from the owner of personal data but the personal data controller must supervise those who carry out research or statistics studies under section 24 (1) or those who carry out scientific research study history or statistics according to section 26 (5) (d) to request consent for participation in the research study (informed consent for research participation) from the participants Research subject (research subject) unless it is one of the following cases: ... (2) In collecting personal data to achieve objectives related to research studies or statistics according to section 24 (1) or to achieve objectives related to scientific research studies history or statistics according to section 26 (5) (d) directly from	

		the owner of personal data, the Data Controller must inform the owner of such personal data about the purpose of the research, study brief details, personal information to be collected in research studies... (3) In collecting Personal data to achieve research studies...in which exercising the right to request access or obtain a copy of personal data related to the owner of personal data who is a research study participant may cause the reseach not be achieved, for example,..., the Personal Data Controller must supervise the processor in the research study to inform the owners of personal data who are research study participants about the limitations of request access to or obtain a copy of such personal information... 7. In the case where the Personal Data Controller has duties under other laws related to research studies or statistics according to section 24 (1) or scientific research studies history or statistics or other public benefits according to Section 26 (5) (d), the Personal Data Controller shall proceed according to that law. But measures are taken to protect the rights, freedoms, and interests of the owners of personal data who are participants of the research study or statistics or scientific research study history or statistics or public interest must also be complied to the Notification	
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for		

	Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)		
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act,		

	No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending		

	proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)		
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and		

	Freedom of Communications		
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)		
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)		

44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		Article 10 Status of the company Companies that collect, use, or disclose personal information related to insurance business operations as an insurer or reinsurer. Have the authority to make decisions regarding the collection, use, or disclosure of information. Personal data for various purposes, as well as the period of personal data retention itself, such as collecting data Personal information of

			customers and related persons for consideration of insurance reinsurance Consider accepting reinsurance and comply with insurance contracts. Consider and perform actions related to compensation payment, prepare legal registers. as evidence in fighting legal cases or to offer for sale or carry out business activities Direct marketing, etc., has the characteristics of being a controller of personal information. However, the company as an insurer or reinsurer may be characterized as a processor. Personal information If the collection, use, or disclosure of personal information has been carried out on behalf of or under the order of Other specific data controllers
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		Article 10 Status of the company Companies that collect, use, or disclose personal information related to insurance business operations as an insurer or reinsurer Have the authority to make decisions regarding the collection, use, or disclosure of information. personal data for various purposes, as well as the period of personal data retention itself, such as collecting data Personal information of customers and related persons for consideration of insurance reinsurance Consider accepting reinsurance and comply with insurance contracts. Consider and perform actions related to compensation payment, prepare legal registers. as evidence in fighting legal cases or to offer for sale or carry out business activities Direct marketing, etc., has the characteristics of being a controller of personal information. However, the company as an

			insurer or reinsurer may be characterized as a processor. Personal information If the collection, use, or disclosure of personal information has been carried out on behalf of or under the order of Other specific data controllers
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)		
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation	opt-out	others
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019		
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from		

	maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects		

	according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		3 The provisions of Chapter 2, Section 3, Section 5, Section 6 and Section 7 and Section 95 of the Personal Data Protection Act B.E. 2019 shall not be applied to the personal data controller who is an agency or business listed in the annex of this Royal Decree. For the benefit of protecting personal information, the personal data controller under paragraph onemust provide measures to maintain the security of personal information in accordance with the standards set by the Ministry Digital Economy and Society
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		3 The provisions of Chapter 2, Section 3, Section 5, Section 6 and Section 7 and Section 95 of the Personal Data Protection Act B.E. 2019 shall not be applied to the personal data controller who is an agency or business listed in the annex of this Royal Decree. For the benefit of protecting personal information, the personal data controller under paragraph onemust provide measures to maintain the security of personal information in accordance with the standards set by the Ministry Digital Economy and Society
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations		

	which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under		

	Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)		
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		

24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)	Section 6: The data sender is a website service provider. Application service provider or service provider types of social media that advertise or encourage the sending of information or electronic mail. must be provided measures or channels for termination Cancel or refuse to receive the above information or electronic mail to users of their websites, applications, or social media. The website service provider Application service provider or social media service providers must provide details of measures or channels for terminating, canceling, or refusing to receive information or electronic mail to users of the service And such measures or channels must be measures that service users can easily understand and access. In the case where the website provider Application service provider or social media service providers online that does not comply with Section 5, it is considered that the website service provider Application service provider or service provide Such type of social media has the same liability as the person sending the information under Section 11.	
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of	Section 5 Service providers according to Item 4 who prove that they have prepared the following measures: to notify and suspending the dissemination or removal of such computer data from the computer system will	

	the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)	not be punished according to Section 15 (of the COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560) (1) Notification procedure The service provider must provide notification measures by preparing a written notice (Take Down Notice) by using any technical means or means to notify the service provider to suspend. The dissemination or deletion of illegal computer data from computer systems under its control. The service provider's notification letter must include the following information: Let the general public know ...(shorten)... (3) Methods for suspending or removing computer data When the service provider receives the complaint according to the form in item 5 (1) (b) and documentary evidence related The service provider must take the following actions: (a) Delete or modify computer data to prevent it from spreading further immediately (b) Prepare a copy of the complaint including details of the complaint of the person making the complaint sent immediately to service users or members or related persons under the control of the service provider. ...(continue)...	
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		

29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)		
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications		
35	The Royal Decree on Measures for Protection and Suppression of		Section 12. The disclosure, exchange, access, as well as the collection, collection, or use of personal information in

	Technology Crimes B.E. 2566 (2023)		accordance with this Royal Decree is not subject to the data protection law personal information, but the person receiving or possessing the information may not disclose it to other persons who do not have relevant duties.
36	The Credit Information Business Operation Act B.E. 2545 (2002)		
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)		Section 27. No one shall advertise or disseminate by means of mass media or any other means of information technology any information on a Child or the Child's Guardian, with the intention to cause damage to the mind, reputation, prestige, or other interests of the

			Child, or for seeking benefits for oneself or for others in an unlawful manner. Section 50. A Guardian of the Child's welfare or a Child's welfare protector shall not reveal the Child's first name, last name, photo, or any information about the Child or the Child's Guardian, in a manner which would damage their reputation or their rights. The provisions under paragraph one shall apply to a Competent Official, social worker, psychologist, or a person having duty to protect the Child's welfare under section 24, who has come into possession of such information during his or her performance of duty mutatis mutandis. No person shall advertise or disseminate by means of mass media or any other form of information technology the disclosed information in violation of the provisions under paragraph one or paragraph two.
43	The National Health Act B.E. 2550 (2007)		
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the		

	Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		Section 4: The company will classify personal data that is collected, used, or disclosed in accordance with the law. Personal data protection is defined as follows: (1) General personal information such as first and last name, address, position, telephone, fax and email, etc. (2) Sensitive personal information such as race, ethnicity, political opinions creed Religion or philosophy, sexual behavior Criminal history, health information, disability, union information genetic information, biological information, or any other information which affects customers Similarly, according to the Protection Committee Personal information announced In addition to categorizing data storage according to (1) and (2), in the case of processing data that There is a high risk that will affect the rights and freedoms of customers as required by the Personal Data Protection Act. The company must arrange for an impact assessment on personal data protection.

49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)		
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

Rights of the Data Subject

#	Regulation	Right to be informed	Right of access
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019		30 The data subject is entitled to request access to and obtain a copy of the Personal Data related to him or her, which is under the responsibility of the Data Controller, or to request the disclosure of the acquisition of the Personal Data obtained without his or her consent.
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for		

	preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for		

	collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)	7 The owner of personal data has the right to know what information the government agency under paragraph one stores about him and have the right to request that government agency to correct and up-to-date information ... 8 The owner of personal data has the right to know what data the local government organization under paragraph one collects about himself and have the right to request that	

		local government organization to correct and up-to-date information... 9 The owner of personal data has the right to know what information does the Cabinet Secretariat keep about itself and have the right to request The Cabinet Secretariat to correct the information to be correct and up-to-date...	
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under		

	Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)	Section 27. In the case where signature creation data can be used to create an electronic signature that has legal effect, each signatory shall: (1) exercise reasonable care to avoid unauthorised use of his signature creation data; (2) without delay, notify any person that may reasonably be expected to act on the basis of the electronic signature or to provide services in support of the electronic signature when: (a) the signatory knows or should have known that the	

		signature creation data has been lost, damaged, compromised, unduly disclosed or known in a manner inconsistent with their purpose (b) the signatory knows from the circumstances that there occurs a substantial risk that the signature creation data may have been been lost, damaged, compromised, unduly disclosed or known in a manner inconsistent with their purpose; (3) in the case where a certificate is issued to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are specified in the certificate.	
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and		

	the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act		

	(No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)		Section 12: Service users have the right to: Take action within the time period in accordance with criteria (1) request to inspect, request access to, or request a certified true copy of personal information about him or her; (2) request to correct or change the personal information of service users to be correct. complete and current (3) Request to suspend the use or disclosure of the service user's personal information. (4) Revoke consent to collect, use, or disclose the service user's persona information. no matter what time ...(continue)...
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications	11. Rights of service users Service users have rights according to the NBTC announcement and the Personal Data Protection Act. etc. As follow (1) Right to receive notification of information (2) Right to withdraw consent (3) Right to access personal information/request a copy (4) The right to request disclosure of the acquisition of personal data that has not been given consent (5) The right to amend the personal data. 1correct1correct (6) The right to delete personal data ...(continue)...	11. Rights of service users Service users have rights according to the NBTC announcement and the Personal Data Protection Act. etc. As follow (1) Right to receive notification of information (2) Right to withdraw consent (3) Right to access personal information/request a copy (4) The right to request disclosure of the acquisition of personal data that has not been given consent (5) The right to amend the personal data. 1correct1correct (6) The right to delete personal data ...(continue)...
35	The Royal Decree on Measures for Protection and Suppression of		

	Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)	Section 25 For the purposes of protection and fairness for an information subject, the information subject shall have the following rights: (1) The right to know which of his information is kept by the credit information company; (2) The right to examine his information; (3) The right to correct incorrect information; (4) The right to protest when learning that his information is incorrect; (5) The right to be notified of the result of examination of his information within the period prescribed; (6) *(reapealed by The Credit Information Business Operation Act No.6 B.E. 2565 (2022)* (7) The right to lodge an appeal to the Committee under Section 27. The information subject may pay a fee for an examination of information as prescribed in the notification of the Committee, provided that it shall not exceed two hundred baht. Section 28 In case the financial institution, member, or service user rejects credit granting or takes any other proceeding that causes an increase of service charge to a customer by reason of learning the information of the said customer, the financial institution, member or service user must state the reasons for its rejection of credit granting or increase of service charge, including the source of information, to the said customer in writing. The	Section 25 For the purposes of protection and fairness for an information subject, the information subject shall have the following rights: (1) The right to know which of his information is kept by the credit information company; (2) The right to examine his information; (3) The right to correct incorrect information; (4) The right to protest when learning that his information is incorrect; (5) The right to be notified of the result of examination of his information within the period prescribed; (6) (reapealed by The Credit Information Business Operation Act No.6 B.E. 2565 (2022) (7) The right to lodge an appeal to the Committee under Section 27. The information subject may pay a fee for an examination of information as prescribed in the notification of the Committee, provided that it shall not exceed two hundred baht. Section 28 In case the financial institution, member, or service user rejects credit granting or takes any other proceeding that causes an increase of service charge to a customer by reason of learning the information of the said customer, the financial institution, member or service user must state the reasons for its rejection of credit granting or increase of service charge, including the source of information, to the said customer in writing. The customer who is the information subject shall then have the right to check the

		customer who is the information subject shall then have the right to check the accuracy of the said information without paying a fee, provided he exercises the said right within thirty days from the date of receipt of the rejection of credit application or the date of taking of such other proceeding.	accuracy of the said information without paying a fee, provided he exercises the said right within thirty days from the date of receipt of the rejection of credit application or the date of taking of such other proceeding.
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)	Section 25 ...(shorten)... (6) The right to know the reason of rejection of credit or service application from the financial institution or rejection of service provision from the member in the category of credit intermediaries in the case where the financial institution or the member in the category of credit intermediaries has used the information of the credit information company as grounds to reject the credit or service application;	
42	The Child Protection Act B.E. 2546 (2003)		

43	The National Health Act B.E. 2550 (2007)	Section11 An individual or a group of people has the right to request for an assessment and participating in the assessment of health impact resulting from a public policy. An individual or a group of people shall have the right to acquire information, explanation and underlying reasons from sate agency prior to a permision or performance of a program or activity which may affect his or her health or the health of acmmunity, and shall have the right to express his or her opinion on such matter.	
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of		

	Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)		
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation	Right to rectification	Right to erasure
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019		33 The data subject shall have the right to request the Data Controller to erase or destroy the Personal Data, or anonymize the Personal Data to become the anonymous data which can not

			identify the data subject, where the following ground applies:
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection		

	Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from		

	the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)	7 The owner of personal data has the right to know what information the government agency under paragraph one stores about him and have the right to request that government agency to correct and up-to-date information ... 8 The owner of personal data has the right to know what data the local government organization under paragraph one collects about himself and have the right to request that local government organization to correct and up-to-date information... 9 The owner of personal data has the right to know what information does the Cabinet Secretariat keep about itself and have the right to request The Cabinet Secretariat to correct the information to be correct and up-to-date...	
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re:		

	Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the		

	Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)		
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)	"Section 17/1. In the case where an input error is made by a natural person and sent through an automated electronic message system of another party and such automated electronic message system does not provide the person with a channel for correcting the resulting error, such person or the representing party has the right to withdraw the portion of the declaration of an intention in which the input error occurred if: (1) such person or the representing party forthwith notifies the other party of the error after having learned of such error and satisfies that the error has been made through the automated electronic message system; and (2) such person or the representing party has not materially used or received any benefit from the goods or services or any other thing from the other party."	
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)	20. (1) Where a person makes an input error in an electronic communication exchanged with the automated message system of another party and the	

		automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has the right to withdraw the portion of the electronic communication in which the input error was made.	
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		Section 5 Service providers according to Item 4 who prove that they have prepared the following measures: to notify and suspending the dissemination or removal of such computer data from the computer system will not be punished according to Section 15 (of the COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560) ...(shorten)... (2) Notification of service users In the event that the service user detects that The service provider distributes computer data

			illegally. According to Section 14, the user may notify the service provider to request that the dissemination be stopped or the computer data deleted. that is illegal by the following methods: ...(shorten)... (4) Argument Owner of computer data that has been suppressed from dissemination Such suspension may be contested. to the service provider to request that the suspension of the dissemination of computer data be canceled by the following methods: : (a) make a daily record or report a complaint as evidence to the investigating officer or police officers By notifying details related to computer data that have been suspended for distribution according to Section 14, details of service providers. Details of the damage caused to oneself along with submitting documentary evidence demonstrating ownership and legality of the computer data. along with other evidence documents ...(continue)...
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining		

	computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	Section 12: Service users have the right to: Take action within the time period in accordance with criteria (1) request to inspect, request access to, or request a certified true copy of personal information about him or her; (2) request to correct or change the personal information of service users to be correct. complete and current (3) Request to suspend the use or disclosure of the service user's personal information. (4) Revoke consent to collect, use, or disclose the service user's persona information. no matter what time ...(continue)...	
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications	11. Rights of service users Service users have rights according to the NBTC announcement and the Personal Data Protection Act. etc. As follow (1) Right to receive notification of information (2) Right to withdraw consent (3) Right to access personal information/request a copy (4) The right to request disclosure of the acquisition of personal data that has not been given consent	11. Rights of service users Service users have rights according to the NBTC announcement and the Personal Data Protection Act. etc. As follow (1) Right to receive notification of information (2) Right to withdraw consent (3) Right to access personal information/request a copy (4) The right to request disclosure of the acquisition of personal data that has not been given consent

		(5) The right to amend the personal data. 1correct1correct (6) The right to delete personal data ...(continue)...	(5) The right to amend the personal data. 1correct1correct (6) The right to delete personal data ...(continue)...
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)	Section 25 For the purposes of protection and fairness for an information subject, the information subject shall have the following rights: (1) The right to know which of his information is kept by the credit information company; (2) The right to examine his information; (3) The right to correct incorrect information; (4) The right to protest when learning that his information is incorrect; (5) The right to be notified of the result of examination of his information within the period prescribed; (6) (reapealed by The Credit Information Business Operation Act No.6 B.E. 2565 (2022) (7) The right to lodge an appeal to the Committee under Section 27. The information subject may pay a fee for an examination of information as prescribed in the notification of the Committee, provided that it shall not exceed two hundred baht. Section 28 In case the financial institution, member, or service user rejects credit granting or takes any other proceeding that causes an increase of service charge to a customer by reason of learning the information of the said customer,	

		the financial institution, member or service user must state the reasons for its rejection of credit granting or increase of service charge, including the source of information, to the said customer in writing. The customer who is the information subject shall then have the right to check the accuracy of the said information without paying a fee, provided he exercises the said right within thirty days from the date of receipt of the rejection of credit application or the date of taking of such other proceeding.	
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)		

44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		
49	The Notification of the Office of Insurance		

	Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)		
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation	Right to restrict processing	Right to data portability
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019	34 The data subject shall have the right to request the Data Controller to restrict the use of the Personal Data, where the following applies:	31 The data subject shall have the right to receive the Personal Data concerning him or her from the Data Controller. The Data Controller shall arrange such Personal Data to be in the format which is readable or commonly used by ways of automatic tools or equipment, and can be used or disclosed by automated means. The data subject is also entitled to:
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of		

	records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		

10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are		

	Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the		

	Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)		
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		

24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer		

	data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	Section 12: Service users have the right to: Take action within the time period in accordance with criteria (1) request to inspect, request access to, or request a certified true copy of personal information about him or her; (2) request to correct or change the personal information of service users to be correct. complete and current (3) Request to suspend the use or disclosure of the service user's personal information. (4) Revoke consent to collect, use, or disclose the service user's persona information. no matter what time ...(continue)...	
34	Guideline of the National Telecommunications Commission Re: Measures to		

	Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications		
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)		
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)		

43	The National Health Act B.E. 2550 (2007)		
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		

49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)		
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation	Right to object	Right not to be subject to a decision based solely on automated processing
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019	32 The data subject has the right to object the collection, use, or disclosure of the Personal Data concerning him or her, at any time, in the following circumstances: 73 The Data subject has the right to file a complaint (to the Commitee) in the event that the Data Controller or the Data Processor, including the employees or the service providers of the Data Controller or the Data Processor violates or does not comply with this Act, or	

		notifications issued in accordance with this Act.	
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565	7 In the case where the personal data controller or personal data processor including employees or contractors of the personal data controller or personal data processor violate or not comply personal data protection laws or announcements issued in accordance with personal data protection laws, the owner of the personal data concerned has the right to complain to the expert committee by submitting a complaint by one of the following methods... 8 Complaints submitted to the office must be clear and understandable, use polite words, not be vulgar, and not be extortionate or threatening, whether directly or indirectly. and must have at least the following details and	

		documentary evidence:...	
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses		

	that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re:		

	Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the		

	Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)		
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance		

	to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of		

	Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	Section 13 Users of the service may complain about cases where their rights regarding personal data have been violated. Right to privacy or the freedom to communicate with each other by means of telecommunications. In accordance with Process for receiving and considering complaints regarding telecommunications business operations	
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications	12. Complaint 12.1 Users of the service have the right to file a complaint in the event that their rights regarding personal data have been violated. Right to privacy or the freedom to communicate with each other by means of telecommunications. This is in accordance with the NBTC announcement regarding the process for receiving and considering complaints regarding telecommunications business operations, 2016. This does not deprive users of the right to submit complaints. Attention 5 of the Office of the Teachers' Council of Thailand. If it appears that the law No. 5 is in the scope of duties and The powers of the NBTC or the NBTC Office have provisions that give 5 powers to the NBTC or the NBTC Office to issue orders to protect people1 Use 1 service But 5 is not 5 enough to equal the power of the expert committee according to The Personal Information Protection Act and the NBTC or the NBTC Office request the Commission. ...(continue)...	
35	The Royal Decree on Measures for Protection and		

	Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)	Section 25 For the purposes of protection and fairness for an information subject, the information subject shall have the following rights: (1) The right to know which of his information is kept by the credit information company; (2) The right to examine his information; (3) The right to correct incorrect information; (4) The right to protest when learning that his information is incorrect; (5) The right to be notified of the result of examination of his information within the period prescribed; (6) (reapealed by The Credit Information Business Operation Act No.6 B.E. 2565 (2022) (7) The right to lodge an appeal to the Committee under Section 27. The information subject may pay a fee for an examination of information as prescribed in the notification of the Committee, provided that it shall not exceed two hundred baht. Section 28 In case the financial institution, member, or service user rejects credit granting or takes any other proceeding that causes an increase of service charge to a customer by reason of learning the information of the said customer, the financial institution, member or service user must state the reasons for its rejection of credit granting or increase of service charge, including the source of information, to the said customer in writing. The customer who is the information subject shall	

		then have the right to check the accuracy of the said information without paying a fee, provided he exercises the said right within thirty days from the date of receipt of the rejection of credit application or the date of taking of such other proceeding.	
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)		
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re:		

	Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		

50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)	Section 8 Where there is clear evidence that an infringement of trade secrets has been committed or is imminent, the affected or imminently to be affected controller of trade secrets has the following remedies: (1) Petition the court for an interim injunction, temporarily to stop the infringement of trade secrets; and, (2) File an action in the court for a permanent injunction, permanently to stop the infringement of trade secrets and claim damages from the wrongdoer. The petition under (1) may be filed prior to the action under (2).	
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation	Right to withdraw consent	others
1	Constitution of the Kingdom of Thailand		
2	Personal Data Protection Act 2019	(6) the rights of the data subject under section 19 paragraph five, section 30 paragraph one, section 31 paragraph one, section 32 paragraph one, section 33 paragraph one, section 34 paragraph one, section 36 paragraph one, and section 73 paragraph one. **** Section19 The data subject may withdraw	36 In the case where the data subject requests the Data Controller to act in compliance with section 35, if the Data Controller does not take action regarding the request of the data subject, the Data Controller shall record such request of the data subject together with reasons, in the record as prescribed in section 39. The provisions of

		his or her consent at any time. The withdrawal of consent shall be as easy as to giving consent, unless there is a restriction of the withdrawal of consent by law, or the contract which gives benefits to the data subject. However, the withdrawal of consent shall not affect the collection, use, or disclosure of personal data that the data subject has already given consent legally under this Chapter.	section 34 paragraph two shall apply mutatis mutandis.
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		

7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers		

	are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the		

	Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data		

	relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)		
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)	"Section 17/1. In the case where an input error is made by a natural person and sent through an automated electronic message system of another party and such automated electronic message system does not provide the person with a channel forcorrecting the resulting error, such person or the representing party has the right to withdraw the portion of the declaration of an intention in which the input error occurred if: (1) such person or the representing party forthwith notifies the other party of the error after having learned of such error and satisfies that the error has been made through the automated electronic message system; and (2) such person or the representing party has not materially used or received any benefit from the goods or services or any other thing from the other party."	
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)	20. (1) Where a person makes an input error in an electronic communication exchanged with the automated message system of another party and the automated message system does not provide the person with	

		an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has the right to withdraw the portion of the electronic communication in which the input error was made.	
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and		

	Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	Section 12: Service users have the right to: Take action within the time period in accordance with criteria (1) request to inspect, request access to, or request a certified true copy of personal information about him or her; (2) request to correct or change the personal information of service users to be correct. complete and current (3) Request to suspend the use or disclosure of the service user's personal information. (4) Revoke consent to collect, use, or disclose the service user's persona information. no	

		matter what time ...(continue)...	
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications	11. Rights of service users Service users have rights according to the NBTC announcement and the Personal Data Protection Act. etc. As follow (1) Right to receive notification of information (2) Right to withdraw consent (3) Right to access personal information/request a copy (4) The right to request disclosure of the acquisition of personal data that has not been given consent (5) The right to amend the personal data. 1correct1correct (6) The right to delete personal data ...(continue)...	
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)		
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		

40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)		Section11 An individual or a group of people has the right to request for an assessment and participating in the assessment of health impact resulting from a public policy. An individual or a group of people shall have the right to acquire information, explanation and underlying reasons from sate agency prior to a permision or performance of a program or activity which may affect his or her health or the health of acmmunity, and shall have the right to express his or her opinion on such matter.
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the		

	Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		

51	Trade Secret Act B.E. 2545 (2002)		Section 9 Before taking any action under Section 8, the controller of trade secrets who is affected or imminently to be affected by the infringement of trade secrets and the other party may agree to submit the dispute concerning trade secrets to the Board for conciliation or mediation. However, such submission shall not prejudice the right of either party to resolve the dispute through arbitration or litigation in the competent court should the conciliation or mediation fail to settle the dispute. The filing of request and procedure for conciliation or mediation of the Board under paragraph one shall be governed by the rules and methods prescribed in the Ministerial Regulation.
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

Extraterritorial application

#	Regulation		
		applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction	applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019	5. This Act applies to the collection, use or disclosure of Personal Data by a Data Controller or a Data Processor that is in the Kingdom of Thailand, regardless of whether such collection, use or disclosure takes place in the Kingdom of Thailand or not. In the event that a Data Controller or a Data Processor is outside the Kingdom of Thailand,	5. This Act applies to the collection, use or disclosure of Personal Data by a Data Controller or a Data Processor that is in the Kingdom of Thailand, regardless of whether such collection, use or disclosure takes place in the Kingdom of Thailand or not. In the event that a Data Controller or a Data Processor is outside the Kingdom of Thailand,

		this Act shall apply to the collection, use or disclosure of Personal Data of data subjects who are in the Kingdom of Thailand, where the activities of such Data Controller or Data Processor are the following activities: (1) the offering of goods or services to the data subjects who are in the Kingdom of Thailand, irrespective of whether the payment is made by the data subject; or (2) the monitoring of the data subject's behavior, where the behavior takes place in the Kingdom of Thailand.	this Act shall apply to the collection, use or disclosure of Personal Data of data subjects who are in the Kingdom of Thailand, where the activities of such Data Controller or Data Processor are the following activities: (1) the offering of goods or services to the data subjects who are in the Kingdom of Thailand, irrespective of whether the payment is made by the data subject; or (2) the monitoring of the data subject's behavior, where the behavior takes place in the Kingdom of Thailand.
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the		

	Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations		

	and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
16	Notification of the Personal Data Protection		

	Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection		

	Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)		
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance		

	to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of		

	Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)		
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications		
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)		
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		

39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)		
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re:		

	Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)		
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation		
		no express territorial scope, but would require some nexus to the jurisdiction	other
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019		
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data		

	breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of		

	the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
17	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement		

	of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
20	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not		

	carried out under Control of Authorized Official Authority under the Law B.E. 2566		
21	Electronic Transactions Act, B.E. 2544 (2001)		
22	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
23	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
24	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
25	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		Section 17 Whoever commits an offence pursuant to this Act outside the Kingdom of Thailand, and (1) the offender is a Thai person and there is a request for punishment by the Government of the country where the offence has occurred or by the injured person; or (2) the offender is an alien, and the Royal Thai Government or a Thai person is the injured person, and there is a request for punishment by the injured person, shall be punished in the Kingdom of Thailand
26	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the		

	characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
30	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
31	The Special Case Investigation Act B.E. 2547 (2004)		

32	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
33	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
34	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)		
35	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications		
36	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		
37	The Credit Information Business Operation Act B.E. 2545 (2002)		
38	The Credit Information Business Operation Act		

	No.2 B.E. 2549 (2006)		
39	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
40	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
42	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
43	The Child Protection Act B.E. 2546 (2003)		
44	The National Health Act B.E. 2550 (2007)		
45	The Payment System Act B.E. 2560 (2017)		
46	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of		

	Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		
51	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
52	Trade Secret Act B.E. 2545 (2002)		

	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation	Representatives of controllers or processors not established in the country
1	Constitution of the Kingdom Of Thailand	
2	Personal Data Protection Act 2019	
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)	
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)	
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)	
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565	

7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565	
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	
9	Guideline for obtaining consent from data subjects according to the PDPA	
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA	
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562	
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers	

	are Exempted from the Applicability of the PDPA B.E. 2563 (2020)	
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)	
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)	
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)	
17	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the	

	Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other	
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	
19	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	
20	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data	

	relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566	
21	Electronic Transactions Act, B.E. 2544 (2001)	
22	Electronic Transactions Act, No.2 B.E. 2551 (2008)	
23	Electronic Transactions Act, No.3 B.E. 2562 (2019)	
24	Electronic Transactions Act, No.4 B.E. 2562 (2019)	
25	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)	
26	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)	
27	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)	

28	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)	
29	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)	
30	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)	
31	The Special Case Investigation Act B.E. 2547 (2004)	
32	The Special Case Investigation Act (No.2) B.E. 2551 (2008)	
33	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)	

34	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	
35	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications	
36	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)	
37	The Credit Information Business Operation Act B.E. 2545 (2002)	
38	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)	
39	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)	
40	The Credit Information Business	

	Operation Act No.4 B.E. 2559 (2016)	
41	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)	
42	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)	
43	The Child Protection Act B.E. 2546 (2003)	
44	The National Health Act B.E. 2550 (2007)	
45	The Payment System Act B.E. 2560 (2017)	
46	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules	
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)	
48	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-	

	life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)	
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)	
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)	
51	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)	
52	Trade Secret Act B.E. 2545 (2002)	
	Trade Secret Act (No.2) B.E. 2558 (2015)	

Notification obligation

#	Regulation		
		Data breach notification to authorities	Data breach notification to affected individuals
1	Constitution of the Kingdom of Thailand		

2	Personal Data Protection Act 2019	37 The Data Controller shall have the following duties: (4) notify the Office of any Personal Data breach without delay and, where feasible, within 72 hours after having become aware of it (Personal Data breach), unless such Personal Data breach is unlikely to result in a risk to the rights and freedoms of the Persons. If the Personal Data breach is likely to result in a high risk to the rights and freedoms of the Persons, the Data Controller shall also notify the Personal Data breach and the remedial measures to the data subject without delay. The notification and the exemption to the notification shall be made in accordance with the rules and procedures set forth by the Committee.	37 The Data Controller shall have the following duties: (4) notify the Office of any Personal Data breach without delay and, where feasible, within 72 hours after having become aware of it (Personal Data breach), unless such Personal Data breach is unlikely to result in a risk to the rights and freedoms of the Persons. If the Personal Data breach is likely to result in a high risk to the rights and freedoms of the Persons, the Data Controller shall also notify the Personal Data breach and the remedial measures to the data subject without delay. The notification and the exemption to the notification shall be made in accordance with the rules and procedures set forth by the Committee.
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		

7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E.		

	2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee		

	Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)		
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		1) Notice procedure The service provider shall carry out the reporting notification measures by preparing a written Take Down Notice, available to the public either by technical measure or any other measure, for notifying the service provider to block the dissemination or to delete unlawful computer data from the computer system which is under the control of the service provider. The said Take Down Notice of the service provider shall include,

			for the general public's knowledge, the following information: (a) name, address, telephone number or e-mail address of the service provider, or the service provider's representative; (b) Complaint Form for the user or another person to notify the service provider to block the dissemination or to delete unlawful computer data. The Complaint Form must at least comprise of the following details:
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		(1) Notice procedure The service provider shall carry out the reporting notification measures by preparing a written Take Down Notice, available to the public either by technical measure or any other measure, for notifying the service provider to block the dissemination or to delete unlawful computer data from the computer system which is under the control of the service provider. The said Take Down Notice of the service provider shall include, for the general public's knowledge, the following information: (a) name, address, telephone number or e-mail address of the service provider, or the

			service provider's representative; (b) Complaint Form for the user or another person to notify the service provider to block the dissemination or to delete unlawful computer data. The Complaint Form must at least comprise of the following details:
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	Section 14 : ...(shorten)... Violation of personal information of any service user risks affecting rights and freedoms of individuals, the license holder must inform the NBTC of the violation without delay as much as possible. Within 72 hours from knowing the cause If any violation has a high risk of affecting the rights and	Section 14 : ...(shorten)... Violation of personal information of any service user risks affecting rights and freedoms of individuals, the license holder must inform the NBTC of the violation without delay as much as possible. Within 72 hours from knowing the cause If any violation has a high risk of affecting the rights and

		freedoms of individuals Licensee The cause of the violation must be reported to the NBTC without delay as much as possible within 24 hours from knowing the cause. and must inform users of the cause of such violation along with remedies without delay as well In this regard, the NBTC may prescribe criteria for such notification and exemptions for licensees to proceed	freedoms of individuals Licensee The cause of the violation must be reported to the NBTC without delay as much as possible within 24 hours from knowing the cause. and must inform users of the cause of such violation along with remedies without delay as well In this regard, the NBTC may prescribe criteria for such notification and exemptions for licensees to proceed
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications	14. Reporting a personal data breach 14.1 The licensee has a duty to report incidents of violations of the personal information of service users to Office A. NBTC and Office of the Provincial Administrative Organization, with the important information as follows: In the case where there is no risk, there is no need to inform. In the case of normal risk. Notify the Office of the NBTC and Office of the National Broadcasting and Telecommunications Commission without delay within 72 hours from the moment you know the reason as much as possible. In cases of high risk that will have an impact on the rights and freedoms of ndividuals - notify the NBTC Office without delay within 24 hours from the moment you know the cause - Notify 5th Public Health - Notify the cause and remedies to service users ...(continue)...	
35	The Royal Decree on Measures for Protection and		

	Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)		
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)		
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		Minimum standards for operations and contingency plans 9.1 Operational system ...(shorten)... In the case of technological systems that support business operations or work systems related to Providing service to customers when there are disruptions or cannot be used normally The service provider must notify the customer quickly and must take corrective action without delay. However, if there is an emergency, It is necessary to stop providing service. Temporarily with the service provider notified in advance. The service provider must notify the operator. The Company will inform customers in advance of such

			action. in an appropriate time as well 9.2 Plan for prevention and support in case of emergencies (business contingency plan) 9.2.1 Set a response plan in the event of an emergency. The said plan should cover important work practices to ensure that they can be carried out. able to continue operating the business without affecting the operations customer transactions or will cause Damage to customers If the impact cannot be avoided There must be a method of communication to do so. to understand customers Both before the incident during the incident and after the incident appropriately 9.2.2 Test the plan to see if it can actually be implemented according to the plan. Able to control effects and damage and restore the operating system for important matters within the specified time, including reviewing and improving the work plan to be up to date and appropriate to the circumstances
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing		

	and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)	Article 11 In the case where the company is the controller of personal data The company also has other additional duties as follows: (1) Proceed to ensure that customer personal information is accurate, current, complete and does not create misunderstanding ...(shorten)... **(5) Report the incident of personal data violation to the Office of the Personal Data Protection Commission and Office according to the criteria and time period specified by the law on personal data protection.** ...(continue)... Article 22 In the case where a life insurance agent is the controller of personal data, he or she has the following duties: ...(shorten)... (12) Report the incident of personal data violation to the Office of the Personal Data Protection Commission. and the office in accordance with the criteria and time period specified by the law on personal data protection. ...(continue)... Article 32 In the case where the life insurance broker is the controller of personal information Life insurance brokers also have other additional duties according to the Personal Data Protection Act, as follows:	

		(1) Proceed to ensure that customer personal information is correct, current, complete and does not cause damage. misunderstand ...(shorten)... (5) Report the incident of personal data violation to the Office of the Personal Data Protection Commission and Office according to the criteria and time period specified by the law on personal data protection. ...(continue)... Article 33 In the case where a life insurance broker is a processor of personal data Has the following duties (1) proceed with collection and use or disclose personal information according to the order received from Only personal data controllers Unless the order of the Personal Data Controller is contrary to the law. ...(shorten)... (3) Notify the Personal Data Controller of the incident of personal data violation as required by law. Regarding the protection of personal information ...(continue)...	
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)	Article 11 In the case where the company is the controller of personal data The company also has other additional duties as follows: (1) Proceed to ensure that customer personal information is accurate, current, complete and does not cause any harm. misunderstand ...(shorten)... (5) Report the incident of personal data violation to the Office of the Personal Data Protection Commission and	

		Office according to the criteria and time period specified by the law on personal data protection. ...(continue)... Article 21 In the case where a non-life insurance agent is a processor of personal data, the non-life insurance agent also has other additional duties in accordance with the law on personal data protection, as follows: (1) proceed with collection and use or disclose personal information according to the order received from Company only Unless the company's order is against the law. (2) provide for the security of personal information; To prevent loss, access, use Change, edit, or disclose personal information without authority or wrongfully. In accordance with the law Regarding the protection of personal information (3) Notify the company of the incident of personal data violation according to the law on protection. Personal information required ...(continue)... Article 22 In the case where the general insurance agent is the controller of personal information, he or she has the following duties: (1) A non-life insurance agent must collect, use or disclose personal information according to the purpose. that have been informed to customers before or while collecting personal information If a non-life insurance agent finds or knows that there is The purpose of collecting, using, or	

		disclosing personal information is in addition to the original purpose. This is in addition to what is specified in the personal data protection policy of the insurance agent itself or in the case where there is a change in the purpose of collecting, using or disclosing personal data. General insurance agent You can add or change the purposes for collecting, using, or disclosing personal information. ...(shorten)... (12) Report the incident of personal data violation to the Office of the Personal Data Protection Commission. and the office in accordance with the criteria and time period specified by the law on personal data protection. ...(continue)... Article 32 In the case where the general insurance broker is the controller of personal information. General insurance broker There are also other additional duties according to the law on personal data protection as follows: (1) Proceed to ensure that customer personal information is correct, current, complete and does not cause damage. misunderstand ...(shorten)... (5) Report the incident of personal data violation to the Office of the Personal Data Protection Commission and Office according to the criteria and time period specified by the law on personal data protection. ...(continue)... Article 33 In the case where a	

		general insurance broker is a processor of personal data. Has the following duties (1) proceed with collection and use or disclose personal information according to the order received from Only personal data controllers Unless the order of the Personal Data Controller is contrary to the law. (2) provide for the security of personal information; To prevent loss, access, use, change, modification, or disclosure of personal information without authority or wrongdoing. In accordance with the law Regarding the protection of personal information (3) Notify the Personal Data Controller of the incident of personal data violation as specified by law. With the protection of personal information specified ...(continue)...	
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)	Article 11 The casualty assessor who has the status of a personal data controller has other additional duties. as follows (1) Proceed to ensure that the insured's personal information is correct, current, complete, and does not cause misunderstanding ...(shorten)... **(5) Report the incident of personal data violation to the Office of the Personal Data Protection Commission and Office according to the criteria and time period specified by the law on personal data protection.** ...(continue)... Article 12 In the case where the casualty assessor is the person processing personal	

		data Has the following duties (1) proceed with collection and use or disclose personal information according to the order received from Only personal data controllers Unless the order of the Personal Data Controller is contrary to the law. (2) provide for the security of personal information; To prevent loss, access, use, change, modification, or disclosure of personal information without authority or wrongdoing. In accordance with the law Regarding the protection of personal information (3) Notify the Personal Data Controller of the incident of personal data violation as required by law. Regarding the protection of personal information ...(continue)..	
51	Trade Secret Act B.E. 2545 (2002)		
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

Obligations of Data Fiduciaries

#	Regulation	external	external
		Notification of data processing	registration of database
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019	19 The Data Controller shall not collect, use, or disclose Personal Data, unless the data subject has given consent prior to or at the time of such collection, use, or disclosure, except the case where it is permitted to do so by the provisions of this Act or any other laws. .... 20 In the event that the data subject is a minor who is not sui juris by marriage or has no capacity as a sui juris person	

		under Section 27 of the Civil and Commercial Code, the request for the consent from such data subject shall be made as follows: .... 23 In collecting the Personal Data, the Data Controller shall inform the data subject, prior to or at the time of such collection, of the following details, except the case where the data subject already knows of such details: ... 24 The Data Controller shall not collect Personal Data without the consent of the data subject, unless: ... 27 The Data Controller shall not use or disclose Personal Data without the consent of the data subject, unless it is the Personal Data which is collected without requirement of consent under Section 24 or Section 26. ...	
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		

6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565	4 Events of personal data violations that the Personal Data Controller has a duty to notify the Office of the Personal Data Protection Committee or owners of personal data according to the law on personal data protection include: Causes arising from violations of security measures that result in loss, access, use, change, modification, or disclosure of personal information without authorization or illegally whether caused by intention, willfulness, negligence, acting without authority or wrongdoing; computer offenses; cyber threats error; defect or accident or any other reason which may be caused by actions the personal information controller's own information or personal data processor that deals with the collection, use, or disclosure of personal information in accordance with on behalf of or on behalf of the controller as well as employees, employees, contractors, agents, or related persons of the controller Personal data or the processor of such personal data or another person or other factors. Each personal data breach incident may involve a specific type of violation or many types as follows:... 6 In reporting personal data	

		violations to the Office of the Personal Data Protection Committee, the Personal Data Controller must report the personal data violations in writing. or notify through the method electronically or any other means as specified by the Office in reporting data breach events. Personal information must be specified. The following important information shall be provided as far as possible:.. 9 The personal data controller may waive the exemption from reporting personal data violation events to the Office for consideration... 10 When there is an incident of personal data violation and the Personal Data Controller has notified the inceident or has already been filed with the office or is in the process of preparing to notify the office, if the personal data controller inspected the facts and found that such personal data breaches carry a high risk of adverse effects. to the rights and freedoms of individuals, the Personal Data Controller shall report the incident of personal data violation with the following important information to the affected personal data owner as far as possible:... 11 In reporting the incident of a personal data breach to the owner of the affected personal data, if in nature it is not possible to do so Notification must be done individually, in writing or by other means electronically because there is no contact method or due to any other necessity, the Personal Data Controller may notify Incident of violation for the owner of	

		personal data as a group or notify in general through public media, social media, online, or by electronic means or any other means...	
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA	2 Type and manner of notifying the purpose and details of data collection Notification of the purpose and details of collecting, using, and disclosing personal information are divided into 2 types: 2.1 In cases where there is a specific law or a control and supervision agency including setting criteria. ... 2.2 In the case where there is no specific law or control and supervision agency, including specific criteria, methods, or guidelines for operations in informing the purpose and details of personal data collection in cases where there is no specific law or specific agency to supervise, the personal data controller should and proceed according to this guidelines. 3. Principles for notifying the purpose and details to the owner of personal data	

		The personal data controller must notify the purpose and details of data collection. personal information to the owner of personal information before or while collecting personal information by informing the objective Such information must be subject to the following: 3.1 Fairness ... 3.2 Limiting the purposes for collecting, using, and disclosing personal information (Purpose Limitation) ... 3.3 Consent ... 3.4 Claim of Legitimate Interest ... 4. Types of personal data collection Collection can be used or disclosed in 2 methods: 4.1 Collection of personal data directly from the owner of personal data Data Controllermust notify the owner of personal data before or while collecting personal data with details as follows unless the owner of personal data is already aware of the details: ... 4.2 Collection of personal data from other sources that are not the data owner. Collection of personal data from other sources that are not the data owner cannot be done according to Section 25 of the Personal Data Protection Act B.E. 2019, except in the following cases: ... 5. Exceptions to notification of the purpose and details of collecting personal information for collecting personal data from sources other than the direct	

		owner of the personal data For the collection of personal data from sources other than the direct owner of the personal data, according to Section 25, the Personal Data Controller may not have to inform the owner of the personal data of the new purpose for collecting personal data in accordance with Section 21 and inform the purpose and details of the collection according to Section 23 as specified in 4.2, when requesting consent from the data owner in the following cases: 5.1 The owner of personal data already knows the new purpose or details. ... 5.2 The Personal Data Controller can prove that notification of the new purpose or details is not possible or will hinder use or disclosure... 5.3 Use or disclosure of information for such personal information must be done urgently as required by law specified, which has provided appropriate measures to protect the interests of the owners of personal data. 5.4 When the Personal Data Controller is a person who knows or obtains personal data from his duties or from the occupation or profession and must keep the new objectives or certain details under Section 23 secret as required by law. ... 6. Notification of the purpose and details of personal data collection to the owner must be made clearly, which may be done in many ways, such as notification in writing, verbal notification, notification via message in the form of SMS, email, MMS or by telephone or by other electronic means, such as	

		specifying details in a URL or QR code, etc ...	
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		

15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal		

	Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)	Section 19. In the case where an acknowledgement of receipt of a data message is required, whether at the originator's request or as agreed with the addressee before or at the time of sending the data message or by means of that data message, the following rules shall apply: (1) in the case where it has not been agreed by the originator that the acknowledgement be given in a particular form or by a particular method, the acknowledgement may be given by any communication by the addressee, whether by an automated information system or by any other method, or by any conduct of the addressee sufficient to indicate to the originator that the addressee has	

		received the data message; (2) in the case where the originator has stated a condition that the data message shall be regarded as having been sent only upon receipt of an acknowledgement by the addressee, it shall be deemed that the data message has never been sent until the originator has received the acknowledgement; (3) in the case where the originator has not stated such a condition under (2) and the originator has not received the acknowledgement within the specified or agreed time, or, if no time has been specified or agreed, within a reasonable time, then: (a) the originator may give notice to the addressee stating that the originator has not received the acknowledgement and specifying a reasonable time by which the acknowledgement must be made by the addressee; and (b) if the originator has not received the acknowledgement within the time under (a), the originator may, upon notice having been given to the addressee, treat the data message as having never been sent, or the originator may exercise any other rights he may have. (b) if the originator has not received the acknowledgement within the time under (a), the originator may, upon notice having been given to the addressee, treat the data message as having never been sent, or the originator may exercise any other rights he may have.	
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		

22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital		

	Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	Section 10 10 The licensee must collect personal data of service users directly from service users as necessary and in accordance with legitimate purposes. You must inform the service user first. or while doing that work, unless (1) The service user has given consent for the licensee to do so. collecting their personal information From other sources, whereby the licensee must notify service users of the collection of personal data from other sources know without delay But must not exceed 30 days from	

		the date of collection. and must comply with the criteria as required by the law on personal data protection (2) It is a collection of personal data of service users who are exempt from requesting consent According to Section 6 and Section7 The licensee must provide a channel for service users to update their personal information. Can be current It has a strong verification and identification system. Section 18 The licensee must provide telecommunications number user information to the person requesting to create it List of service users according to Section 12, paragraph five of the Telecommunications Business Act B.E. 2001, which has received consent from service users. The expenses can be calculated only for the expenses Provide information only Section 21 The license holder must inform details and details. to specify measures for the person who prepares the list Service users and persons assigned by the licensee to do so responsible for collecting, using, disclosing, and preserving Personal information of service users Follow the criteria set forth as specified in this announcement and the law on protection Personal information, as the case may be, strictly If the person assigned by the licensee to do responsible for collecting, using, disclosing, and preserving Personal information of service users Intentionally do not comply with this announcement. The license holder must control and supervise the person. Such	

		action is suspended. violating or amending or complying with the law to be correct and appropriate and licensee Must be bound to perform any action by such person as if the license holder were the one performing the action. to proceed on your own	
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications		
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)	Section 28 In case the financial institution, member, or service user rejects credit granting or takes any other proceeding that causes an increase of service charge to a customer by reason of learning the information of the said customer, the financial institution, member or service user must state the reasons for its rejection of credit granting or increase of service charge, including the source of information, to the said customer in writing. ...(continue)...	
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)	Section 18 For the purpose of controlling and processing information by a credit information company, a member shall send the information of its customers to the credit information company of which it is a member, and shall notify its	

		customers in writing of the information sent, or notify them by other method agreed upon, within thirty days from the date of sending the information to the credit information company. If the member is unable to do so within the said timeframe, it may apply for an extension of time to the Committee for not more than fifteen days, in accordance with the rules, procedures and conditions prescribed by the Committee. In sending to the credit information company additional information in respect of history of credit payment and history of payment for goods or services by credit card, the member shall notify its customers of the same in accordance with the rules, procedures, conditions and period prescribed by the Committee.	
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)		

43	The National Health Act B.E. 2550 (2007)		
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		

49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)		
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation	external	external
		Data protection impact assessment	Others
1	Constitution of the Kingdom of Thailand		
2	Personal Data Protection Act 2019		
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		

5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565	5 When the Personal Data Controller receives initial information from anyone whether verbally, in writing, or by other electronic means or the personal data controller knows himself that there is or should be cause of personal data breach, the personal data controller must take the following actions: (1) Evaluate the reliability of such information. and investigate the facts.... (2) if during the investigation regarding the violation of personal data according to (1), it is found that there is a high risk that it will have an impact individual rights and freedoms, the personal data controller shall take action himself or order the personal data processor or related person to take action to prevent, stop, or correct so that the personal data violation ends.... (3) After considering the facts under (1), it is considered that there are reasonable grounds to believe that there has been a breach, the Personal Data	

		Controller shall report the violation incident to the Office of the Personal Data Protection Commission .... (4) In the case where the violation of personal data has a high risk of affecting rights. and individual freedom, the Personal Data Controller shall notify the Personal Data Owner of the violation. Along with guidelines for remedies without delay. (5) Carry out the necessary measures to stop, respond, correct, or recover... 12 In risk assessment for for personal data breaches that there is a risk of How much does it affects the rights and freedoms of individuals, the Personal Data Controller may consider the following factors:...	
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		

11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re:		

	Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of		

	Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)		
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		Section 16. The provisions of section 22, section 23, section 24 and section 25 of the Commission of Computer-Related Offences Act, B.E. 2550 (2007) shall be repealed and replaced by the following:

			"Section 22. The competent official and the inquiry official in the case under section 18 paragraph two shall not disclose or hand over computer data, computer traffic data or users' data acquired under section 18 to any person. The provisions of paragraph one shall not apply to any act performed for the purpose of taking legal proceedings against offenders under this Act or offenders under other laws in the case under section 18 paragraph two or for the purpose of taking legal proceedings against the competent official in connection with the unlawful exercise of powers or against the inquiry official insofar as it is concerned with the unlawful performance of duties under section 18 paragraph two or any act done as ordered or permitted by the Court. Any competent official or inquiry official who violates paragraph one shall be liable to imprisonment for a term not exceeding three years or to a fine not exceeding sixty thousand Baht or to both. Section 23. Any competent official or inquiry official in the case under section 18 paragraph two who does any negligent act causing another person to know computer data, computer traffic data or users' data acquired under section 18 shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding twenty thousand Baht or to both. Section 24. Any person who knows computer data, computer traffic data or users'

			data acquired by the competent official or the inquiry official under section 18 and discloses such data to any person shall be liable to imprisonment for a term not exceeding two years or to a fine not exceeding forty thousand Baht or to both. Section 25. Data, computer data or computer traffic data acquired by the competent official under this Act or acquired by the inquiry official under section 18 paragraph two shall be admissible into evidence in accordance with the provisions of the Criminal Procedure Code or other laws on evidence taking, provided that they have not occurred in consequence of any inducement, promise, threat or deceit or any other unlawful means."
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and		

	removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and		Section 6. The licensee will collect, use or disclose personal information of service users as much as necessary for operations to operate telecommunications business according to the telecommunications service contract entered into with service users

	Freedom of Communications B.E.2566 (2023)		Users may give consent for the licensee to use or disclose their personal information. For purposes other than business operations carrying out telecommunications business according to paragraph one before or while doing so Consent under paragraph two must be separated from the contract or conditions for providing telecommunications services. ...(continue)... Section 7. The licensee must not collect personal information of service users regarding race, ethnicity, political opinions. creed Religion or philosophy sexual behavior Criminal history, health information, disability, union information Genetic data, biological data, or any other data that affects the owner of personal data in the process in the same manner as the law on protection Personal information is specified without the express consent of the user, which must be for the benefit To provide appropriate services according to physical disabilities Section 8: Collection, use, or disclosure of personal information of service users in the following cases: There is no need to follow the criteria in items 6 and 7. (1) Send personal data of service users to the NBTC or NBTC Office according to item 19. (2) In the case of exemption according to the law on personal data protection
34	Guideline of the National Telecommunications Commission Re: Measures to Protect		

	Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications		
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)		
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		Section 24 Subject to Section 20, Section 24/1 and Section 24/2, the following persons shall be prohibited from disclosing the information: (1) A credit information company, information controller, information processor, member or service user; (2) A person who knows the

			information from working or carrying out duties in (1); (3) A person who knows the information from a person under (1) or (2).
42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)		
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of		

	Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)		
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation	internal	internal
		technical and organisational measures	Purpose Limitation
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019	37 The Data Controller shall have the following duties: (1) provide appropriate security measures for preventing the unauthorized or unlawful loss,...; (2) in the circumstance where the Personal Data is to be provided to other Persons or legal persons, apart from the Data Controller, the Data Controller shall take action to	

		prevent such person from using or disclosing such Personal Data unlawfully or without authorization; (3) put in place the examination system ... (4) notify the Office of any Personal Data breach ... (5) in the event of being the Data Controller pursuant to Section 5 paragraph two, the Data Controller shall designate in writing a representative of the Data Controller who must be in the Kingdom of Thailand and be authorized to act on behalf of the Data Controller without any limitation of liability with respect to the collection, use or disclosure of the Personal Data according to the purposes of the Data Controller. 40 The Personal Data Processor shall have the following duties: (1) carry out the activities related to the collection, use or disclosure of Personal Data only pursuant to the instruction given by the Data Controller, except ... (2) provide appropriate security measures ...; and (3) prepare and maintain records of personal data processing activities...	
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)	4 The Personal Data Controller has a duty to provide appropriate security measures to prevent loss, access, use, change, modification, or disclosure of personal data without authority or wrongdoing. By the said security measures At least there must be the following actions: ... 5 The Personal Data Controller must review the security measures according to Article 4 when necessary or when technology changes in order to be effective in maintaining security appropriate safety,	

		taking into account the level of risk based on technological factors, context, environment, and accepted standards for for agencies or businesses of the same or similar type or nature Nature and purpose of collecting, using and disclosing personal information resources required and the possibility of doing so and proceed with assembly... 6 In establishing an agreement between the personal data controller and the data processor, the personal data controller consider the requires personal data processors to provide appropriate security measures to prevent loss, access, use, change, modification, or disclosure of personal information without authorization... 7 In the case where the Personal Data Controller has duties under other laws to provide measures to maintain appropriate security, to prevent loss, access, use, change, modification, or reveal personal information without authorization, let the Personal Data Controller take action according to that law but the said security measures of the personal data controller Must also meet the minimum standards specified in this announcement.	
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		

5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data		

	from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		

15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	4. The Personal Data Controller has a duty to ensure the security of Appropriate personal information To prevent loss, access, use, change, modification, or disclosure of personal information without authority or illegally. There must be security measures in place. that complies with the following standards: (1) Measures to maintain such security must cover collection and use and disclose personal information... (2) Measures to maintain such security must include organizational measures. appropriate organizational measures and technical measures... (3) Measures to maintain such security must consider operations regarding Security From identifying important risks ... (4) Measures to maintain such security muxt have ability to maintain confidentiality, integrity, and availability... (5) For collecting, using, and disclosing personal information in electronic form, such security measures must cover the various components of the information system related to the collection, use, and disclosure of personal information... (6) Measures to maintain such security with respect to accessing, using, changing, correcting, deleting or disclosing personal information must include at least an action below according to the risk level.... (7) Measures to maintain such security must include raising awareness on the importance of personal data protection and security (privacy and security awareness) and notification...	

		(8) Measures to maintain such security should include measures to make personal data information be unable to identify the owner... 5. The Personal Data Controller must review security measures according to Article 4 when necessary or when technology changes... 6. In the case where the Personal Data Controller has a personal data processor or person or other juristic persons who are not the controllers of personal data which involves collecting, using, or disclosing personal data according to the order or on behalf of the personal data controller...must consider requiring personal data processors or individuals or juristic persons to provide measures to maintain appropriate security of personal information ... 7. In the case where the Personal Data Controller has duties under other laws to provide measures to maintain appropriate security to prevent loss, access, use, change, modification, or disclosure of personal information without authority or illegally, let the Personal Data Controller take action. according to that law...	
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or	4. In collecting personal data without the consent of the owner of the personal data to achieve the objectives related to research studies or statistics according to Section 24 (1) of the Personal Data Protection Act 2019, the Personal Data Controller must provide appropriate protection measures to protect the rights and freedoms of personal data	

	Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other	owners as follows: (1) The Personal Data Controller must provide organizational measures. appropriate organizational measures and technical measures, which may include necessary physical measures.... (2) The Personal Data Controller must provide appropriate security measures for risks to individual rights and freedoms which must meet the minimum standards set by the Personal Data Protection Committee... (3) The Personal Data Controller must provide appropriate measures to control and supervise the collection of personal data to achieve the objectives related to such research studies or statistics in compliance with relevant ethical standards without violating the law... 5. In collecting personal information regarding race, ethnicity, political opinions, creed, religion or philosophy, sexual behavior, criminal history, health information, disability, union information, genetic information, biological information, or any other information that affects the data owner in the same manner as specified in the announcement of the Personal Data Protection Committee without the express consent of the owner of personal data that is necessary to comply with the law in order to achieve objectives regarding scientific research studies. history or statistics or other public benefits according to Section 26 (5) (d) of the Personal Data Protection Act B.E. 2019, the Personal Data Controller must provide appropriate measures to protect basic rights and interests of the	

		owner of personal data as follows: (1) The Personal Data Controller must consider the reasons for necessity and consider that collection of personal data to achieve purposes related to scientific research studies history or statistics or other such public benefits is a case where it is necessary as provided by law, necessary for the performance of duties in carrying out missions in the public interest... (2) The Personal Data Controller must provide organizational measures and technical measures, which may include necessary physical measures to control the collection of such personal data to the extent necessary for purposes related to scientific research, history or statistics or other public benefits taking into account relevant academic principles, including... (3) The personal data controller must provide appropriate security measures with risks to individual rights and freedoms which must meet the minimum standards set by the Personal Data Protection Committee... (4) The Personal Data Controller must provide appropriate measures to control and supervise the collection of personal data to achieve purposes related to scientific research studies, history or statistics are in accordance with relevant and accepted ethical standards and do not violate the law...Such relevant and accepted ethical standards shall include the contents of the following documents: (a) The Belmont Report:... (b) Good Clinical Practice (GCP) by... (c) International Ethical Guidelines for Health-related	

		Research Involving Humans by ... . 6. Subject to Articles 4 and 5 in collecting personal data to achieve objectives related to research studies or statistics according to section 24(1) or to achieve the objectives about scientific research history or statistics according to Section 26 (5) (Ngor) of the Personal Data Protection Act B.E. 2019, the Personal Data Controller shall also provide the following measures: (1) Even though the collection, use, or disclosure of personal data to achieve the said purpose will be exempt from requesting consent from the owner of personal data but the personal data controller must supervise those who carry out research or statistics studies under section 24 (1) or those who carry out scientific research study history or statistics according to section 26 (5) (d) to request consent for participation in the research study (informed consent for research participation) from the participants Research subject (research subject) unless it is one of the following cases: ... (2) In collecting personal data to achieve objectives related to research studies or statistics according to section 24 (1) or to achieve objectives related to scientific research studies history or statistics according to section 26 (5) (d) directly from the owner of personal data, the Data Controller must inform the owner of such personal data about the purpose of the research, study brief details, personal information to be collected in research studies... (3) In collecting Personal data to	

		achieve research studies...in which exercising the right to request access or obtain a copy of personal data related to the owner of personal data who is a research study participant may cause the reseach not be achieved, for example,..., the Personal Data Controller must supervise the processor in the research study to inform the owners of personal data who are research study participants about the limitations of request access to or obtain a copy of such personal information... 7. In the case where the Personal Data Controller has duties under other laws related to research studies or statistics according to section 24 (1) or scientific research studies history or statistics or other public benefits according to Section 26 (5) (d), the Personal Data Controller shall proceed according to that law. But measures are taken to protect the rights, freedoms, and interests of the owners of personal data who are participants of the research study or statistics or scientific research study history or statistics or public interest must also be complied to the Notification	
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		

18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566	5. The Personal Data Controller will collect personal information regarding criminal history only when there is a provision of law that requires a criminal history check or inspection, qualifications or prohibited characteristics related to committing a criminal offense or receiving a criminal penalty or having received the express consent of the owner of personal data only. For cases where it is for the following purposes: (1) Consideration of accepting persons to work. or qualification verification prohibited characteristics or consider the suitability of the person to hold any position. (2) Inspection of qualifications or prohibited characteristics of persons in granting permission, issuing licenses, approving, registering, ... or provide other services to individuals by government agencies or designated personal data controllers to perform duties in exercising authority on behalf of government agencies. (3) Inspection of qualifications or prohibited characteristics of persons in permitting, approving, certifying, ... or provide other services to individuals by the person controlling personal data other than what is specified in	

		(2). 7. The Personal Data Controller must provide appropriate organizational measures and technical measures, which may include necessary physical measures to control the collection, use, and disclosure of personal data according to this announcement to the extent necessary under the legitimate purposes of the personal data controller. 8. In collecting personal information according to this Notification, he personal data controller must provide security measures appropriate to the risks to individual rights and freedoms which must be in accordance with the minimum standards announced by the Personal Data Protection Board in accordance with Section 37 (1).	
20	Electronic Transactions Act, B.E. 2544 (2001)	Section 29. In determining the trustworthiness of systems, procedures and human resources under section 28 (6), regard may be had to the following factors: (1) financial status, human resources and existing assets; (2) quality of hardware and software systems; (3) procedures for issuing certificates, applications for certificates and retention of records in relation to the provision of the service; ...(continue)... Section 30. A relying party shall: (1) take reasonable steps to verify the reliability of an electronic signature; (2) in the case where an electronic signature is supported by a certificate, take reasonable steps to:	

		(a) verify the validity, suspension or revocation of the certificate; and (b) observe any limitation with respect to the certificate.	
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation		

	of computer information and removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)	Section 8: Service providers must provide a digital identity verification and verification system for for all service users using technology that complies with minimum conditions and standards Leading in the level of reliability and electronic media used to confirm identity as specified in The Electronic Transactions Development Agency stipulates in Section 3/1 regarding the digital identity verification system of the Electronic Transactions Act B.E. 2001 or according to other criteria that have standards that are consistent with and not lower than those. Specified in this announcement or as specified The Minister of Digital Economy and Society announce lin order to protect the reliability of the information system to be accurate and not be altered, as well as to protect the personal information of service users. Service providers must provide security measures. Data security in the authentication and verification system should cover	

		administrative safeguards, technical safeguards, and physical safeguards regarding access or control of use. work Information in the identity verification and verification system (access control) must at least consist of the following actions: (1) Controlling access to data and equipment for storing and processing data in the system. Verification and verification of identity by taking into account usage and security; ...(continue)...	
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	Section 14 : The license holder must provide measures to prevent and maintain the security of Personal data of service users, both technical and internal management, in an appropriate format To prevent loss, access, use, change, correction, or disclosure of personal information of service users. without authority or illegally and must review such measures when necessary is it necessary or when technology changes in order to be effective in maintaining appropriate security. The NBTC may set minimum standards. causing the licensee to operate You can take action. Violation of personal information of any service user risks affecting rights and freedoms of	

		individuals, the license holder must inform the NBTC of the violation without delay as much as possible. Within 72 hours from knowing the cause If any violation has a high risk of affecting the rights and freedoms of individuals Licensee The cause of the violation must be reported to the NBTC without delay as much as possible within 24 hours from knowing the cause. and must inform users of the cause of such violation along with remedies without delay as well In this regard, the NBTC may prescribe criteria for such notification and exemptions for licensees to proceed	
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications		
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)		
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information		

	Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)		
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		

47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)		
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation	internal	internal
		Accuracy	Retention Limitation
1	Constitution of the Kingdom of Thailand		
2	Personal Data Protection Act 2019		
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		

8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the		

	Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under		

	Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority		

	under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)	Section 10. In the case where the law requires that any information be presented or retained in its original form as an original document, if the presentation or retention is made in the form of a data message in accordance with the following rules, it shall be deemed as the presentation or retention of the original document under the law: (1) a reliable method is used with that data message for assuring the integrity of the information from the time when it was generated in its final form; and (2) the information is capable of being subsequently displayed. The consideration of the integrity of the information under (1) shall be made by having regard to its completeness and absence of alteration, apart from any additional endorsement or recordation or any change which may arise in the normal course of communication, storage or display of the information, which does not affect the integrity of that information. In determining the reliability of the method used for assuring the integrity of the information under (1), regard shall be had to all the relevant circumstances, including the purposes for which the information was generated. Section 12. Subject to the provisions of section 10, in the case where the law requires that any document or information be retained, if the retention is made in the form of a data message in accordance with the following rules, it shall be deemed as the retention of the document or information as required by the law:	

		(1) such data message is accessible and usable for subsequent reference without its meaning being altered; (2) such data message is retained in the format in which it was generated, sent or received or in a format which can display accurately the information generated, sent or received; and (3) the information, if any, which enables the identification of the origin, source and destination of such data message including the date and time when it was sent or received is retained. The provisions of paragraph one shall not apply to the information the sole purpose of which is to enable the data message to be sent or received. The State agency responsible for the retention of any document or information may prescribe supplemental details with regard to the retention of such document or information insofar as they are not contrary to or inconsistent with the provisions of this section. Section 28. In the case where a certification service is provided to support an electronic signature that may be used for legal effect as a signature, the certification service provider shall: (1) act in accordance with the policies and practices it has represented; (2) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are specified in the certificate; (3) provide means for reasonable access that enable a relying party to	

		ascertain from the certificate all the material representations, as follows: ...(continue)... Section 30. A relying party shall: (1) take reasonable steps to verify the reliability of an electronic signature; (2) in the case where an electronic signature is supported by a certificate, take reasonable steps to: (a) verify the validity, suspension or revocation of the certificate; and (b) observe any limitation with respect to the certificate.	
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		Section 26 (first paragrph repealed by No.2 act) A service provider shall keep user's data as necessary for the purpose of identifying the user from the first day of such a service and store such user's data for a period not less than ninety days from its expiry date. The Minister shall prescribe the type of service providers, how and when the provisions ofParagraph 1 shall apply by promulgation in the Government Gazette. Any service provider, who fails to comply with this Section, shall be liable to a fine not

			exceeding Five Hundred Thousand Baht.
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		Section 17. The provisions of paragraph one of section 26 of the Commission of Computer-Related Offences Act, B.E. 2550(2007) shall be repealed and replaced by the following: "Section 26. A service provider must retain computer traffic data for a period of not less than ninety days as from the date on which such data enter a computer system, provided that, in the case of necessity, the competent official may order any service provider to retain computer traffic data for a period exceeding ninety days but not exceeding two years as a matter of an individually exceptional case and on an ad hoc basis." (continue from original act) A service provider shall keep user's data as necessary for the purpose of identifying the user from the first day of such a service and store such user's data for a period not less than ninety days from its expiry date. The Minister shall prescribe the type of service providers, how and when the provisions ofParagraph 1 shall apply by promulgation in the Government Gazette. Any service provider, who fails to comply with this Section, shall be liable to a fine not exceeding Five Hundred Thousand Baht.
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of		

	information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		Section 4 In the case where the court orders to stop the dissemination or deletion of computer data from the location of the data The competent official will suspend the dissemination or delete the computer data or you can order the service provider to stop the dissemination or delete the computer data ...(continue)... Section 5 Subject to Section 4, if the competent official will stop the spread or delete the computer data itself This must be done immediately after receiving a copy of the court proceeding report that appears. to see court orders and details of the location of the information Except in the case of reasonable necessity that cannot Immediately stop the

			dissemination or delete computer data. Let the official stop it. Making available or deleting computer data when such necessity has ceased. But it must not be more than seven days. ...(continue)... Section 7 Subject to Section 4 in ordering the service provider to stop disseminating or deleting computer information Have the official prepare the order. The order must at least contain: (1) A copy of the court proceeding report showing the court order and the details of the computer, the location of the that the court has ordered to stop dissemination or delete computer data (2) Specify whether the service provider will take steps to stop the dissemination or delete computer data.In which part and when must the work be completed? (3) Other relevant documents and evidence (if any) which have been certified as correct. An order for a service provider to suspend the dissemination or deletion of computer data shall be made according to the form D.S.R. 1 attached to this announcement Section 8. When a service provider receives an order to suspend the dissemination or delete computer data. from the official Action must be taken to stop the dissemination or delete computer data. According to the details appearing in the official's order immediately after receiving the order. But must not exceed the period specified in the order Except in the case of reasonable necessity which the official allows to proceed. beyond

			the period specified in the order But it must not exceed fifteen days. To suspend the dissemination or delete computer data of the service provider to proceed with any technical measures (Technical Measures) that meet standards in order to give effect to the court order.
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)	Section 9: Preserving computer traffic data. The service provider must use the following secure and secure methods: (1) Store in media or computer equipment or computer systems. that can be treated Completeness, accuracy, authenticity (Integrity) and personal identification (Identification) who have access to such media; (2) There is a system for maintaining the confidentiality of stored information and specifying the level of confidentiality for access. Such information To maintain the reliability of the information and does not allow administrators to edit information that is preserved such as storing it in a Centralized Log Server or doing Data Archiving or doing Data Hashing, etc., ...(continue)... Section 11 To make computer traffic information accurate and usable that can actually be useful Service providers must set the clocks of all service equipment to match the universal reference time (Stratum 0). with related computer equipment (Clock Synchronization) and data storage standards Computer traffic must comply with international standards as stipulated. as specified in the appendix to this announcement.	Section 5 The following types of service providers have a duty to maintain computer traffic data. (1) a service provider for the general public to access the Internet; or to be able to contact each other by any other means, through the computer system. Whether providing services on your own behalf or on behalf of another person or for the benefit of others can be classified as follows: ...(continue)... Section 6 Computer traffic data that the service provider has a duty to maintain must be as specified In Appendix B attached to this announcement. Section 7 Each type of service provider as specified in Section 5 has a duty to maintain traffic information via computer as follows: (1) The service provider according to Section 5 (1) A. has a duty to collect computer traffic data as specified In Appendix B (2) The service provider according to Section 5 (1) B. has a duty to collect computer traffic data as specified in Appendix B. according to type, type and function of service (3) The service provider according to Section 5 (1) C. has a duty to collect computer traffic data as specified in Appendix B. according to type, type and function of service

			(4) The service provider according to Section 5 (1) D. has the duty to collect computer traffic data as specified In Appendix B. (5) The service provider under Section 5 (1) E has a duty to collect computer traffic data as specified In Appendix B (6) The service provider according to Section 5 (1) Ch. has the duty to collect computer traffic data as specified In Appendix B (7) The service provider under Section 5 (2) has a duty to collect computer traffic data as specified In Appendix B Section 10 In the case where the service provider has an agreement, contract or hires a third party who is not. The service provider provides who performs duties or is involved in maintaining computer traffic data in lieu of their own duties that must be carried out according to this announcement Service providers still have a legal obligation to keep copies of data. computer traffic and possess important information Copies related to computer traffic data which can Identify yourself and hand it over to the official immediately upon request by the official. by traffic information Such computers must have an authentication and authentication system. (Identification and Authentication) that are reliable as specified in this announcement. Section 12 The service provider must retain computer traffic data according to the following period of time: (1) In general cases, the service provider shall retain computer

			traffic data for not less than ninety days. From the date that information enters the computer system (2) In the case of necessity when there is reasonable cause to believe that there has been an action committing an offense under this Act or for the benefit of collecting facts and evidence regarding the action committing an offense related to security of the kingdom terrorism Transnational criminal organization or public order which uses a computer system Computer data or devices used to store computer data are components.or is part of the commission of an offense or has computer data related to the commission of an offense, regardless of the fact of necessity Such necessity is evident to the official himself. or upon request From the official responsible for the investigation or inquiry before the time period under (1) expires, the official Officials have Order any service provider to maintain computer traffic data of service users as a special case. Only for the next one, each time not exceeding six consecutive months. But it must not exceed two years. Section 13 Service providers have a duty to maintain computer traffic data from the date of this announcement.The clause is effective (1) The service provider according to Section 5 (1) D. shall collect computer traffic data as specified. Within one year from the effective date of this announcement. (2) The service provider according to Section 5 (2) C. shall collect computer traffic data as specified. Within one hundred

			and eighty days from the date this announcement comes into effect
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)		Section 11 The licensee must keep the personal information of service users in the event that the service is being used not less than 90 days in the past throughout the service period Except in the case where a user complains about using the service. Telecommunications which It is necessary to use personal information of service users to prove the correctness of service use Service charge or checking the quality of service Licensees must maintain personal information of service users only as necessary It is necessary for the benefit of such proof to be kept until the complaint is considered. will be completed. However, there is no need to keep it for more than 2 years from the date of receipt of the complaint. In the case where telecommunications services are terminated Licensees must maintain personal information of the service user under paragraph one for not less than 90 days from the end of the service contract, except in the case. If it is necessary or there is an outstanding service charge, the licensee must keep personal information of the service user

			but need not keep it for more than 2 years from the end of the service contract or in the case Need to be kept within the period specified by other laws. In this regard, the NBTC may set criteria for maintaining personal information of service users in other cases. In addition to what may be specified in this announcement.
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications		
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)	Section 17 In processing information, a credit information company or a person assigned by it to process information on its behalf shall set up at least the following systems and requirements: (1) Stored information classification system; (2) Information revision system to ensure that it is accurate, complete and up-to-date at all times; ...(continue)... Section 19 A member has the following duties: (1) To report and send the information under Section 18 to the credit information company, and notify its customers of the sending of the said information without discrimination;	Section 7. In the case where the financial institution or business operator receives notification from the injured party who is the holder of a deposit account or electronic money account that transactions have been made using the deposit account or Such electronic money accounts and is related to technology crimes. to financial institutions or the business operator has a duty to stop doing business Temporarily store the transaction and enter the information into the system. or the process ofdisclosing or exchanging information according to Section 4 for financial institutions and business operators All transfereesknow and stop doing

		(2) To send correct and up-to-date information. If it knows that any information is not correct, it must make a correction and send the correct information to the credit information company; (3) In case the member receives a report from the credit information company that an information subject is of the opinion that his or her information is incorrect, the member shall proceed to: ...(continue)... Section 26 Upon the information subject having exercised the right to examine or correct his information kept with a credit information company or a member, the credit information company or the member shall promptly consider the request and check the said information, and shall notify the result of examination or correction of the information, together with reasons therefor, to the information subject within thirty days from the date of receipt of the request. In case the credit information company or the member is of the opinion that the information is incorrect for any reason, the credit information company or the member shall promptly correct the information, and shall notify the corrected information to the source of information, the members or the service users concerned, so that they can also correct the information accordingly.	business. ...(continue)...
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information		

	Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)		
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		

47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)		
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation	internal	internal
		drawing up of codes of conduct	record of processing activities
1	Constitution of the Kingdom of Thailand		
2	Personal Data Protection Act 2019		39 The Data Controller shall maintain, at least, the following records in order to enable the data subject and the Office to check upon, which can be either in a written or electronic form: 40 The Personal Data Processor shall have the following duties: (1) carry out the activities related to the collection, use or disclosure of Personal Data only pursuant to the instruction given by the Data Controller, except ... (2) provide appropriate security measures ...; and (3) prepare and maintain records of personal data processing activities...
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		3 Personal data processors must prepare and maintain records of activities Processing of personal data for each type of activity is recorded. with at least the following details: (1) Name and information about the personal data processor. and representatives of the data processor Personal data in the case where a representative is appointed. (2) Name and information about the personal data controller that the personal data processor processes according to the order or on behalf of the personal data controller. and representative of the personal data controller In the event that a representative is appointed (3) Name and information about the Personal Data Protection

			Officer, including contact locations and methods. Contact in the case where the personal data processor has appointed a personal data protection officer (4) Type or nature of collection, use, or disclosure of personal information that the personal data processor performs on the order or on behalf of the personal data controller, including the personal data and the purposes for collecting, using, or disclosing the personal data as received; Assigned by the Personal Data Controller (5) Types of persons or agencies receiving personal data in the case of sending or transferring personal data abroad. (6) Explanation of security measures according to section 40, paragraph one (2) The personal data processor must prepare and maintain records of activities. The processing of personal data according to paragraph one shall be in writing, which will be in writing or In electronic form, this is a record of such personal data processing activities. It must be easily accessible. and can show Office of the Personal Data Protection Commission, Personal Data Controller or the person who Contact the Office of the Personal Data Protection Commission or the Data Controller. Individuals can be assigned to check quickly upon request
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small		

	organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case		

	Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data		

	Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the	6 Personal data controller or personal data processor who will send or transfer personal data to the personal data controller or personal data processor located abroad and being in the same business group or business group can propose a policy to protect personal information in the affiliate the same business or	

	Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	business group (binding corporate rules) for conducting business or joint business according to Article 5 so that the Office of the Personal Data Protection Commission can inspect and certify according to this announcement by submitting the said policy by any of the following methods: (1) Submit directly to the Office of the Personal Data Protection Commission. (2) Submit via post to theOffice of the Personal Data Protection Commission. (3) Submit via electronic channels or any other channels as specified by the Office of the Personal Data Protection Commission.	
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)	Section 28. In the case where a certification service is provided to support an electronic signature that may be used for legal effect as a signature, the certification service provider shall: (1) act in accordance with the policies and practices it has represented; (2) exercise reasonable care to ensure the accuracy and completeness of all	Section 29. In determining the trustworthiness of systems, procedures and human resources under section 28 (6), regard may be had to the following factors: (1) financial status, human resources and existing assets; (2) quality of hardware and software systems; (3) procedures for issuing certificates, applications for certificates and

		material representations made by it that are relevant to the certificate throughout its life cycle or that are specified in the certificate; (3) provide means for reasonable access that enable a relying party to ascertain from the certificate all the material representations, as follows: ...(continue)...	retention of records in relation to the provision of the service; ...(continue)...
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		

27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		

33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	Section 20 : The license holder must prepare Create a policy to protect the rights of service users regarding information Personal, right to privacy and freedom to communicate with each other through telecommunications in accordance with this announcement and the law on personal data protection Complete in Thai and other languages.As far as marketing has been done by the licensee, it must be submitted to the NBTC Secretary-General for inspection and certification according to the criteria.that the NBTC specifies within 90 days from the date the NBTC announces it and must provide Publication is general At least it must be published on the licensee's website. Service point service users and in service application documents or service contracts Policy on rights protection according to paragraph one Must at least consist of (1) Period of retention of personal data of service users according to Section 11. (2) Rights of service users according to Section 12 (3) Complaint rights of service users according to Section 13. (4) Submission of personal information of service users according to Section 19.	Section 15 license holder must provide measures to build confidence in communication with each other.by telecommunications and is prohibited from doing the following: (1) eavesdropping, inspecting, quarantining signals or disclosing things communicated by telecommunications that a person Keep in touch with each other in any form. except by virtue of with authority under the provisions of specific laws to maintain State security or to maintain peace and order or good morals of the people and comply completely according to the process provided by that law In this regard, the licensee shall record such request and what the licensee has decided to do. or not taking action and reporting to the NBTC Office in the form of quarterly statistics. (2) Doing anything to change the meaning of data (3) Accessing and using equipment without consent. The license holder must also provide a system to prevent actions under (1), (2), and (3)
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications		

35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)		Section 27 In case there is a dispute between the information subject and the credit information company concerning the accuracy of the information, and no agreement can be reached, the credit information company shall record the dispute, together with supporting evidence of the information subject, within the information system of the information subject. ...(continue)...
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		

42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)		
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life		

	Insurance Business B.E. 2564 (2021)		
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)		
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation	internal	internal
		Designation of the data protection officer	Others
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019	37 The Data Controller shall have the following duties: (1) provide appropriate security measures for preventing the unauthorized or unlawful loss,...; (2) in the circumstance where the Personal Data is to be provided to other Persons or legal persons, apart from the Data Controller, the Data Controller shall take action to prevent such person from using or disclosing such Personal Data unlawfully or without authorization; (3) put in place the examination	

		system ... (4) notify the Office of any Personal Data breach ... (5) in the event of being the Data Controller pursuant to Section 5 paragraph two, the Data Controller shall designate in writing a representative of the Data Controller who must be in the Kingdom of Thailand and be authorized to act on behalf of the Data Controller without any limitation of liability with respect to the collection, use or disclosure of the Personal Data according to the purposes of the Data Controller. 41 The Data Controller and the Data Processor shall designate a data protection officer in the following circumstances: 42 The data protection officer shall have the following duties: (1) give advices to the Data Controller or the Data Processor, including the employees or service providers of the Data Controller or of the Data Processor with respect to compliance with this Act; (2) investigate the performance of the Data Controller or the Data Processor, including the employees or service providers of the Data Controller or of the Data Processor with respect to the collection, use, or disclosure of the Personal Data for compliance with this Act; (3) coordinate and cooperate with the Office in the circumstance where there are problems with respect to the collection, use, or disclosure of the Personal Data undertaken by the Data Controller or the Data Processor, including the employees or service providers of the Data Controller or of the Data Processor with respect to	

		the compliance with this Act; (4) keep confidentiality of the Personal Data known or acquired in the course of his or her performance of duty under this Act. The Data Controller or the Data Processor shall support the data protection officer in performing the tasks by providing adequate tools or equipment as well as facilitate the access to the Personal Data in order to perform the duties. The Data Controller or the Data Processor shall not dismiss or terminate the data protection officer's employment by the reason that the data protection officer performs his or her duties under this Act. In the event that there is any problem when performing the duties, the data protection officer must be able to directly report to the chief executive of the Data Controller or the Data Processor. The data protection officer may be able to perform other duties or tasks but the Data Controller or the Data Processor must warrant to the Office that such duties or tasks are not against or contrary to the performance of the duties under this Act.	
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		

5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		8 Where the personal data controller has an agreement with the personal data processor to control operations to carry out the duties of the personal data processor in accordance with the law Personal information protection or assign or order the personal data processor to collect, use, or disclose personal data in accordance with the request under orders or on behalf of oneself personal data controller, It must be specified in the agreement or relevant contract that the personal data processor has a duty to report the incident. violation of personal data to the personal data controller without delay within seventy-two hours from the personal data processor is also aware of the incident to the best of his ability.
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under		4 for the benefit of protecting personal information, the data controller and data processors whose operations carrying out activities to collect, use or disclose personal information as part of core activities, it is

	Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		necessary to check personal information or systems on a regular basis, due to having a large amount of personal data (on a large scale), according to Article 5 and Article 6 5 Activities of the personal data controller and personal data processor which is part of core activities that are tracked, monitored, analyzed, or predicted behavior, attitude, or individual characteristics (profile), which generally include systematic or regular collection, use, or disclosure of personal information shall be considered to be an activity necessary to check regularly Collection, use, or disclosure of personal information in the following cases shall also be considered as necessary to check personal information or systems regularly according to paragraph one:... 6 Activities of the personal data controller and personal data processor which is part of core activities that contain a large amount of personal data (on a large scale), shall be considered by the following factors:... ... 8 Personal Data Protection Officer of the Personal Data Controller or Processor according to this announcement may perform other duties or missions but the controller of personal data or Processors of personal data must certify with the office that such duties or missions does not conflict with the duties under the law on personal data protection.
9	Guideline for obtaining		

	consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562	2.2. Question: Appointing a personal data protection officer from outsiders or personnel within the organization. What are the different advantages and disadvantages? and the organization needs to set up a department with duties specific responsibility To perform such work or not? How? Answer: Section 41, paragraph seven, of the Personal Data Protection Act 2019 stipulates that the Personal Data Protection Officer may be an employee of the Personal Data Controller or Data Processor. Personally or as a contractor providing services according to a contract with the personal data controller or data processor. Therefore, it is important to consider, according to the appropriateness and necessity of the organization, how it can arrange for personal data protection officers.... 2.3. Question: Personal Data Controller (Data Controller) means a juristic person or organization, right? And is it necessary to appoint a natural person to act on behalf of the juristic person or organization in performing the duties as a personal data controller? If it is necessary to appoint a natural person to act on behalf of the	

		juristic person or organization? Performing such duties What qualities should that person have? And does it have to be the owner of personal data or the owner of the data (Data Owner) or not? How? And should it be an outside person or within the organization? Answer: If an organization that is a juristic person has the authority to decide or take action regarding the collection, use, or disclosure of personal information. The said organization will be considered the personal data controller according to Section 6 of the Personal Data Protection Act B.E. 2019 without having to appoint any other person to act as the personal data controller. The division, agency, as well as The organization's employees and personnel will not have separate personal data controller or personal data processor status from the organization.	
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562		

	(2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal		

	Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		9. In the case where there is no specific provision of law and there is no necessity according to the law on personal data protection in collecting personal information about Criminal history for proceeding according to Section 5, paragraph one, when such proceeding is completed, the Personal Data Controller shall collect personal data relating to criminal history for no longer than six months from the date such processing is completed for each personal data subject according to the purpose and necessity of collecting, using, or disclosing personal information unless received the express consent of the owner of personal data is otherwise.
20	Electronic Transactions Act, B.E. 2544 (2001)		Section 16. The addressee is entitled to regard a data message as being that of the originator and to act on that

			assumption with respect to that data message if: (1) the addressee has properly ascertained whether the data message was that of the originator in accordance with the procedure previously agreed with the originator; or (2) the data message as received by the addressee resulted from the action of a person who used a method which is used by the originator to identify data messages as his own and to which such person gained access through the relationship between such person and the originator or a person having the authority to act on behalf of the originator. The provisions of paragraph one shall not apply if: (1) at that time, the addressee has received notice from the originator that the data message as received by the addressee is not that of the originator and, at the same time, the addressee had reasonable time to take steps in verifying the facts to which the notice relates; or (2) in a case under paragraph one (2), the addressee knew or should have known, had the addressee exercised reasonable care or acted in accordance with the agreed procedure, that the data message was not that of the originator.
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		Section10 ...(shorten)... In the case of a printout of the data message under paragraph one for the purpose of reference of the information contained therein, if such printout contains complete information corresponding to that data message and certified by such competent agency as designated, by Notification, by the Commission, it shall be deemed

			that such printout is equivalent to the original. Section 12/1.7 The provisions of section 10, section 11 and section 12 shall also apply mutatis mutandis to a document or information subsequently prepared or transformed into the form of a data message by an electronic means and to the retention of such document or information The preparation or transformation of a document and information into the form of a data message under paragraph one shall be in accordance with the rules and procedure prescribed by the Commission.
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission.		

	which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public		

	Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)		
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications		
35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		Section 6 In the case where a financial institution or business operator finds reasonable cause of doubt or receives information From the system or process for disclosing or exchanging information according to Section 4, whether a deposit account or What electronic money accounts are or may be used Doing transactions related to technological crimes or committing a predicate offense or money laundering offense according to the law on prevention and suppression Money laundering: Financial institutions or business operators have a duty to stop money laundering. ...(continue)...
36	The Credit Information		Section 22 A service user shall have the following duties:

	Business Operation Act B.E. 2545 (2002)		(1) To use information according to the objectives prescribed under Section 20, Section 20/1, Section 24/1 and Section 24/3; (2) Not to disclose or disseminate information to others who are not entitled to know the information.
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)		
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re:		

	Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		

50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)		
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

Data Cross Boarder Dist

#	Regulation	Cross-border data transfer	Exception/Existence and Description of Exception
		Provisions for Transborder Data Transfer	What are the exceptions (e.g., sufficient authorization, transfers based on contracts equivalent to standard contract clauses (SCCs) or binding corporate rules (BCRs), transfers based on corporate certification, etc.)?
		Provisions for cross boarder data transfer	Conditions for exemption of complying to localization
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019	28 In the event that the Data Controller sends or transfers the Personal Data to a foreign country, the destination country or international organization that receives such Personal Data shall have adequate data protection standard, and shall be carried out in accordance with the rules for the protection of Personal Data as prescribed by the Committee in Section 16(5), except in the following circumstances:	28 In the event that the Data Controller sends or transfers the Personal Data to a foreign country, the destination country or international organization that receives such Personal Data shall have adequate data protection standard, and shall be carried out in accordance with the rules for the protection of Personal Data as prescribed by the Committee in Section 16(5), except in the following circumstances: (1) where it is for compliance with the law; (2) where the consent of the data subject has been obtained, provided that the data subject

			has been informed of the inadequate Personal Data protection standards of the destination country or international organization; (3) where it is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract; (4) where it is for compliance with a contract between the Data Controller, and other Persons or juristic persons for the interests of the data subject; (5) where it is to prevent or suppress a danger to the life, body, or health of the data subject or other Persons, when the data subject is incapable of giving the consent at such time; or (6) where it is necessary for carrying out the activities in relation to substantial public interest. ... 29. In the event that the Data Controller or the Data Processor who is in the Kingdom of Thailand has put in place a Personal Data protection policy regarding the sending or transferring of Personal Data to another Data Controller or Data Processor who is in a foreign country, and is in the same affiliated business, or is in the same group of undertakings, in order to jointly operate the business or group of undertakings. If such Personal Data protection policy has been reviewed and certified by the Office, the sending or transferring of Personal Data to a foreign country, which is in accordance with such reviewed and certified Personal Data protection policy, can be carried out and shall be exempt from

			compliance with Section 28. ...
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)	3 Personal data processors must prepare and maintain records of activities processing of personal data for each type of activity is recorded. with at least the following details: (5) Types of persons or agencies receiving personal data in the case of sending or Transferring personal data abroad.	
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection		

	Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from		

	the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research		

	Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	3. "Send or transfer personal data" means sending or transferring personal data by the sender or transfer personal information whether it is sending or transferring information by physical means or through the computer system or network system to the recipient of personal information but it does not include...	3. "Send or transfer personal data" means ... but it does not include sending and receiving personal information in a way that is just a medium (intermediary) in the transmission of data (data transit) between computer systems or network systems or the storage of data (data storage) in temporary or permanent form that no third party has access to such personal information in addition to the personal data controller or the personal data processor who sends the personal data or its personnel, employees, or employees. The controller of personal data or the processor of that personal data, such as in the case of sending data over a network system abroad or sending data through the cloud computing service provider's system provider)where there is no person other than the personal data controller or personal data processor who is The sender of that personal information or the personnel, employees, or employees who access the personal information because there are technical measures or legal conditions to support it. 5. in the case where the Personal Data Controller sends or transfers personal data abroad. The destination country or international organization receiving personal data must have sufficient data protection standards which must comply with the criteria for personal data protection according to this Notification, except (1) It is compliance with the law. (2) obtain consent from the owner of personal data by

			informing the owner of personal data be aware of the inadequate personal data protection standards of the destination country or international organization. That has received personal information (3) it is necessary for the performance of a contract to which the owner of personal data is a party or to be used to carry out the request of the owner of personal data before entering into the contract. (4) It is an action based on a contract between the Personal Data Controller and another person or juristic person. For the benefit of the owner of personal data (5) To prevent or stop danger to the life, body, or health of the owner of personal data or another person When the owner of personal data is unable to give consent at that time (6) It is necessary for carrying out a mission for important public benefits.
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)	4. "Send or transfer personal data" means sending or transferring personal data by the sender or Transfer personal information whether it is sending or transferring information by physical means or through the computer system or network system to the recipient of personal information <u>but this does not include</u> ...	4."Send or transfer personal data" means.... but this does not include sending and receiving personal information in a way that is just a medium (intermediary) in the transmission of data(data transit) between computer systems or network systems or the storage of data (data storage) in temporary or permanent form. that no third party has access to such personal information In addition to the personal data controller or The personal data processor who sends the personal data or its personnel, employees, or employees. The controller of personal data or the processor of that personal data, such as in the case of sending data through a network system in a foreign country or sending

			data through the system of a cloud computing service provider where there is no person other than Personal data controller or personal data processor who is The person who sends that personal information or the personnel, employee, or employee who has access to the personal information because there are measures technical or legal conditions support. 8. In the case where there is still no decision regarding adequate personal data protection standards of the destination country or international organization that receives personal data of the committee according to Article 28 of the Personal Data Protection Act B.E. 2019 or does not yet have a policy for protection Personal data according to Section 5, the Personal Data Controller or Personal Data Processor may send or Personal data can be transferred abroad without having to comply with Article 28 when appropriate safeguards have been put in place to enforce the owner's rights. Personal information and has effective legal remedies Appropriate protection measures according to paragraph one It may be in the following format: (1) Contractual terms that are in accordance with acceptable contractual terms ... (2) Certification regarding collection, use, and disclosure of personal data of the personal data controller or personal data processor In respect of sending or transferring Personal data across borders ... (3) provisions for personal data protection measures in instruments or binding

			agreements... 9. Appropriate protection measures according to Article 8 must meet the following criteria: (1) Effectiveness and legal force of personal data protection measures and legal remedies for juristic persons or natural persons... (2) Requirements ensuring the protection of personal information, rights of the owner of personal data and complaints For personal information sent or transferred abroad (3) There are measures to protect personal information and measures to maintain security. that complies with the law on personal data protection ... 10. Subject to Article 9, contractual terms regarding the sending or transfer of personal data according to Article 8 Paragraph two (1) must have one of the following characteristics: (1) Contract terms that the contracting parties make and are binding, containing content and terms related to Protection of personal information as follows: ... (2) Contract terms that the contracting parties made in accordance with foreign law or prepared by the organization International and has content and requirements related to the protection of personal data using one of the model contracts as follows: (a) ASEAN Model Contractual Clauses for Cross Border Data Flows; (b) Standard Contractual Clauses for the Transfer of Personal Data to Third Countries issued in accordance with Article 46 (1) in conjunction with Article 46 (2) (c) and Article 28 (7) of the

			Regulation Law (EU) 2016/679 of the European Union or the General Data Protection Regulation (GDPR). (c) Standard contractual terms for sending or transferring personal data overseas of other agencies or international organizations as specified by the Personal Data Protection Committee. 11. Contract provisions according to Article 10 (2) must contain content regarding personal data protection. In the following matters: ... 12. In the case where contract terms according to Article 10 (2) are used, if applicable law is referenced, amendments to other matters in the contract or add appropriate personal data protection measures or amendment of content in non-essential parts which does not conflict with the principles in Article 11 and does not affect the rights and freedoms of the owners of personal data shall be able to do Clause 13 The Office shall also publish information and details of the model contract terms under Clause 10 (2) through the Office's website. 14. Certification regarding the collection, use, and disclosure of personal information of the personal data controller or personal data processor in respect of sending or transferring information Personal cross-border or sending or transferring personal information between countries that there are data protection measures with appropriate safeguards in accordance with

			accepted standards according to Article 8, paragraph two (2) shall be as prescribed by the Personal Data Protection Committee which must have content according to Section 11 as well.
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)		
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)		
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)		
26	Notification of Ministry of Digital Economy and Society Re:		

	characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service		

	providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)		
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	Section 8: Collection, use, or disclosure of personal information of service users in the following cases: There is no need to follow the criteria in items 6 and 7. (1) Send personal data of service users to the NBTC or NBTC Office according to item 19. (2) In the case of exemption according to the law on personal data protection	
		Section 9: Sending or transferring personal data of service users abroad. In addition to having to practice According to Section 6 and Section 8 of this announcement must also comply with the criteria stipulated by the law on protection Personal information is also specified. The NBTC may set criteria for sending or transferring personal information of service users going abroad to the license holder. You can take action.	
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and	7. Sending or transferring personal data of service users abroad 7.1 Sending or transferring data1 Personal information of users1 who use the service abroad If it is an action for Providing 1 telecommunications service The license holder must confirm that it is necessary for the operation of	

	Freedom of Communications	telecommunications business. According to the telecommunications service contract entered into with the users of the service or if it is done for other purposes In addition to operating telecommunications businesses, license recipients must proceed in accordance with the NBTC announcement, Section 1A 6 paragraphs two to paragraph 4 7.2 in all cases as mentioned in Section 1A 7.1. Must comply with the Personal Data Protection Act. Including the secondary criteria issued by the Personal Data Protection Committee for the time being. During the time that No. 5 There are no secondary criteria of the NBTC, which are 1 to 5 (1) Designating 1 destination country or international organization.Countries that receive personal data of service users must have adequate personal data protection standards. This must be in accordance with the criteria. Providing protection for personal data as specified by the Data Protection Committee 5 Personnel Department announces specifications Including information except for sending or transferring personal data of users of the service to (2) sending or transferring personal data of service users to the controller of personal data or A person who processes personal data 5 who is 5 abroad and is 5 in the same business group or group as Person 1 who receives a license to operate a business or joint business	
35	The Royal Decree on Measures for Protection and Suppression of Technology		

	Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)	Section 12 No credit information company or information controller or information processor carrying on or operating business in the Kingdom shall operate, control or process information outside the Kingdom.	
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)		
43	The National Health Act B.E. 2550 (2007)		
44	The Payment System Act B.E. 2560 (2017)		
45	The Notification of the Bank of Thailand	5.3 Criteria Management principles for providing fair services to	

	SorGorSor2. 4/2563 re: Market Conduct Rules	customers include: Criteria regarding the management of 9 work systems related to providing services to customers, disclosure of information about being compared, fined or blamed. Disclosing product information and service quality information and setting additional conditions, ordering corrections, delays, or suspension of services in whole or in part. ...(shorten)... However, for the branch's compliance with the criteria in this announcement. **oversea branch of the service providers mentioned in Section 4, including companies in the financial business group located oversea**, if the supervisory authority in that country has regulations and regulations regarding management of Providing services to customers fairly Or are there any other criteria that have restrictions The regulations are set in the same manner in order to supervise and protect financial service users so that they receive services fairly. **Branches and companies in the overseas financial business group of the above service providers must comply with the criteria as follows.** and in the case of a service provider that is a specialized The Islamic Bank of Thailand Follow the management criteria. regarding providing services to customers fairly in this announcement by giving taking into account the consistency with Principles of Islam financial institution as specified in Section 4.3, if the law allows it	

		to do so is possible or has been determined The criteria have been specified specifically. to financial institutions Special operations are carried out in accordance with the established	
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)	Article 9 In the case where the company transfers personal information to the recipient of the information who is abroad. follow Criteria for transferring personal data abroad according to the law on personal data protection	
		Article 19 In the case where the life insurance agent who is the personal data processor is assigned by the company allows the transfer of personal information to recipients who are abroad. Follow the rules for transferring personal	

		information. Go abroad according to the guidelines set by the company.	
		Article 22 In the case where a life insurance agent is the controller of personal data, he or she has the following duties: ...(shorten)... **(7) In the case where a life insurance agent transfers personal data to a recipient who is abroad, follow the rules for transferring personal data abroad in accordance with the law on personal data protection.** ...(continue)...	
		Article 30 In the case where a life insurance broker transfers personal information to a recipient who is abroad. Follow the rules for transferring personal information abroad in accordance with the Personal Data Protection Act.	
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)	Article 9 In the case where the company transfers personal information to the recipient of the information who is abroad. follow Criteria for transferring personal data abroad according to the law on personal data protection	
		Article 19 In the case where a non-life insurance agent who is a personal data processor is assigned from the company to transfer personal information to recipients who are abroad Follow the data transfer guidelines. Individuals traveling abroad according to the guidelines set by the company.	
		Article 22 In the case where the general insurance agent is the controller of personal information, he or she has the following duties: (1) A non-life insurance agent must collect, use or disclose personal information according to the purpose. that have been	

		informed to customers before or while collecting personal information If a non-life insurance agent finds or knows that there is The purpose of collecting, using, or disclosing personal information is in addition to the original purpose. This is in addition to what is specified in the personal data protection policy of the insurance agent itself or in the case where there is a change in the purpose of collecting, using or disclosing personal data. General insurance agent You can add or change the purposes for collecting, using, or disclosing personal information. ...(shorten)... **(7) In the case where a non-life insurance agent transfers personal information to a recipient who is abroad. Follow the rules for transferring personal information abroad in accordance with the Personal Data Protection Act.** ...(continue)...	
		Article 30 In the case where a non-life insurance broker transfers personal information to a recipient who is abroad. Follow the rules for transferring personal information abroad in accordance with the Personal Data Protection Act.	
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)	Article 9 In the case where the casualty assessor transfers personal information to the recipient who is abroad. Follow the rules for transferring personal information abroad in accordance with the Personal Data Protection Act.	
51	Trade Secret Act B.E. 2545 (2002)		
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

#	Regulation	Data localisation	Government Access
		Presence or absence of provisions, stipulations regarding the types of data that must be stored in the country	National Security Law, Cybersecurity Law Provisions
		Provisions on requirement of localization; and Type of data required for localization	Provision allowed the government to access regulated data/to not comply to data regulation
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019	No	4 This Act shall not apply to: (2) operations of public authorities having the duties to maintain state security, including financial security of the state or public safety, including the duties with respect to the prevention and suppression of money laundering, forensic science or cybersecurity; (3) a Person or a juristic person who uses or discloses Personal Data that is collected only for the activities of mass media, fine arts, or literature, which are only in accordance with professional ethics or for public interest; (4) The House of Representatives, the Senate, and the Parliament, including the committee appointed by the House of Representatives, the Senate, or the Parliament, which collect, use or disclose Personal Data in their consideration under the duties and power of the House of Representatives, the Senate, the Parliament or their committee, as the case may be; (5) trial and adjudication of courts and work operations of officers in legal proceedings, legal execution, and deposit of property, including work operations in accordance with the criminal justice procedure; ...
3	PDPC Notification on security measures for the		

	data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565		
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act		

	B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		Issue1 According to Section 4 (5) of the Personal Data Protection Act B.E. 2019, Implementation of the criminal justice process is the operation of officials to determine punishment.commit an offense according to the Criminal Code. Therefore, collecting, using7 or disclosing7 personal information To be used7 in the process that leads to,such punishment, Therefore, it is considered to be an operation according to the justice process. Criminal matters which are exempted according to Section 4 (5) of the Personal Information Protection Act B.E. 2019 ...
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses		

	of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the		

	Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		

20	Electronic Transactions Act, B.E. 2544 (2001)		
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME ACT B.E. 2550 (2007)	Section 21 In case where the competent official finds that any computer data comprises undesirable programs, the competent official may file a petition with the court having jurisdiction requesting for an order to prohibit the distribution or dissemination or to instruct the owner or the possessor of such computer data to cease using, to destroy or to correct such computer data or may specify conditions of use, possession, or dissemination of such undesirable programs.	
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)	Section 13. The provisions of section 18 and section 19 of the Commission of Computer-Related Offences Act, B.E. 2550(2007) shall be repealed and replaced by the following: "Section 18. Subject to section 19, for the purpose of investigations and inquiries in the case where there is a reasonable cause to believe that the commission of an offence under this Act has occurred or in the case where a request is made under paragraph two, the competent official shall have any of the following powers to the extent necessary for using the matters concerned	

		as evidence involving the commission of the offence and in the findingof the offender: (1) addressing a written enquiry to, or issuing a summons on, a person connected with the commission of the offence for the purpose of giving statements, furnishing written explanations or furnishing documents, data or any other evidence in an intelligible form; (2) summoning computer traffic data from providers of services relating to communications via computer systems or from other persons concerned; (3)ordering a service provider to hand over to the competent official data concerning users, which are required to be retained under section 26 or which are in possession or in custody of the service provider, or to retain the such data; (4) making a copy of computer data or computer traffic data from a computer system in respect of which there is a reasonable cause to believe that an offence is committed therein, in the case where such computer system is not yet in possession of the competent official; (5) ordering the person having in possession or custody computer data or equipment used for retaining computer data to hand over such computer data or equipment to the competent official; (6) inspecting or accessing a computer system, a computer data, a computer traffic data or equipment used for retaining computer data of any person, which is evidence or may	

		be used as evidence in connection with the commission of an offence or which facilitates inquiries leading to the finding of offenders, and also ordering such person to furnish relevant computer data or computer traffic data to the extent necessary; (7) decrypting computer data of any person or ordering persons concerned in the encryption of computer data to undertake decryption thereof or co-operate with the competent official in such decryption; (8) seizing or attaching a computer system to the extent necessary only for the purpose of acquiring the knowledge of details of offences and offenders. For the purpose of investigations and inquiries by inquiry officials under the Criminal Procedure Code in criminal offences under other laws involving the use of a computer system, a computer data or equipment for the retention of computer data as an element or part of the commission of the offence or involving a computer data connected with the commission of a criminal offence under other laws, the inquiry official may request the competent official under paragraph one to take action under paragraph one, or if such facts are apparent to the competent official on account of the performance of duties under this Act, the competent official shall expeditiously gather facts and evidence and make a notification to officials concerned for further proceedings. The person receiving a request from the competent official	

		under paragraph one (1), (2) and (3) shall take action in response to the request without delay, provided that it shall not be later than seven days as from the date of receipt of the request, or within the period of time specified by the competent official, which must not be less than seven days and must not be more than fifteen days except in the case where permission is obtained from the competent official when there exists a reasonable cause. In this regard, the Minister may, by publication in the Government Gazette, prescribe the period of time within which action must be taken by service providers, as appropriate for respective types of service providers	
		Section 14. The provisions of section 20 of the Commission of Computer-Related Offences Act, B.E. 2550 (2007) shall be repealed and replaced by the following: Section 20. In the case where there occurs the proliferation of the following computer data, the competent official, with the approval of the Minister, may file with the Court of competent jurisdiction a motion, accompanied by supporting evidence, for an order compelling the discontinuance of the proliferation of the computer data or the deletion thereof from a computer system: (1) a computer data constituting an offence under this Act; (2) a computer data likely to affect the security of the Kingdom as provided in Part II, Title I or Title I/I of the Penal Code; (3) a computer data constituting a criminal offence under the law relating to intellectual property or other law, provided that such	

		computer data is, by nature, against public order or good morals of the public and a request is made by the official under such law or the inquiry official under the Criminal Procedure Code ...(continue)...	
		Section 15. The provisions of paragraph two of section 21 of the Commission of Computer-Related Offences Act, B.E. 2550(2007) shall be repealed and replaced by the following: "Undesirable instruction sets under paragraph one means instruction sets which cause a computer data or a computer system or other instruction sets to be damaged, destroyed, modified, supplemented, interrupted or function in departure from the instruction or in any other manner prescribed in the Ministerial Regulation, except undesirable instruction sets which may be used for preventing or correcting the aforesaid instruction sets, provided that the Minister may, by publication in the Government Gazette, prescribe the names, descriptions or details of undesirable instruction sets which may be used for preventing or correcting undesirable instruction sets.	
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and		

	method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		
27	Notification of Ministry of Digital Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		
28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)	Section 22. For the benefit of coordination to prevent and suppress crime in relation to Special Cases, the BSC shall have the power to issue regulations on special case duty performance between	

		government agencies as follows ...(shorten)... **(3) Exchange of information relating to the prevention and suppression of Special Cases;** and ...(continue)...	
		Section 25. In cases where there is a reasonable ground to believe that any document or information sent by post, telegram, telephone, facsimile, computer, communication device or equipment or any information technology media has been or may be used to commit a Special Case offence, the Special Case Inquiry Official approved by the Director-General in writing may submit an ex parte application to the Chief Judge of the Criminal Court asking for his/her order to permit the Special Case Inquiry Official to obtain such information. ...(continue)...	
		Section 26. No person shall disclose information obtained from an operation under Section 25, unless it is the information with regard to a Special Case offence permitted under Section 25, and it is a performance under oneûs duty or power or under the law or the courtûs order.	
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		
32	The Emergency Decree on Public Administration in a State of Emergency B.E. 2548 (2005)	Section 9. In the case of necessity in order to remedy and promptly resolve an emergency situation or to prevent the worsening of such situation, the Prime Minister shall have the power to issue the following Regulations: ...(shorten)... (3) **to prohibit the press release, distribution or dissemination of letters, publications or any means of communication**	

		containing texts which may instigate fear amongst the people or is intended to distort information which misleads understanding of the emergency situation to the extent of affecting the security of state or public order or good moral of the people both in the area or locality where an emergency situation has been declared or the entire Kingdom; ...(continue)...	
		Section 11. In the case where an emergency situation involves terrorism, use of force, harm to life, body or property, or there are reasonable grounds to believe that there exists a severe act which affects the security of state, the safety of life or property of the state or person, and there is a necessity to resolve the problem in an efficient and timely manner, the Prime Minister, upon the approval of the Council of Ministers, shall have the power to declare that such emergency situation is a serious situation, and the provisions of section 5 and section 6 paragraph two shall apply mutatis mutandis Upon a declaration under paragraph one, in addition to powers section 9 and section 10, the Prime Minister shall also have the following powers: ...(shorten)... (5) to issue a Notification that a competent official shall have the power to issue an order to inspect letters, books, printed matters, telegraphic transmissions, telephone communications or any other means of communication as well as to cancel or suspend any contact or communication in order to prevent or terminate the serious incident provided	

		that the rules prescribed in the law on special investigation are complied with mutatis mutandis	
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)	Section 19 The licensee has a duty to send the personal information of service users in the licensee's possession. To the NBTC or NBTC Office upon request. For the benefit of determining to supervise assembly Telecommunications business according to law	
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications	19. Duties of sending personal information of users of services that the license holder provides to the NBTC or the office NBTC NBTC Announcement, Section 10r 8 (1) together with Section 19 is the duty to transmit personal information of users of services that the holder of the possession license gives to the NBTC or the NBTC Office upon receipt of the request. For the benefit of Regulate telecommunications business operations according to laws such as 5N for consideration of complaints. For the purpose of regulating the quality of providing 1 service This exception is a legal obligation, consistent with the Personal Data Protection Act, Section 24 (6), together with Section 27 Paragraph 1 can therefore proceed1 even 1 no 5 no 1 receive consent from1 users1 of the service. The licensee has a duty to record the transmission of personal information of the user of the service in a list (RoPA) according to Personal Information Protection Act	
35	The Royal Decree on Measures for Protection and	Section 4, to prevent and suppress technological crimes. In the event that there are	

	Suppression of Technology Crimes B.E. 2566 (2023)	reasonable grounds to suspect that There is or may be an action of committing technological crimes for financial institutions and business operators Has a duty to disclose or exchange information about accounts and related customer transactions during Financial institutions and business operators go through systems or processes to disclose or exchange information. At the Ministry of Digital Economy and Society, Royal Thai Police, Department of Special Investigation, Anti-Money Laundering Office and the Bank of Thailand mutually agree To carry out the objectives under paragraph one to telephone network operators, other telecommunications service providers or other related service providers have a duty to disclose or exchange service information that are related to each other through the system or process of disclosing or exchanging information at the Ministry of Digital For the economy and society and for Office of the Broadcasting Commission Television business and the National Telecommunications Commission mutually agree When information has been disclosed or exchanged according to paragraph one or paragraph two. Let the revealer or exchange information, notify the Royal Thai Police or the Department of Special Investigation, as the case may be, and the Anti-Money Laundering Office immediately and when notified to the Royal Thai Police, Department of Special Investigation, or Office of the Anti-Money Laundering As the case may be, has the authority to use such information	

		to prevent, suppress or stop crimes technologically possible	
		Section 5. In the case where there are reasonable grounds to suspect that there has been an act of committing technological crimes and it is necessary to know user registration information or computer traffic information to the Royal Thai Police, Department of Special Investigation, or Office of the Anti-Money Laundering As the case may be, has the authority to order the telephone network service provider Other telecommunications service providers or other service providers related to such actions, disclose relevant information as necessary and, upon receiving the order, to the telephone network service provider Other telecommunications service providers or other service providers related to In that action, the duty is to send such information to the orderer within the time period specified by the orderer.	
36	The Credit Information Business Operation Act B.E. 2545 (2002)	Section 12 No credit information company or information controller or information processor carrying on or operating business in the Kingdom shall operate, control or process information outside the Kingdom. Section 34 The Committee shall have the power to order any person to send documents or information relating to the subject on which a person has lodged a complaint, or any other subjects related to protection of information of an information subject, for consideration. In this instance, the Committee may also summon any persons concerned to make a clarification.	

37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)		
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)		
42	The Child Protection Act B.E. 2546 (2003)	Section 30. For the purpose of implementing this Act, a Competent Official, pursuant to Chapter 3 and Chapter 4, shall have the powers and duties as follows: ...(shorten)... (3) to issue a letter summoning the Guardian or any other persons to testify or give statements about the living conditions, behavior, health, and relationship within the family of the Child; **(4) to issue a written order to a Child's Guardian, employer, or business operator, owner or possessor of the place where the Child works or used to work, lives or used to live, owner or possessor or keeper of a place where the Child**	

		studies or used to study, or a person in charge of the Child's welfare, to submit documents or evidence relating to living conditions, education, employment, or behavior of the Child; (5) to enter the residence of the Guardian, place of business of the Child's employer, place of education of the Child, or place which the Child is related to, during sunrise to sunset for the purpose of interrogating persons living nearby and gathering information or evidence relating to living conditions, relationship within the family, care provided, character, and behavior of the Child; ...(continue)...	
43	The National Health Act B.E. 2550 (2007)		
44	The Payment System Act B.E. 2560 (2017)	Section 26. The BOT may require a business provider to submit financial statements, reports or data in any form of media or produce any document at any interval or from time to time, including to provide clarifications or elaborate such reports, data or documents in accordance with the rules as prescribed in the notification of the BOT. The BOT may order the business provider to cause its directors, managers, officers or employees to make a statement, adduce data, accounts, documents and other evidences relating to the business within the time prescribed. The financial statements, reports, data, accounts, documents or clarifications submitted or adduced pursuant to the first paragraph and the second paragraph shall be completely and truthfully prepared by the business provider. In the case	

		where the BOT determines that the financial statements, reports, data, accounts, documents or clarifications submitted or adduced pursuant to the first paragraph are incomplete or ambiguous, or where the BOT deems it necessary or appropriate, the BOT shall have the power to appoint an auditor or a specialist, at the expense of such business provider, to conduct an examination and report the results thereof to the BOT.	
		Section 33. For the purposes of supervision of the payment system stability or con sumer protection, where there is a reasonable ground to believe that there are provision of payment systems or payment services in Thailand which are not subject to this Act, the BOT shall have the power to order any person relating to such systems or services to testify, submit documents or related information within the time prescribed.	
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)		

47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)		
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)	Section 15 In cases where the law requires the applicant for a permit to manufacture, import, export or sale of drugs or agricultural chemical products with new chemical substance to	

		file information supporting the permit; and if such information, either wholly or in part is trade secrets in the form of testing result, or other information regarding its preparation, discovery or creation which has involved in a great deal of effort, and the applicant has requested the state agencies to maintain the trade secrets, the state agencies concerned shall have the duties to maintain the trade secrets from being disclosed, deprived of or used in unfair trading activities, in accordance with the regulations prescribed by the Minister. The regulations under paragraph one shall, as minimum requirements, contain the following provisions: (1) Conditions of request submitted to state agencies for maintenance of trade secrets; (2) Details of testing result and information that is qualified as trade secrets; (3) Period of time for which trade secrets are to be maintained; (4) Method for maintenance of the trade secrets, taking into consideration the type of technology and testing result or confidential information; and, (5) Duties and liabilities of state officials in the maintenance of trade secrets.	
52	Trade Secret Act (No.2) B.E. 2558 (2015)		

Penalty

#	Regulation	Corporate Punishments	Individual Punishments
		Forms of penalties (e.g., recommendations for corrective action, public penalties, fines, confiscation of assets and income, data deletion, data processing, business suspension, etc.)	Penalties (penalties, fines, demotion, etc.)

		Forms of penalties on corporate	Forms of penalties on individual
1	Constitution of the Kingdom Of Thailand		
2	Personal Data Protection Act 2019	77 The Data Controller or the Data Processor, whose operation in relation to Personal Data violates or fails to comply with the provisions of this Act which causes damages to the Data subject, shall compensate the Data subject for such damages, regardless of whether such operation is performed intentionally or negligently, except where the Data Controller or the Data Processor can prove that such operation was a result of: ... 79 Any Data Controller who violates the provisions under Section 27 paragraph one or paragraph two, or fails to comply with Section 28, which relates to the Personal Data under Section 26 in a manner that is likely to cause other person to suffer any damage, impair his or her reputation, or expose such other person to be scorned, hated, or humiliated, shall be punished with imprisonment for a term not exceeding six months, or a fine not exceeding five hundred thousand Baht, or both 82 Any Data Controller who fails to comply with Section 23, Section 30 paragraph four, Section 39 paragraph one, ..., shall be punished with an administrative fine not exceeding one million Baht. 83 Any Data Controller who violates or fails to comply with Section 21, Section 22,...shall be punished with an administrative fine not exceeding three million Baht.	80 Any person who comes to know the Personal Data of another person as a result of performing duties under this Act and discloses it to any other person shall be punished with imprisonment for a term not exceeding six months, or a fine not exceeding five hundred thousand Baht, or both. The provisions of paragraph one shall not be enforced against disclosures in any of the following circumstances: ... 81 In the case where the offender who commits the offense under this Act is a juristic person and the offense is conducted as a result of the instructions given by or the act of any director, manager or person, who shall be responsible for such act of the juristic person, or in the case where such person has a duty to instruct or perform any act, but omits to instruct or perform such act until the juristic person commits such offense, such person shall also be punished with the punishment as prescribed for such offense. 88 Any representative of the Data Controller or of the Data Processor who fails to comply with Section 39 paragraph one ..., shall be punished with an administrative fine not exceeding one million Baht. 89 Any person who fails to act in compliance with the order given by the expert committee, or fails to ..., shall be punished with an administrative fine not exceeding five hundred thousand Baht.

		84 Any Data Controller who violates Section 26 paragraph one or three, ..., shall be punished with an administrative fine not exceeding five million Baht. 85 Any Data Processor who fails to comply with Section 41 paragraph one, or..., shall be punished with an administrative fine not exceeding one million Baht. 86 Any Data Processor who fails to comply with Section 40 without appropriate reasons, or ..., shall be punished with an administrative fine not exceeding three million Baht. 87 Any Data Processor who send or transfer the Personal Data under Section 26 paragraph one or ..., shall be punished with an administrative fine not exceeding five million Baht.	
3	PDPC Notification on security measures for the data controller B.E. 2565 (2022)		
4	PDPC Notification on rules and methods for preparation and maintenance of records of personal data processing activities for the data processor B.E. 2565 (2022)		
5	PDPC Notification on the exemption from maintenance of record obligations of the data controller which is a small		

	organization B.E. 2565 (2022)		
6	Rules of the PDPC re: the Filing, Refusal of Acceptance, Dismissal, Consideration, and Timeframe for the Consideration of the Complaints B.E. 2565		
7	PDPC Notification on rules and methods of personal data breach notification B.E. 2565	7 In the case where there is a necessary reason causing the notification of personal data violation to be delayed by more than seventy-two hours since knowing the cause whether it is due to an initial inspection of the information, necessary action to prevent, stop, or correct the incident of personal data violation, or there are other necessary reasons that cannot be overcome, the Personal Data Controller may request theOffice of the Personal Data Protection Commission to consider exempting the offense from late reporting by...	
8	Notification of the Personal Data Protection Committee Re: Personal Data Protection Officers under Art.41(2) of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
9	Guideline for obtaining consent from data subjects according to the PDPA		
10	Guideline for notifying purposes and		

	details for collecting personal data from the data subjects according to the PDPA		
11	Guideline for Data Controllers and Data Processors: Case Studies from Consultation Concerning Enforcement of the Personal Data Protection Act B.E. 2562		
12	Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020)		
13	Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Applicability of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2564 (2021)		
14	Royal Decree Prescribing Characteristics, Businesses, or Organizations which are Exempted from the Personal Data Protection		

	Act B.E. 2562 (2019) B.E.2566 (2023)		
15	Notification of the Personal Data Protection Committee Re: Security Measures of Personal Data for the Data Controller exempted from the Personal Data Protection Act B.E. 2562 (2019)B.E. 2566 (2023)		
16	Notification of the Personal Data Protection Committee Re: Appropriate Measures for the Collection of Personal Data for the Achievement of the Purpose relating to Research or Statistics under Section 24 (1) and the Scientific, Historical, or Statistic Research Purposes, or other		
17	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.28 of the Personal Data Protection Act		

	B.E. 2562 (2019) B.E. 2566 (2023)		
18	Notification of the Personal Data Protection Committee Re: Criteria for Protection of Personal Data for Cross-border Transfer under Art.29 of the Personal Data Protection Act B.E. 2562 (2019) B.E. 2566 (2023)		
19	Notification of the Personal Data Protection Committee Re: Criteria on the Protection Measures for the Collection of Personal Data relating to Criminal Records which is not carried out under Control of Authorized Official Authority under the Law B.E. 2566		
20	Electronic Transactions Act, B.E. 2544 (2001)		
21	Electronic Transactions Act, No.2 B.E. 2551 (2008)		
22	Electronic Transactions Act, No.3 B.E. 2562 (2019)		
23	Electronic Transactions Act, No.4 B.E. 2562 (2019)		
24	COMPUTER-RELATED CRIME		Section 5 Whoever illegally accesses to a computer system that has specific security

	ACT B.E. 2550 (2007)		measures and such security measures are not intended for his/her use, shall be liable to an imprisonment for a term not exceeding six months, ora fine not exceeding TenThousand Baht or both.
			Section 6 Whoever having knowledge of the security measures to access to a computer system created specifically by another person, wrongfully discloses, without right, such security measures in a manner that is likely to cause damage to another person, shall be liable to an imprisonment for a term not exceeding one year, or a fine not exceeding Twenty Thousand Baht or both.
			Section 7 Whoever illegally accesses to a computer data that has specific security measures which are not intended for his/her use, shall be liable to an imprisonment for a term not exceeding two years, or a fine not exceeding Forty Thousand Baht or both.
			Section 8 Whoever illegally makes, by any electronic means, an interception of computer data of another person that is being transmitted in a computer system and such computer data is not for the benefit of the public or is not available for any other persons to generally utilize, shall be liable to an imprisonment for a term not exceeding three years, or a fine not exceeding Sixty Thousand Baht or both.
			Section 9 Whoever illegally acts in a manner that causes damage, impairment, deletion, alteration or addition either in whole or in part of computer data of another person, shall be liable to an imprisonment for a term not exceeding five years, or a fine not exceeding One Hundred Thousand Baht or both.

			Section 10 Whoever illegally acts in a manner that causes suspension, deceleration, obstruction or interference of a computer system of another person so that it cannot function normally, shall be liable to an imprisonment for a term not exceeding five years, or a fine not exceeding One Hundred Thousand Baht or both.
			Section 11 Whoever sends computer data or an electronic mail to another person while hiding or faking its sources, in a manner that interferes with such another person's normal utilization of the computer system, shall be liable to a fine not exceeding One Hundred Thousand Baht.
25	COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560 (2017)	Section 9. The provisions of section 15 of the Commission of Computer-Related Offences Act, B.E. 2550 (2007) shall be repealed and replaced by the following: Section 15. Any service provider who collaborates in, gives consent to or connives at the commission of an offence under section 14 in a computer system under his control shall be liable to the same penalty as that to be inflicted upon the offender under section 14. The Minister shall issue a Notification prescribing procedures for giving warnings, discontinuing the proliferation of the computer data and removing such computer data from a computer system. If the service provider can prove that he has complied with the Notification of the Minister issued under paragraph two, such person shall not be liable	Section 4. The following provisions shall be added as paragraph two and paragraph three of section 11 of the Commission of Computer-Related Offences Act, B.E. 2550 (2007): "Any person who transmits to another person a computer data or an electronic mail in a manner causing annoyance to the recipient thereof without providing the recipient with an opportunity to discontinue or indicate an intention to refuse acceptance thereof at ease shall be liable to a fine not exceeding two hundred thousand Baht. The Minister shall issue a Notification prescribing the nature and method of transmission as well as the nature and the amount of computer data or electronic mails which do not cause annoyance to recipients and the manner in which discontinuance of acceptance or

			an indication of an intention to refuse acceptance at ease can be made."
			Section 5. The provisions of section 12 of the Commission of Computer-Related Offences Act, B.E. 2550 (2007) shall be repealed and replaced by the following: "Section 12. If the commission of an offence under section 5, section 6, section 7, section 8 or section 13 is the commission against a computer data or a computer system connected with the maintenance of national security, public security, national economic security or an infrastructure involving public interest, the offender shall be liable to imprisonment for a term of one year to seven years and to a fine of twenty thousand Baht to one hundred forty thousand Baht. If the commission of the offence under paragraph one results in damage to such computer data or computer system, the offender shall be liable to imprisonment for a term of one year to ten years and to a fine of twenty thousand Baht to two hundred thousand Baht. If the commission of an offence under section 9 or section 10 is the commission against a computer data or a computer system under paragraph one, the offender shall be liable to imprisonment for a term of three years to fifteen years and to a fine of sixty thousand Baht to three hundred thousand Baht. If the commission of an offence under paragraph one or paragraph three is without any intent to murder but causes death of another person, the offender shall be liable to imprisonment for a term of five years to twenty years and to a

			fine of one hundred thousand Baht to four hundred thousand Baht.
			Section 6. The following provisions shall be added as section 12/1 of the Commission of Computer-Related Offences Act, B.E. 2550 (2007): Section 12/1. If the commission of an offence under section 9 or section 10 causes injury to another person or any property of another person, the offender shall be liable to imprisonment for a term not exceeding ten years and to a fine not exceeding two hundred thousand Baht. If the commission of an offence under section 9 or section 10 is without any intent to murder but causes death of another person, the offender shall be liable to imprisonment for a term of five years to twenty years and to a fine of one hundred thousand Baht to four hundred thousand Baht
			Section 8. The provisions of section 14 of the Commission of Computer-Related Offences Act, B.E. 2550 (2007) shall be repealed and replaced by the following: Section 14. Any person who commits any of the following offences shall be liable for imprisonment for a term not exceeding five years or to a fine not exceeding one hundred thousand Baht or to both: (1) dishonestly or by deceit, bringing into a computer system a computer data which is distorted or fake, whether in whole or in part, or a computer data which is false, in a manner likely to cause loss to the public, where it is not the commission of an offence of defamation under the Penal Code;

			(2) bringing into a computer system a computer data which is false in a manner likely to cause loss to the maintenance of national security, public security, national economic security or an infrastructure involving national public interest or in a manner causing public anxiety; (3) bringing into a computer system any computer data which constitutes an offence relating to security of the Kingdom or an offence relating to terrorism under the Penal Code; (4) bringing into a computer system any computer data of a pornographic nature, provided that such computer data is accessible by the general public; (5) disseminating or forwarding a computer data with the knowledge that it is a computer data under (1), (2), (3) or (4). If the offence under paragraph one (1) is not committed against the public but is committed against any particular person, the perpetrator, the disseminator or the forwarder of the such computer data shall be liable for imprisonment for a term not exceeding three years or to a fine not exceeding sixty thousand Baht or to both and the offence shall be a compoundable offence.
			Section 10. The provisions of section 16 of the Commission of Computer-Related Offences Act, B.E. 2550 (2007) shall be repealed and replaced by the following: "Section 16. Any person who brings into a computer system accessible by the public a computer data which appears to be a photograph of another person, where such photograph has been created, edited, supplemented or modified by an electronic means

			or any other means, in a manner likely to cause that other person to be defamed, insulted, hated or embarrassed shall be liable for imprisonment for a term not exceeding three years and to a fine not exceeding two hundred thousand Baht. If the act under paragraph one is committed against a photograph of the deceased and such act is likely to cause the deceased's parent, spouse or child to be defamed, insulted, hated or embarrassed, the perpetrator shall be liable to the same penalty as that provided in paragraph one. If the act under paragraph or paragraph two subsists inthe bringing into a computer system in good faith, which constitutes a fair comment on any person or matter which is ordinarily made by a member of the public, the perpetrator shall not be guilty. The offences under paragraph one and paragraph two are compoundable offences. If the injured person for the offence under paragraph one or paragraph two dies before making a complaint, the parent, spouse or child of the injured person shall be entitled to make a complaint and shall be deemed to be the injured person
			Section 11. The following provisions shall be added as section 16/1 and section 16/2 of the Commission of Computer-Related Offences Act, B.E. 2550 (2007): Section 16/1. In a case involving an offence under section 14 or section 16, the Court, when a

			judgment is rendered for convicting the accused, may give an order: (1) requiring destruction of the data under such section; (2) requiring publication or dissemination of the judgment in whole or in part via electronic media, radio broadcasting, radio and television broadcasting, newspapers or any other media as the Court deems appropriate, provided that the costs incurred in the publication or dissemination shall be borne by the accused; (3) requiring other action as the Court deems appropriate in mitigation of loss resulting from the commission of such offence. Section 16/2. Ant person who knows that the computer data in his possession is the data ordered by the Court to be destroyed under section 16/1 shall destroy such data, failing which such person shall be liable to one half of the penalty provided under section 14 or section 16, as the case may be
26	Notification of Ministry of Digital Economy and Society Re: characteristics and methods of sending of information, and the characteristics and quantity of information, frequency and method of transmission. which does not cause annoyance to the recipient, B.E. 2560 (2017)		-
27	Notification of Ministry of Digital		Section 4 4 If the following service

	Economy and Society Re: Notification process, Suppression of the proliferation of computer information and removal of computer data from computer systems B.E 2560 (2017)		providers can prove that they have complied with the following announcements, that service provider You will not be punished for cooperating. give consent or know and understand, which Committing an offense according to Section 15 *(of the COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560)* (1) service provider as an intermediary (Intermediary) which provides computer data transmission services Through the network or computer system of the service provider or service facilitating transmission computer data through computer traffic routes on the Internet (routing) or providing computer services Computer equipment or computer network systems to cause the transmission of computer data ...(continue)...
			Section 5 Service providers according to Item 4 who prove that they have prepared the following measures: to notify and suspending the dissemination or removal of such computer data from the computer system will not be punished according to Section 15 *(of the COMPUTER-RELATED CRIME ACT (NO. 2), B.E. 2560)* (1) Notification procedure The service provider must provide notification measures by preparing a written notice (Take Down Notice) by using any technical means or means to notify the service provider to suspend. The dissemination or deletion of illegal computer data from computer systems under its control. The service provider's notification letter must include the following information: Let the general public know ...(continue)...

28	Notification of Ministry of Digital Economy and Society Re Criteria, timelines, and procedures for suspending proliferation. or delete computer data of officials or service providers, B.E 2560 (2017)		
29	Notification of Ministry of Digital Economy and Society Re: Criteria for maintaining computer traffic data of service providers B.E. 2564 (2021)		
30	The Special Case Investigation Act B.E. 2547 (2004)		
31	The Special Case Investigation Act (No.2) B.E. 2551 (2008)		Section 39.Any person who violates Section 26 shall be subjected to imprisonment from three to five years or a fine from sixty thousands up to one hundred thousand baht, or both. Should an offence under paragraph one be committed by Special Case Inquiry Officials, Special Case Officers, Public Prosecutors or Military Prosecutors who join the investigation or who join the operation under Section 32, or by persons who jointly perform duty according to Section 22/1, or Section 25, the offender shall be subjected to three times of the punishment provided in paragraph one
32	The Emergency Decree on Public Administration in a State of		Section 18. Any person who violates a Regulation, Notification or order issued under section 9, section 10, section 11, or section

	Emergency B.E. 2548 (2005)		13 shall be liable to imprisonment for a term not exceeding two years or to a fine not more than forty-thousand baht, or to both.
33	The Notification of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications B.E.2566 (2023)		
34	Guideline of the National Telecommunications Commission Re: Measures to Protect Telecommunications Users, Data Privacy, Privacy Rights and Freedom of Communications		22. Administrative enforcement measures and penalties 22.1 In the case that the person 1 receives a violating license or does not comply with the NBTC announcement, the Secretary-General of the NBTC has the authority According to the Telecommunications Business Act of 2001, license recipients are ordered to stop violating the rules. or fix 1 update or perform1 correctly or appropriately within a specified period of time1 in the event that the license recipient does not5 comply with such orders5 and P1 determines the time period for appeals or the NBTC decides to uphold With that order, when the Secretary-General of the NBTC receives a warning letter and there is still no compliance with the order, the Secretary-General of the NBTC will consider determining the administrative fine according to the law. 1 with administrative procedures which must not be less than 20,000 baht per 5 days, and if the license recipient still ignores it, the NBTC has the power to suspend or revoke the license. ...(continue)...

35	The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023)		
36	The Credit Information Business Operation Act B.E. 2545 (2002)	Section 39 The Minister shall, with the recommendation of the Committee, have the power to suspend or revoke the license to operate credit information business of a credit information company, when it appears that: (1) The credit information company operates business dishonestly or may cause damage to the public. (2) The credit information company deliberately omits to do any act, or violates a prohibition, prescribed by law. (3) The credit information company deliberately violates or fails to comply with the rules, procedures or conditions prescribed by the Minister or the Committee under this Act.	Section 43 Whoever violates Section 9, Section 14, or Section 15 shall be punished with imprisonment from five to ten years, or a fine not exceeding five hundred thousand baht, or both.
		Section 40 Upon the Minister having revoked the license to operate credit information business of any credit information company, the Committee shall have the power to prescribe in its notification the rules, procedures and conditions concerning management of information of the said credit information company.	Section 45 Whoever violates Section 11 shall be punished with imprisonment not exceeding one year, or a fine not exceeding one hundred thousand baht, or both.
		Section 42 Any credit information company which fails to comply with Section 7, Section 8 or Section 16 shall be punished with a fine not exceeding three hundred thousand baht, and a further daily fine not exceeding ten thousand baht throughout the period of violation or until compliance.	Section 53 If any person or committee member or sub-committee member, by learning information of any person as provided in Section 23 or from performing duties under this Act, discloses such information to other persons, such person shall be punished with imprisonment from five to ten years, or a fine not exceeding five hundred thousand baht, or

			both. The provisions of paragraph one shall not apply to a disclosure in the following cases: (1) Disclosure under one's duties; (2) Disclosure for the benefit of investigation or court trial; ...(continue)...
		Section 44 Any credit information company, information controller or information processor that violates Section 10 or Section 12 shall be punished with imprisonment from five to ten years, or a fine not exceeding five hundred thousand baht, or both.	Section 58 Whoever fails to comply with a notification or order of the Committee under Section 30 (1), (2), (3) or (4) or Section 34 shall be punished with imprisonment not exceeding one month, or a fine not exceeding ten thousand baht, or both.
		Section 46 Any credit information company, information controller, or information processor that violates Section 13 shall be punished with a fine not exceeding three hundred thousand baht, and a further daily fine not exceeding ten thousand baht throughout the period of violation or until compliance.	Section 60 Whoever tampers with the information in the memory system of the computer of a credit information company, member, service user or information subject, or gathers, changes, discloses, deletes, or destroys the information in the memory system of such computer illegally, or without permission from the authorized person concerned, shall be punished with imprisonment from five to ten years, or a fine not exceeding five hundred thousand baht, or both.
		Section 47 Any credit information company or information processor that fails to comply with Section 17, paragraph one, or fails to comply with the rules, procedures and conditions prescribed by the Committee under Section 17, paragraph two, shall be punished with a fine not exceeding three hundred thousand baht, and a further daily fine not exceeding ten thousand baht throughout the period of violation or until compliance	Section 61 Any committee member, manager, employee, or person who is responsible for the operations of a credit information company or information controller or information processor and who acts or omits to act so as to seek undue benefit under the law for oneself or others, which causes damage to others or the information subject, shall be punished with imprisonment from five to ten years, or a fine not exceeding five hundred thousand baht, or both.
		Section 49 Any member that conceals or gives incorrect	Section 62 If there appears a commission of any offence under

		information of its customer to the credit information company shall be punished with a fine not exceeding three hundred thousand baht, and a further daily fine not exceeding ten thousand baht throughout the period of violation or until compliance.	this Act, it shall be regarded that the Bank of Thailand is an injured person under the Criminal Procedure Code, and, in such criminal case, the public prosecutor shall have the power to claim property or price or compensation for damage on behalf of the information subject or the actual injured person. In this instance, the provisions governing filing of civil cases in connection with an offence under the Criminal Procedure Code shall apply mutatis mutandis. The provisions of this Section shall not prejudice the right of the information subject or the actual injured person to file a lawsuit or to take any legal action against the offender.
		Section 52 Any service user that violates or fails to comply with Section 22 shall be punished with imprisonment from five to ten years, or a fine not exceeding five hundred thousand baht, or both	
		Section 54 Any credit information company, information controller, information processor, member or service user or any person who violates Section 24 shall be punished with imprisonment from five to ten years, or a fine not exceeding five hundred thousand baht, or both.	
		Section 55 Any credit information company or member that fails to comply with Section 26 shall be punished with a fine not exceeding three hundred thousand baht, and a further daily fine not exceeding ten thousand baht throughout the period of violation or until compliance.	
		Section 56 Any credit information company, financial institution, member or service user that fails to comply with	

		Section 27 shall be punished with a fine not exceeding three hundred thousand baht, and a further daily fine not exceeding ten thousand baht throughout the period of violation or until compliance.	
37	The Credit Information Business Operation Act No.2 B.E. 2549 (2006)	Section 48 Any member that fails to send information of its customers to the credit information company of which it is a member shall be punished with a fine not exceeding five hundred thousand baht, and a further daily fine not exceeding ten thousand baht throughout the period of violation or until compliance. Any member that fails to notify its customers of the information sent to the credit information company, or fails to notify within the prescribed period under Section 18, or fails to comply with the rules, procedures and conditions prescribed by the Committee under Section 18 shall be punished with imprisonment not exceeding one year, or a fine not exceeding one hundred thousand baht, or both.	
38	The Credit Information Business Operation Act No.3 B.E. 2551 (2008)		
39	The Credit Information Business Operation Act No.4 B.E. 2559 (2016)		
40	The Credit Information Business Operation Act No.5 B.E. 2559 (2016)		Section 64 In the case where an offender is a juristic person, if the offence committed came from the order or act of the director, the manager or any other person responsible for the operation of the juristic person, or in case such person has duties to order or act and omits

			to order or act such that the juristic person commits such offence, such person shall also be liable to the penalty prescribed for such offence.
41	The Credit Information Business Operation Act No.6 B.E. 2565 (2022)	Section 50 Any member that fails to comply with Section 19 (2), (3), (4) or (5) or violates or fails to comply with the rules, procedures and conditions prescribed in Notifications issued by the Committee under Section 19, paragraph two, Section 20/1, paragraph four or Section 24/3, paragraph four shall be liable to a fine not exceeding three hundred thousand baht and to additional fine at a daily rate not exceeding ten thousand baht throughout the period of violation or until due compliance. Any member in the category of financial institutions that fails to comply with Section 20/1, paragraph one or paragraph two or violates or fails to comply with the rules, procedures and conditions prescribed in Notifications issued by the Committee under Section 20/1, paragraph three shall be liable to the same punishment provided in paragraph one. Any member in the category of credit intermediaries that fails to comply with Section 24/2 or Section 24/3, paragraph one or paragraph two or violates or fails to comply with the rules, procedures and conditions prescribed in Notifications issued by the Committee under Section 24/2 or Section 24/3, paragraph three shall be liable to the same punishment provided in paragraph one.	
		Section 51 Any credit information company or information processor that discloses or provides information to its members or	

		the service users for other purposes, or discloses or provides information to persons other than those prescribed in Section 20 or Section 24/1 shall be liable to imprisonment for a term not exceeding three years or to a fine not exceeding three hundred thousand baht or to both.	
		Section 57 Any financial institution, member or service user that fails to comply with Section 24/4 or Section 28 shall be liable to a fine not exceeding three hundred thousand baht and to additional fine at a daily rate not exceeding ten thousand baht throughout the period of violation or until due compliance.	
42	The Child Protection Act B.E. 2546 (2003)		Section 79. Any person who violates section 27, section 50, or section 61 shall be liable to imprisonment for a term of not exceeding six months or to a fine not exceeding sixty thousand baht or to both.
			Section 80. Any person who obstructs a Competent Official in the performance of his or her duties under section 30 (1) or (5), or refuses to submit documents or knowingly submits documents which are false to a Competent Official when is being called for under section 30 (4) shall be liable to imprisonment for a term of not exceeding one month or to a fine not exceeding ten thousand baht or to both. Any person who fails to appear to give a statement, refuses to give a statement without reasonable ground, or gives false statements to the Competent Official which performs his or her duty under section 30 (3) shall be liable to imprisonment for a term of not exceeding one month or to a fine not exceeding ten thousand baht or to both. However, if the person giving a

			statement reverses his or her position by providing a true statement before the testimony is over, the criminal proceedings against such person shall be withheld.
43	The National Health Act B.E. 2550 (2007)		Section 49. Any person violates section 7 or section 9 shall be liable to an imprisonment for a term not exceeding six months, or to a fine not exceeding ten thousand Baht, or to both. An offence under this section is a compoundable offence.
44	The Payment System Act B.E. 2560 (2017)		Section 47. Any person who violates or fails to comply with Section 33 or Section 34 shall be subject to imprisonment for a term of not exceeding one year or a fine of not exceeding one hundred thousand baht or both.
			Section 53. Any person who damages, destroys, conceals, takes away, causes the loss or renders useless any property or document which the examiner seized, attached, kept or ordered to be sent as evidence or for enforcement of law, whether the examiner has kept such property or document by himself or ordered such person or other person to send or to keep it, shall be liable to imprisonment for a term of six months to three years or a fine of sixty thousand baht to three hundred thousand baht or both.
			Section 54 Any person, in the performance under the authorities and duties provided by law, or in giving assistance to the person performing under the authorities and duties provided by law, having acquired knowledge about the affairs of a business provider which under normal circumstances should not be disclosed, reveals such knowledge to other person, shall be liable to imprisonment for a term of not exceeding one year

			or a fine of not exceeding one hundred thousand baht or both. The provisions of the first paragraph shall not apply to the disclosure in the following cases: (1) disclosure in the performance of duty or for the purposes of investigation or court proceedings; (2) disclosure relating to the commission of an offence under this Act; (3) disclosure to agencies in the country and foreign country which have the authorities and duties to supervise such business provider; (4) disclosure for the purposes of performance of duty by the agencies in the country and foreign country which have the authorities and duties to supervise such business provider according to an agreement made; (5) disclosure for the purposes of improving the standing of the operation of such business provider; (6) disclosure of confidential information of the service users upon consent of such services users ; (7) disclosure for the purposes of compliance with the provisions of law.
			Section 55. Any person who knows or acquired confidential information of a business provider because such person has the power of management or is an officer or employee of the business provider and discloses such confidential information in a manner likely to cause damage to other person or the public, shall be liable to imprisonment for a term of not exceeding one year or a fine of not exceeding one hundred thousand baht or both. The provision of the first

			paragraph shall not apply to the disclosure in cases under the second paragraph of Section 54.
			Section 56. In the case where an offender is a juristic person, if the commission of an offence of such juristic person caused by an order or action of a director, manager, or any person responsible for its operations, or where the person has a duty to issue an order or to take action and fails to do so which thereby causes the juristic person to have committed the offence, such person shall also be liable to the penalties specified for such offence as well.
45	The Notification of the Bank of Thailand SorGorSor2. 4/2563 re: Market Conduct Rules		
46	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Life Insurance Policy for Sale and the Performing of Duty of Life Insurance Agent, Broker and Bank B.E. 2563 (2020)	Chapter 9 Violation or Non-compliance of this Notification Clause 39 In the case of a Company's violation of or non-compliance with the criteria, procedures, and conditions under this Notification, the Office is empowered to proceed as follows: (1) issuing an order commanding the Company to restore its compliance with this Notification within a period specified by the Office; (2) issuing an order commanding the Company to pursue any act or omission, if it appears that the Company has failed to pursue the restoration as required under (1) without justifiable reason, or has deliberately committed a violation of or non-compliance with this Notification.	
		Clause 40 In the case a Life Insurance Agent's, Life Insurance Broker's, or a Bank's violation of or non-compliance with the	

		criteria, procedures, and conditions prescribed by this Notification, the Registrar is empowered to issue an order commanding the Life Insurance Agent, Life Insurance Broker, or Bank, to undertake any act, omission or rectification of such non-compliance within a period specified by the Registrar. ...(continue)...	
		Clause 41 In the case where any person's violation of or non-compliance with the criteria, procedures, and conditions prescribed in this Notification constiutes a punishable offense, the Office shall take actions against the violating or non-complying person in accordance with the law on life insurance.	
47	The Notification of the Office of Insurance Commission Re: Rules, Methods for Issuing and Offering of Non-life Insurance Policy for Sale and the Performing of Duty of Non-life Insurance Agent, Broker and Bank B.E. 2563 (2020)	Chapter 9 Violation or Non-compliance of this Notification Clause 37 In the case of a Company's violation of or non-compliance with the criteria, procedures, and conditions under this Notification, the Office is empowered to proceed as follows: (1) issuing an order commanding the Company to restore its compliance with this Notification within a period specified by the Office; (2) issuing an order commanding the Company to pursue any act or omission, if it appears that the Company has failed to pursue the restoration as required under (1) without justifiable reason, or has deliberately committed a violation of or non-compliance with this Notification.	
		Clause 38 In the case a Non-life Insurance Agent's, Non-life Insurance Broker's, or a Bank's violation of or non-compliance with the criteria, procedures, and conditions prescribed by this Notification, the Registrar is empowered to issue an order	

		commanding the Non-life Insurance Agent, Non-life Insurance Broker, or Bank, to undertake any act, omission or rectification of such non-compliance within a period specified by the Registrar. ...(continue)...	
		Clause 39 In the case where any person's violation of or non-compliance with the criteria, procedures, and conditions prescribed in this Notification constiutes a punishable offense, the Office shall take actions against the violating or non-complying person in accordance with the law on non-life insurance.	
48	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Life Insurance Business B.E. 2564 (2021)		
49	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Non-life Insurance Business B.E. 2564 (2021)		
50	The Notification of the Office of Insurance Commission Re: Personal Data Protection Guideline for Loss Adjuster Business B.E. 2564 (2021)		
51	Trade Secret Act B.E. 2545 (2002)		Section 11 Where the controller of trade secrets files an action

			for injunction under Section 8(2), and the court finds infringement of trade secrets but there are special circumstances where injunction should not be granted, the court may order the infringer to pay appropriate compensation to the controller of trade secrets and set appropriate time period for the use. In case where the court grants an injunction under Section 8(2) stopping further infringement of the trade secrets, and if at a later stage, the trade secrets have been disclosed to the public or have ceased to be trade secrets, the person enjoined by the court can file a petition to have the order rescinded. In an action for injunction under Section 8(2), the controller of trade secret may request the court to order the destruction or confiscation of materials, apparatus, tools or other equipments used in the infringement of trade secrets. The products that are manufactured by the infringement of trade secrets and are still vested in the ownership of the infringer shall be vested with the State or with the controller of trade secrets as so ordered by the court. In case where the possession of such product is illegal, the court may order its destruction.
			Section 13 In determining the measure of damages where an action under Section 8 (2) has been filed, the court is empowered to apply the following rules: (1) In addition to the damages for the actual damage suffered, the court may include in the damages for the plaintiff, account of profits accrued from or in connection with the infringement by the infringer.

			(2) In case where the court is unable to measure the damages under (1), it may order such amount of damages to the controller of trade secrets, as it deems appropriate. (3) In case where there is clear evidence that the infringement of trade secrets is conducted willfully or maliciously causing the trade secrets to cease the quality of secrecy, the court is empowered to order the infringer to pay punitive damages in addition to the amount of damages granted under (1) and (2). However, the punitive damages shall not exceed two times the amount of damages under (1) or (2).
			Section 33 Whosoever discloses a trade secret of other person to the public in the manner which causes the trade secret to cease as a secret, with malicious intent to cause damage to the business of the controller of trade secrets, whether by publication through documents, audio or video broadcasting, or disclosure by any other means, shall be liable to imprisonment not exceeding one year or fine not exceeding two hundred thousand baht, or both.
			Section 36 If the offender is a legal entity and the offence is committed through the instruction, act, non-instruction or omission that is the duty of the director, manager, or any person responsible for the management of the legal entity, such person shall be subject to the liability prescribed for such offence
			Section 37 The offence under Section 33 and Section 36 is a compoundable offence.
			Section 38 The Board has the authority to settle the offence under Section 33 and Section 36

			by imposing a fine on the offender. In this respect the Board shall have the power to assign a sub-board, the Director-General, an inquiry official, or a competent officer to settle the offence by stipulating settlement rules or conditions for the assignee, as it deems appropriate. Subject to paragraph one, if the inquiry official in an investigation finds that a person commits an offence under this Act and such person consents to settle the offence, the inquiry official shall forward the matter to the Board or the person assigned by the Board for settlement within seven days from the date that such person expresses his consent to settle. Upon payment of a fine in the amount stipulated in the settlement within the prescribed period, the case shall be considered closed in accordance with the Criminal Procedure Code. If the offender does not consent to the settlement, or after the consent, he fails to pay the fine within the prescribed period, the case shall proceed.
52	Trade Secret Act (No.2) B.E. 2558 (2015)		Section 34. Any person, by his or her position to maintain trade secrets in accordance with the rules prescribed under Section 15 paragraph one, unlawfully disclosing or using such trade secrets for his or her or other persons' benefits, shall be liable to imprisonment for a term of not more than two years or a fine not exceeding two hundred thousand baht, or both.
			Section 35.Any person disclosing certain facts concerning the business of the controller of trade secrets which should normally be kept confidential and which he or she has

			obtained or known in the course of the performance of duties under this Act, shall be liable to imprisonment for a term not exceeding one year or a fine not exceeding one hundred thousand baht, or both, except for disclosure in the course of an official duty or for the purpose of an investigation or legal proceedings. Any person obtaining or knowing certain facts from the person under paragraph one in the course of an official duty or investigation or legal proceedings, discloses such facts shall be similarly liable. Whosoever discloses facts, which have been obtained or aware of as a result of his engagement in official duty, investigation or legal proceedings shall be subject to the same liability.

J) Viet Nam

Legal System Overview

#	Regulation	Translation	Purpose of the Legal System
			What purpose does the legal system serve?(e.g. cybersecurity)
		Google translation or Translation by certain organization	
1	Decree No. 13/2023/ND-CP) (PDPD : Personal Data Protection Decree)	Translation by certain organization	This Decree provides for personal data protection and responsibilities of relevant agencies, organizations and individuals for protection of personal data.
2	Law on Cyber-information Security No.86/2015/QH13	Translation by certain organization	This Law prescribes cyberinformation security activities, and rights and responsibilities of agencies, organizations and individuals in ensuring cyberinformation security; civil cryptography; standards and technical regulations on cyberinformation

			security; trading in the field of cyberinformation security; development of human resources for cyberinformation security; and state management of cyberinformation security.
3	Law on Cybersecurity 24/2018/QH14	Google translation	This Law regulates activities of protecting national security and ensuring social order and safety in cyberspace; and the responsibilities of agencies, organizations and individuals involved. Domestic and foreign companies providing telecommunications networks and internet-based services and value-added services in cyberspace in Viet Nam. The law was passed in June 2018 and came into force in January 2019. The law consists of seven chapters and 47 articles and provides for the security of critical information related to security, the prevention of acts that compromise network security, and the implementation of data and network protection. The Act includes obligations for critical information system managers to store data in-country and to conduct safety assessments when providing (taking) data out of the country, which covers personal data and critical data. It also obliges foreign telecommunications and internet service providers to set up servers and offices in the country for the data of users in Vietnam. Translated with DeepL.com (free version)
4	Decree No. 53/2022/ND-CP	Google translation	The Act regulates Data Localisation obligations for domestic and foreign operators providing online services in Viet Nam. It applies to personal data of service users as well as non-personal data such as data

			created by service users (e.g. user account names, duration of service use, etc.).
5	Law on Information Technology No.67/2006/QH11	Google translation	The PCR Law 2023 defines a consumer as a person who purchases and/or uses products, goods or services for consumption or daily life purposes of a person, a household or an organisation, and not for a commercial purpose. Under this definition, consumers do not include persons purchasing and/or using goods, services or products for any commercial purpose.
6	the Law on Protection of Consumer Rights No. 19/2023/QH15	Google translation	Article 1. Scope of regulation This Law provides principles of and policies on protection of consumer rights; rights and obligations of consumers; responsibilities of business organizations and individuals toward consumers; activities of agencies and organizations to protect consumer rights; settlement of disputes between consumers and business organizations and individuals; and state management of protection of consumer rights.
7	Decree regarding e-commerce, No.85/2021/NDCP	Google translation	The current Decree No. 52/2013/ND-CP (hereinafter referred to as "Decree 52") is the current regulation on cross-border e-commerce. Decree No. 85/2021/NDCP ("Decree No. 85"), which amends and supplements Decree No. 52, was enacted on 25 September 2021 and was enacted on 25 September 2021 and is scheduled to enter into force on 1 January 2022. It stipulates Data Localisation obligations for domestic and foreign operators providing online services in Vietnam. In addition to personal data of service users, it also applies to non-personal data such as data created by service users (e.g.

			user account names, duration of service use, etc.). Translated with DeepL.com (free version)
8	Law on 86/2015/QH13	Google translation	The law consists of eight chapters and 54 articles and was enacted to address issues such as personal data protection, spam and inappropriate information distribution.
9	Decree 27/2018/ND-CP	Google translation	Decree 27 intends to create an investment environment that will increase online activities ranging from online gaming, social networks and website creation. At the same time, it will regulate the management of social network sites.
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information	Google translation	It regulates internet services and online information and plays a key role in governing important services such as social networks, online games and information aggregation sites, as well as important matters such as domain names and online information security. Given the rapid pace of development in these areas, Decree 72, which has been in force for nearly a decade, needs updating.
11	Law No. 91/2015/QH13	Google translation	The Civil Code provides the legal status, legal standards for the conduct of natural and juridical persons; the rights and obligations of natural and juridical person (hereinafter referred to as persons) regarding personal and property rights and obligations in relations established on the basis of equality, freedom of will, independence of property and self-responsibility (hereinafter referred to as civil relations).
12	Law on Inspection No. 56/2010/QH12	Google translation	

#	Regulation	Form of legal system	Target Business
		Is it introduced in accordance with government ordinances and guidelines? (Is it introduced in a format that ensures lead time?)	Does the law target specific industry or in general? Is it clearly stated in the regulations?
		Regulation level	Industry
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)	Law	General
2	Law on Cyber-information Security No.86/2015/QH13	Law	General
3	Law on Cybersecurity 24/2018/QH14	Law	A domestic and international company that provides telecommunications networks, Internet-based services and value-added services in cyberspace in Vietnam.
4	Decree No. 53/2022/ND-CP	Subordinate Laws and Guidelines	A domestic and international company that provides telecommunications networks, Internet-based services and value-added services in cyberspace in Vietnam.
5	Law on Information Technology No.67/2006/QH11	Law	Telecom sector
6	the Law on Protection of Consumer Rights No. 19/2023/QH15	Law	consumer
7	Decree regarding e-commerce, No.85/2021/NDCP	Subordinate Laws and Guidelines	e-commerce
8	Law on 86/2015/QH13	Law	General
9	Decree 27/2018/ND-CP	Subordinate Laws and Guidelines	General
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the	Subordinate Laws and Guidelines	General

	management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13	Law	
12	Law on Inspection No. 56/2010/QH12	Law	

#	Regulation	Regulatory authority	Jurisdiction
		Which regulatory authority has jurisdiction over regulation?	Cyber security, data security, personal information protection, etc.
		Name of ministry/organization	Similar to purpose?
1	Decree No. 13/2023/ND-CP) （PDPD：Personal Data Protection Decree)	Personal Data Protection Commissioner	personal information protection
2	Law on Cyber-information Security No.86/2015/QH13	Personal Data Protection Commissioner	Cyber information security
3	Law on Cybersecurity 24/2018/QH14	Personal Data Protection Commissioner	Cyber security
4	Decree No. 53/2022/ND-CP	Personal Data Protection Commissioner	Data Localization
5	Law on Information Technology No.67/2006/QH11	Personal Data Protection Commissioner	Protection of Intellectual Property Rights
6	the Law on Protection of Consumer Rights No. 19/2023/QH15	Personal Data Protection Commissioner	consumer rights protection
7	Decree regarding e-commerce, No.85/2021/NDCP	MOIT	
8	Law on 86/2015/QH13		Network Information Security
9	Decree 27/2018/ND-CP	the Ministry of Information and Communications (the Authority	data security

		of Broadcasting and Electronic Information)	
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information	the Ministry of Information and Communications (MIC)	data security
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation	Status	Citation
		Legislation / Public Comment / Passage / Enforcement / Amendment, etc.	
		Status of the regulation: Draft = drafting (new regulation) published = published in the gazzette but not yet enacted Enact = published in the gazzette and already enacted Amendment = enacted regulation being on amending process	URL
1	Decree No. 13/2023/ND-CP （PDPD： Personal Data Protection Decree）	Enact	
2	Law on Cyber-information Security No.86/2015/QH13	Enact This Law takes effect on July 1, 2016.	https://www.economica.vn/Content/files/LAW%20%26%20REG/86_2015_QH13%20Law%20on%20Cyberinformation%20Security.pdf
3	Law on Cybersecurity 24/2018/QH14	Enact	https://www.economica.vn/Content/files/LAW%20%26%20REG/Law%20on%20Cyber%20Security%202018.pdf
4	Decree No. 53/2022/ND-CP	Enact	https://thuvienphapluat.vn/van-ban/EN/Cong-nghe-thong-tin/Decree-53-2022-ND-CP-elaborating-the-Law-on-

			cybersecurity-of-Vietnam/527750/tieng-anh.aspx
5	Law on Information Technology No.67/2006/QH11	Enact	https://www.global-regulation.com/translation/vietnam/6608663/law-67-2006-qh11%253a-information-technology.html
6	the Law on Protection of Consumer Rights No. 19/2023/QH15	Enact	https://www.tilleke.com/insights/significant-aspects-of-vietnams-new-consumer-protection-law/
7	Decree regarding e-commerce, No.85/2021/NDCP	Enact	https://english.luatvietnam.vn/decree-no-85-2021-nd-cp-dated-september-25-2021-of-the-government-amending-and-supplementing-a-number-of-articles-of-the-governments-decree-no-53-210029-doc1.html
8	Law on 86/2015/QH13	Enact	https://vbpl.vn/TW/Pages/vbpqen-toanvan.aspx?ItemID=11048
9	Decree 27/2018/ND-CP	Enact	https://vnnic.vn/sites/default/files/vanban/decree_no._27.2018.nd-cpof1march2018.pdf
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information	Enact	https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/vn/vn133en.pdf
11	Law No. 91/2015/QH13		https://vietanlaw.com/the-law-no-91-2015-qh13/
12	Law on Inspection No. 56/2010/QH12		https://vbpl.vn/TW/Pages/vbpqen-toanvan.aspx?ItemID=10730

Definitions for basic items

#	Regulation	Type and Scope of Data	Data processing and handling
		Personal data, personal information/sensitive and important data/children and minors' data, etc. Is the scope of data clearly written in the regulations? What are the unclear points?	Processing, handling / disclosure, sharing, provision, transmission, outsourcing / use for advertising, etc.
		Specific type of data required to complied with the regulation	Provision for data processing

1	Decree No. 13/2023/ND-CP) (PDPD : Personal Data Protection Decree)	2. “Information used for identification of an individual" refers to information that results from an individual's activities and may identify an individual when it is combined with other stored information and data. 3. "General personal data" includes: a) Last name, middle name and first name, other names (if any); b) Date of birth; date of death or going missing; c) Gender; d) Place of birth, registered place of birth; place of permanent residence; place of temporary residence; current place of residence; hometown; contact address; dd) Nationality; e) Personal image; e) Phone number; ID Card number, personal identification number, passport number, driver’s license number, license plate, taxpayer identification number, social security number and health insurance card number; h) Marital status; i) Information about the individual’s family relationship (parents, children); k) Digital account information; personal data that reflects activities and activity history in cyberspace; l) Information associated with an individual or used to identify an individual other than that specified in Clause 4 of this Article. 4. “Sensitive personal data” refers to personal data in association with individual privacy which, when being infringed, will directly affect an individual's legal rights and interests, including: a) Political and religious opinions;	7. “Personal data processing” refers to one or multiple activities that impact on personal data, including collection, recording, analysis, confirmation, storage, rectification, disclosure, combination, access, traceability, retrieval, encryption, decryption, copying, sharing, transmission, provision, transfer, deletion, destruction or other relevant activities.

		b) Health condition and personal information stated in health record, excluding information on blood group; c) Information about racial or ethnic origin; d) Information about genetic data related to an individual's inherited or acquired genetic characteristics; dd) Information about an individual's own biometric or biological characteristics; e) Information about an individual's sex life or sexual orientation. g) Data on crimes and criminal activities collected and stored by law enforcement agencies; h) Information on customers of credit institutions, foreign bank branches, payment service providers and other licensed institutions, including: customer identification as prescribed by law, accounts, deposits, deposited assets, transactions, organizations and individuals that are guarantors at credit institutions, bank branches, and payment service providers; i) Personal location identified via location services; k) Other specific personal data as prescribed by law that requires special protection.	
2	Law on Cyber-information Security No.86/2015/QH13	Article 3. Interpretation of terms In this Law, the terms below are construed as follows: 15. Personal information means information associated with the identification of a specific person. 16. Owner of personal information means a person identified based on such information. 17. Processing of personal information means the performance of one or some operations of collecting, editing, utilizing, storing, providing, sharing or spreading personal	

		information in cyberspace for commercial purpose.	
3	Law on Cybersecurity 24/2018/QH14	Article 21. Collect, process and use personal information on network environment 1. Individual organizations collect, process and use the personal information of other people on the network environment must be that person agrees, unless otherwise specified by law. 2. organizations and individuals collect, process and use the personal information of others responsibly: a) inform that person about the form, scope, place and purpose of the collection, processing and use of personal information of that person; b) use purpose of personal information properly collected and stored the information in a certain period of time as prescribed by the law or by agreement between the two parties; c) to conduct technical, management measures needed to ensure your personal information is not lost, stolen, disclosed, altered or destroyed; d) proceed immediately the necessary measures when get request to check back, or cancelled in accordance with paragraph 1 Article 22 of this law; not provided or use the relevant personal information until it was revised again. 3. organizations and individuals have the right to collect, process and use the personal information of another person without that person's consent in the event that personal information is used for the following purposes: a) signed, modify or execute a contract to use the information, product , service on network environment;	

		b) Computer reviews, cost of use of the information, products or services on the network environment; c) perform other duties specified by law. Article 22. Archive, provides personal information on network environment 1. Individuals have the right to request personal organizer, personal information stored on their network environment to perform the test, or remove such information. 2. organizations and individuals are not provided in other people's personal information to third parties, except as otherwise specified by law or consent of that person. 3. the individual has the right to request compensation for damage caused by violation of the provision of the personal information. Article 23. Establish electronic information page 1. The Organization, individuals have the right to establish electronic information page under the provisions of the law and is responsible for managing the content and operation of electronic information page. 2. organizations and individuals who use the national Vietnam domain name ".vn" when setting up the electronic information page without notice with the Ministry of posts and telecommunications. Individual organization when setting up electronic information page does not use the national Vietnam domain name ".vn" is announced on the network environment of postal and telecommunications Ministry with the following information: a) institution name recorded in the establishment decision, active license, registration certificate or	

		business license to open a representative office; personal names; b) Number, date of issue, where the level of people's ID or number, date of issue, issuing personal passport; c) addresses the Organization's headquarters or place of permanent residence of the individual; d) phone numbers, fax numbers, electronic mail address; DD) The registered domain name. 3. organizations and individuals to be responsible before the law for the accuracy of the information specified in paragraph 2 of this article, when the information changes, then have to inform about the changes. 4. electronic information Page is used for the operation of the press must be made to the provisions of this law, the law on the press and the other provisions of the relevant laws. 5. electronic information Page is used for the operation of social-economic, foreign, defense and security to implement the provisions of this law and the provisions of relevant laws.	
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		
6	the Law on Protection of Consumer Rights No. 19/2023/QH15	Under the CPL 2023, a consumer is defined to be "a person who purchases and/or uses products, goods and services with the aim of consumption for daily needs of individuals, families, or organizations, and not for commercial purposes" (Article 3.1). "consumer information" includes consumers' personal	

		information, information about their process of purchasing and using products, goods, and services and other information related to transactions between consumers and traders (Article 3.3). Therefore, the scope of consumer information is broader than that of personal data. "influencer," which is defined as an expert or a person with credibility or recognized by society in a specific field, industry, or profession (Article 3.9). "vulnerable consumer." This term pertains to a consumer who, at the time of purchase or use of products/services, is potentially subject to various adverse situations in terms of information access, health, property, or dispute settlement. This category encompasses individuals such as the elderly and disabled, children, ethnic minorities, people of remote or economically difficult regions, pregnant women and breastfeeding mothers of infants under 36 months, individuals with severe illnesses, and members of poor households (Article 8.1).	
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13	Article 3. Interpretation of terms 15. Personal information means information associated with the identification of a specific person. 16. Owner of personal information means a person identified based on such information. 17. Processing of personal information means the performance of one or some operations of collecting, editing,	

		utilizing, storing, providing, sharing or spreading personal information in cyberspace for commercial purpose.	
9	Decree 27/2018/ND-CP	a/ To register and store personal information of members, including full name, date of birth, people's identity card/citizen identification card/passport number and date and place of issue, phone number and email address (if any). If an Internet user is under 14 years old and has no people's identity card, citizen identification card or passport, his/her lawful guardian shall decide to register his/her own personal information as specified at this Point to show his/her consent and take responsibility before law for that registration; b/ To verify service users via messages sent to phone numbers or email addresses when registering service use or changing personal information; c/ To block or remove information violating Clause 1, Article 5 of this Decree at the request of competent state management agencies; d/ To set up a mechanism for warning members that post violating information (filtering system);	
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information	Article 3. Interpretation of terms In this Decree, the terms below are construed as follows: 14. Public information means online information of an organization or individual that is publicized without requiring specific identifications or addresses of recipients. 15. Private information means online information of an organization or individual that is not publicized by that organization or individual, or only provided to a single recipient or publicized among a	

		group of recipients with specific identifications and addresses. 16. Personal information means information associated with the identification of individuals, including names, ages, addresses, people's identity card numbers, phone numbers, email addresses and other information defined by law.	
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation	Data handlers
		Classification/ distinction by responsibility (data processor, data controller)/ size of data, (national security) critical services, etc.
		Provision on type of data handler
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)	6. "Data subject" refers to an individual to whom the data relates. 9. "Personal Data Controller" refers to an organization or individual that decides purposes and means of processing personal data. 10. "Personal Data Processor" refers to an organization or individual that processes data on behalf of the Personal Data Controller via a contract or agreement with the Personal Data Controller. 11. "Personal Data Controller-cum-Processor" refers to an organization or individual that jointly decides purposes and means, and directly processes personal data. 12. "Third Party" refers to an organization or individual other than the data subject, Personal Data Controller, Personal Data Processor, and Personal Data Controller-cum-Processor that is permitted to process personal data. 13. "Automated processing of personal data" refers to a form of personal data processing performed by electronic devices with a view to assessing, analyzing and predicting an individual's activities, including habits, preference, reliability, behavior, location, trends, capability and other circumstances.
2	Law on Cyber-information Security No.86/2015/QH13	
3	Law on Cybersecurity 24/2018/QH14	
4	Decree No. 53/2022/ND-CP	
5	Law on Information Technology No.67/2006/QH11	

6	the Law on Protection of Consumer Rights No. 19/2023/QH15	
7	Decree regarding e-commerce, No.85/2021/NDCP	
8	Law on 86/2015/QH13	
9	Decree 27/2018/ND-CP	
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information	
11	Law No. 91/2015/QH13	
12	Law on Inspection No. 56/2010/QH12	

Legal Basis

#	Regulation		
		consent	necessary for the performance of a contract
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)	Article 11. Consent of a data subject 1. The consent of the data subject shall be granted to all activities in the processing of his/her personal data, unless otherwise provided for by law. 2. The consent is only valid when the data subject voluntarily consents and clearly knows the following contents: a) Type of personal data; b) Purposes; c) Organization or individual permitted to process personal data; d) Rights and obligations of the data subject. 3. The consent of the data subject shall be expressed in a	4. The personal data shall be processed to fulfill obligations under contracts the data subjects with relevant agencies, organizations and individuals as prescribed by law;

		clear and specific manner in writing, by voice, by ticking the consent box, by consent syntax via message, by selecting consent settings or by other forms. 4. The consent must be bound to the same purpose. In case of multiple purposes, the Personal Data Controller and the Personal Data Controller-cum-Processor shall list these purposes so that the data subject consents to one or several purposes that have been set out. 5. The consent of the data subject shall be expressed in a format that can be printed and reproduced in writing, including in electronic or verifiable format. 6. Silence or non-response is not considered as consent. 7. The data subject may give partial or conditional consent. **** Article 13. Notification of personal data processing 1. The notification shall be made once before the personal data is processed. 2. The following contents of the processing of personal data shall be notified to the data subject: a) Processing purposes; b) Type of used personal data related to the purposes specified in Point a Clause 2 of this Article; c) Method of processing personal data; d) Information on other organizations and individuals related to the processing purposes specified in point a Clause 2 of this Article; dd) Undesirable consequences and damage that may occur; e) Starting and ending time. 3. The notification to the data subject shall be expressed in a format that can be printed and reproduced in writing, including	

		in electronic or verifiable format. 4. The Personal Data Controller and the Personal Data Controller-cum-Processor are not required to comply with regulations specified in Clause 1 of this Article in the following cases: a) The data subject knows and fully consents to the contents specified in Clauses 1 and 2 of this Article before permitting the Personal Data Controller and the Personal Data Controller-cum-Processor to collect his/her personal data in accordance with regulations in Article 9 of this Decree; b) The personal data is processed by the competent state agency with a view to serving operations by such agency as prescribed by law. ****	
2	Law on Cyber-information Security No.86/2015/QH13	Article 9. Classification of information 1. Information-owning agencies and organizations shall classify information based on its secrecy in order to take appropriate protection measures. 2. Information regarded as state secret shall be classified and protected in accordance with the law on protection of state secrets. Agencies and organizations that use classified and unclassified information in activities within their fields shall develop regulations and procedures for processing information; determine contents and methods of recording authorized accesses to classified information. Article 17. Collection and use of personal information 1. Organizations and individuals that process personal information shall: a/ Collect personal information	

		only after obtaining the consent of its owners regarding the scope and purpose of collection and use of such information; b/ Use the collected personal information for purposes other than the initial one only after obtaining the consent of its owners; c/ Refrain from providing, sharing or spreading to a third party personal information they have collected, accessed or controlled, unless they obtain the consent of the owners of such personal information or at the request of competent state agencies. 2. State agencies shall secure and store personal information they have collected. 3. Owners of personal information may request personal information processing organizations and individuals to provide their personal information collected and stored by the latter.	
3	Law on Cybersecurity 24/2018/QH14		
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11	Article 21. Collect, process and use personal information on network environment 1. Individual organizations collect, process and use the personal information of other people on the network environment must be that person agrees, unless otherwise specified by law. 2. organizations and individuals collect, process and use the personal information of others responsibly: a) inform that person about the form, scope, place and purpose of the collection, processing and use of personal information of that person; b) use purpose of personal	Article 21. Collect, process and use personal information on network environment 1. Individual organizations collect, process and use the personal information of other people on the network environment must be that person agrees, unless otherwise specified by law. 2. organizations and individuals collect, process and use the personal information of others responsibly: a) inform that person about the form, scope, place and purpose of the collection, processing and use of personal information of that person; b) use purpose of personal

		information properly collected and stored the information in a certain period of time as prescribed by the law or by agreement between the two parties; c) to conduct technical, management measures needed to ensure your personal information is not lost, stolen, disclosed, altered or destroyed; d) proceed immediately the necessary measures when get request to check back, or cancelled in accordance with paragraph 1 Article 22 of this law; not provided or use the relevant personal information until it was revised again. 3. organizations and individuals have the right to collect, process and use the personal information of another person without that person's consent in the event that personal information is used for the following purposes: a) signed, modify or execute a contract to use the information, product , service on network environment; b) Computer reviews, cost of use of the information, products or services on the network environment; c) perform other duties specified by law. Article 22. Archive, provides personal information on network environment 1. Individuals have the right to request personal organizer, personal information stored on their network environment to perform the test, or remove such information. 2. organizations and individuals are not provided in other people's personal information to third parties, except as otherwise specified by law or consent of that person. 3. the individual has the right to request compensation for	information properly collected and stored the information in a certain period of time as prescribed by the law or by agreement between the two parties; c) to conduct technical, management measures needed to ensure your personal information is not lost, stolen, disclosed, altered or destroyed; d) proceed immediately the necessary measures when get request to check back, or cancelled in accordance with paragraph 1 Article 22 of this law; not provided or use the relevant personal information until it was revised again. 3. organizations and individuals have the right to collect, process and use the personal information of another person without that person's consent in the event that personal information is used for the following purposes: a) signed, modify or execute a contract to use the information, product , service on network environment; b) Computer reviews, cost of use of the information, products or services on the network environment; c) perform other duties specified by law. Article 22. Archive, provides personal information on network environment 1. Individuals have the right to request personal organizer, personal information stored on their network environment to perform the test, or remove such information. 2. organizations and individuals are not provided in other people's personal information to third parties, except as otherwise specified by law or consent of that person. 3. the individual has the right to request compensation for

		damage caused by violation of the provision of the personal information. Article 23. Establish electronic information page 1. The Organization, individuals have the right to establish electronic information page under the provisions of the law and is responsible for managing the content and operation of electronic information page. 2. organizations and individuals who use the national Vietnam domain name ".vn" when setting up the electronic information page without notice with the Ministry of posts and telecommunications. Individual organization when setting up electronic information page does not use the national Vietnam domain name ".vn" is announced on the network environment of postal and telecommunications Ministry with the following information: a) institution name recorded in the establishment decision, active license, registration certificate or business license to open a representative office; personal names; b) Number, date of issue, where the level of people's ID or number, date of issue, issuing personal passport; c) addresses the Organization's headquarters or place of permanent residence of the individual; d) phone numbers, fax numbers, electronic mail address; DD) The registered domain name. 3. organizations and individuals to be responsible before the law for the accuracy of the information specified in paragraph 2 of this article, when the information changes, then have to inform about the	damage caused by violation of the provision of the personal information. Article 23. Establish electronic information page 1. The Organization, individuals have the right to establish electronic information page under the provisions of the law and is responsible for managing the content and operation of electronic information page. 2. organizations and individuals who use the national Vietnam domain name ".vn" when setting up the electronic information page without notice with the Ministry of posts and telecommunications. Individual organization when setting up electronic information page does not use the national Vietnam domain name ".vn" is announced on the network environment of postal and telecommunications Ministry with the following information: a) institution name recorded in the establishment decision, active license, registration certificate or business license to open a representative office; personal names; b) Number, date of issue, where the level of people's ID or number, date of issue, issuing personal passport; c) addresses the Organization's headquarters or place of permanent residence of the individual; d) phone numbers, fax numbers, electronic mail address; DD) The registered domain name. 3. organizations and individuals to be responsible before the law for the accuracy of the information specified in paragraph 2 of this article, when the information changes, then have to inform about the

		changes. 4. electronic information Page is used for the operation of the press must be made to the provisions of this law, the law on the press and the other provisions of the relevant laws. 5. electronic information Page is used for the operation of social-economic, foreign, defense and security to implement the provisions of this law and the provisions of relevant laws.	changes. 4. electronic information Page is used for the operation of the press must be made to the provisions of this law, the law on the press and the other provisions of the relevant laws. 5. electronic information Page is used for the operation of social-economic, foreign, defense and security to implement the provisions of this law and the provisions of relevant laws.
6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13	Section 2 PROTECTION OF PERSONAL INFORMATION Article 16. Principles of protecting personal information in cyberspace 1. Individuals shall themselves protect their personal information and comply with the law on provision of personal information when using services in cyberspace. 2. Agencies, organizations and individuals that process personal information shall ensure cyberinformation security for the information they process. 3. Organizations and individuals that process personal information shall develop and publicize their own measures to process and protect personal information. 4. The protection of personal	

		information must comply with this Law and other relevant laws. 5. The processing of personal information for the purpose of ensuring national defense and security and social order and safety or for non-commercial purposes must comply with other relevant laws. Article 17. Collection and use of personal information 1. Organizations and individuals that process personal information shall: a/ Collect personal information only after obtaining the consent of its owners regarding the scope and purpose of collection and use of such information; b/ Use the collected personal information for purposes other than the initial one only after obtaining the consent of its owners; c/ Refrain from providing, sharing or spreading to a third party personal information they have collected, accessed or controlled, unless they obtain the consent of the owners of such personal information or at the request of competent state agencies. 2. State agencies shall secure and store personal information they have collected. 3. Owners of personal information may request personal information-processing organizations and individuals to provide their personal information collected and stored by the latter.	

		Article 18. Updating, alteration and cancellation of personal information 1. Owners of personal information may request personal information-processing organizations and individuals to update, alter or cancel their personal information collected or stored by the latter or to stop providing such personal information to a third party. 2. Upon receiving the request of an owner of personal information for update, alteration or cancellation of personal information or for stoppage of the provision of personal information to a third party, a personal information-processing organization or individual shall: a/ Comply with the request and notify such owner or grant him/her/it the right to access information for the latter to update, alter or delete his/her/its personal information; b/ Take appropriate measures to protect personal information; and notify such owner if it/he/she fails to comply with the request for technical or other reasons. 3. Personal information-processing organizations and individuals shall delete the stored personal information when they have accomplished their use purposes or the storage time has expired and notify such to the owners of such personal information, unless otherwise prescribed by law. Article 19. Security assurance for personal information in cyberspace	

		1. Personal information-processing organizations and individuals shall take appropriate management and technical measures to protect personal information they have collected and stored; and comply with standards and technical regulations on assurance of cyberinformation security. 2. When a cyberinformation security incident occurs or threatens to occur, personal information-processing organizations and individuals shall take remedy and stoppage measures as soon as possible. Article 20. Responsibilities of state management agencies in protecting personal information in cyberspace 1. To establish online information channels for receiving petitions and reports from the public which are related to security assurance for personal information in cyberspace. 2. To annually inspect and examine personal information-processing organizations and individuals; to conduct extraordinary inspection and examination when necessary.	
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		

12	Law on Inspection No. 56/2010/QH12		

#	Regulation		
		necessary for compliance with a legal obligation	necessary in order to protect the vital interests
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)	2. Disclosure of personal data in accordance with the law; 5. The personal data shall be processed to serve operations by regulatory authorities as prescribed by relevant laws.	Article 17. Personal data processing without the consent of data subject 1. The personal data shall be processed to protect the life and health of the data subject or others in an emergency situation. The Personal Data Controller, the Personal Data Controller-cum-Processor, the Personal Data Processor and the Third Party shall be responsible for proving such situation.
2	Law on Cyber-information Security No.86/2015/QH13		
3	Law on Cybersecurity 24/2018/QH14		
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11	Article 21. Collect, process and use personal information on network environment 1. Individual organizations collect, process and use the personal information of other people on the network environment must be that person agrees, unless otherwise specified by law. 2. organizations and individuals collect, process and use the personal information of others responsibly: a) inform that person about the form, scope, place and purpose of the collection, processing and use of personal information of that person; b) use purpose of personal information properly collected and stored the information in a	

		certain period of time as prescribed by the law or by agreement between the two parties; c) to conduct technical, management measures needed to ensure your personal information is not lost, stolen, disclosed, altered or destroyed; d) proceed immediately the necessary measures when get request to check back, or cancelled in accordance with paragraph 1 Article 22 of this law; not provided or use the relevant personal information until it was revised again. 3. organizations and individuals have the right to collect, process and use the personal information of another person without that person's consent in the event that personal information is used for the following purposes: a) signed, modify or execute a contract to use the information, product , service on network environment; b) Computer reviews, cost of use of the information, products or services on the network environment; c) perform other duties specified by law. Article 22. Archive, provides personal information on network environment 1. Individuals have the right to request personal organizer, personal information stored on their network environment to perform the test, or remove such information. 2. organizations and individuals are not provided in other people's personal information to third parties, except as otherwise specified by law or consent of that person. 3. the individual has the right to request compensation for damage caused by violation of the provision of the personal	

		information. Article 23. Establish electronic information page 1. The Organization, individuals have the right to establish electronic information page under the provisions of the law and is responsible for managing the content and operation of electronic information page. 2. organizations and individuals who use the national Vietnam domain name ".vn" when setting up the electronic information page without notice with the Ministry of posts and telecommunications. Individual organization when setting up electronic information page does not use the national Vietnam domain name ".vn" is announced on the network environment of postal and telecommunications Ministry with the following information: a) institution name recorded in the establishment decision, active license, registration certificate or business license to open a representative office; personal names; b) Number, date of issue, where the level of people's ID or number, date of issue, issuing personal passport; c) addresses the Organization's headquarters or place of permanent residence of the individual; d) phone numbers, fax numbers, electronic mail address; DD) The registered domain name. 3. organizations and individuals to be responsible before the law for the accuracy of the information specified in paragraph 2 of this article, when the information changes, then have to inform about the changes. 4. electronic information Page is	

		used for the operation of the press must be made to the provisions of this law, the law on the press and the other provisions of the relevant laws. 5. electronic information Page is used for the operation of social-economic, foreign, defense and security to implement the provisions of this law and the provisions of relevant laws.	
6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation		
		necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	necessary for the purposes of the legitimate interests pursued by the controller or by a third party
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data	3. Processing of personal data by competent regulatory authorities in the event of a state of emergency regarding national defense, security, social order	

	Protection Decree)	and safety, major disasters, or dangerous epidemics; when there is a threat to security and national defense but not to the extent of declaring a state of emergency; to prevent and fight riots and terrorism, crimes and law violations according to the provisions of law; Article 18. Processing of personal data obtained from audio and video recording activities in public places Competent agencies and organizations may make audio and video recording and process personal data obtained from audio or video recording activities in public places in order to protect national security, social order and safety, legitimate rights and interests of organizations and individuals as prescribed by law without the consent of the data subjects. When making audio and video recording, competent agencies and organizations shall notify the data subjects that such data subjects are being recorded, unless otherwise provided for by law. ****	
2	Law on Cyber-information Security No.86/2015/QH13		
3	Law on Cybersecurity 24/2018/QH14		
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		
6	the Law on Protection of Consumer Rights		

	No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation	opt-out	others
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)		
2	Law on Cyber-information Security No.86/2015/QH13		
3	Law on Cybersecurity 24/2018/QH14		Article 17. Prevention of and combatting cyberespionage; and protection of information classified as State secret, work secrets, business secrets, personal secrets, family secrets and private life in cyberspace 1. Conduct constituting cyberespionage; and infringement of State secrets, work secrets, business secrets,

			personal secrets, family secrets and private life in cyberspace comprises: (a) Appropriating, buying or selling, seizing and/or intentionally disclosing information classified as State secret or work secrets; business secrets, personal secrets, family secrets and private life [adversely] impacting on the honour, reputation, dignity and lawful rights and interests of agencies, organizations and individuals; (b) Deliberately deleting, damaging, misplacing and/or changing information classified as State secret, or work secrets, business secrets, personal secrets, family secrets and private life which is transmitted and/or stored in cyberspace; (c) Deliberately altering, cancelling or invalidating technical measures which have been constructed and/or applied in order to protect information classified as State secret, work secrets, business secrets, personal secrets, family secrets and private life; (d) Putting in cyberspace information being State secret or work secrets, business secrets, personal secrets, family secrets and private life contrary to law; (dd) Deliberately listening to or recording in sound or images conversations, contrary to law; (e) Other acts of intentional infringement of State secrets, work secrets, business secrets, personal secrets, family secrets and private life.
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		

6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		Article 3. Basic principles of civil law 1. Every person shall be equal in civil relations, may not use any reason for unequal treatment to others, and enjoy the same protection policies of law regarding moral rights and economic rights. 2. Each person establishes, exercises/fulfills and terminates his/her civil rights and obligations on the basis of freely and voluntarily entering into commitments and/or agreements. Each commitment or agreement that does not violate regulations of law and is not contrary to social ethics shall be bound by contracting parties and must be respected by other entities. 3. Each person must establish, exercise/ fulfill, or terminate his/her civil rights and/or obligations in the principle of goodwill and honesty. 4. The establishment, exercise

			and termination of civil rights and/or obligations may not infringe national interests, pubic interests, lawful rights and interests of other persons. 5. Each person shall be liable for his/her failure to fulfill or the incorrect fulfillment of any such civil obligations.
12	Law on Inspection No. 56/2010/QH12		

Rights of the data subject

#	Regulation	Right to be informed	Right of access
1	Decree No. 13/2023/ND-CP (PDPD：Personal Data Protection Decree)	Article 9. Data subject's rights 1. Right to be informed The data subject has the right to be informed of his/her personal data processing, unless otherwise provided for by law.	3. Right to access personal data The data subject has the right to access his/her personal data in order to look at, rectify or request rectification of his/her personal data, unless otherwise provided for by law.
2	Law on Cyber-information Security No.86/2015/QH13		Article 18. Updating, alteration and cancellation of personal information 1. Owners of personal information may request personal informationprocessing organizations and individuals to update, alter or cancel their personal information collected or stored by the latter or to stop providing such personal information to a third party. 2. Upon receiving the request of an owner of personal information for update, alteration or cancellation of personal information or for stoppage of the provision of personal information to a third party, a personal information-processing organization or individual shall: a/ Comply with the request and notify such owner or grant him/her/it the right to access information for the latter to update, alter or delete his/her/its personal information;

3	Law on Cybersecurity 24/2018/QH14		Article 29. Child protection in cyberspace 1. Children have the right to be protected; to access information; to participate in social, entertainment and recreational activities; to keep their personal secrets confidential, and other rights when they participate in cyberspace. 2. Information system administrators and cyberspace service providers are responsible to control information on [their] information systems or on services provided by them, in order not to cause harm to or mistreatment of children or infringing children's rights; and to block the sharing of and to delete information the contents of which may cause harm to or mistreat children or infringe their rights; and [are responsible to] promptly notify and co-ordinate with the CTF under the Ministry of Public Security for resolution. 3. Agencies, organizations and individuals participating in activities in cyberspace are responsible to co-ordinate with competent State administrative agencies to guarantee children's rights in cyberspace, and prevent [block] network information with contents causing harm to children, in accordance with this Law and the law on children. 4. Agencies, organizations, parents, teachers, child carers and other relevant individuals are responsible to guarantee children's rights and to protect children in accordance with the law on children when they [the former] participate in cyberspace. 5. Cybersecurity Task Forces and functional agencies are responsible to take measures to

			preclude, discover, prevent and strictly deal with the use of cyberspace to cause harm to or intrude on children or to infringe their rights.
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		1. organizations or individuals to participate in information technology applications have the following rights: a) search, Exchange and use of information on the network environment, except for the content information prescribed in clause 2 of article 12 of this Law;(Article 12. The prohibited acts) b) required to restore your information or recover the ability to access your information source in case the content of information that do not violate the provisions in paragraph 2 of article 12 of this Law; c) requires that State agencies have jurisdiction under the provisions of the law in the case denied the information recovery or restore the ability to access sources of information; d) distribute the contact address on network environment when the consent of the owner of contacts; DD) refuse to provide or receive on the network environment of products, services, contrary to the provisions of the law and must take responsibility for that. 2. organizations and individuals participate in the development of information technology has the following rights: a) research and development in information technology products; b) producing information technology products; digitized, maintaining and increasing the value of information resources. Article 15. Management and use

			of information 1. The Organization, individuals have the right to freely use the information of legitimate purposes, in accordance with the provisions of the law. 2. the competent State agencies responsible for implementing measures to ensure the access and use of information advantage. 3. The provision, Exchange, give, use, storage of information are guaranteed not to violate prescribed in clause 2 of article 12 of this Law and the provisions of relevant laws. 4. organizations and individuals not be cited content information of the Organization, other individuals in the case of information owners had warned or law regulating the quoted information is not allowed. 5. Cases are allowed to cite information, organizations, individuals are responsible for stating the source of that information. Article 16. Information transmission of 1. organizations and individuals have the right to transmit information of other individual of the Organization, consistent with the provisions of this law. 2. organizations and individuals put some of the information transmission organization, the other individual is not responsible for the content of information to be stored automatically, temporarily, due to the technical requirements if temporary storage activities aim to serve for the transmission of information and the information is stored in the time enough to make the transmission take. 3. organizations and individuals put information transfer of

			responsibility to conduct the necessary measures in time to prevent the access information or remove unlawful information at the request of the competent State bodies. 4. organizations and individuals put information transmission the number of organizations and individuals are not responsible for the content of such information, unless you do one of the following behaviors: a) himself started the transmission of information; b) choose the recipient information was transmitted bringing; c) option and modify the content of the information transmitted. Article 17. The temporary storage of information 1. The Organization, individuals have the right to temporary storage of information of the Organization, the other individual. 2. organizations and individuals, the temporary storage of information of the Organization, the other individual is not responsible for the content of such information, unless you do one of the following behaviors: a) modify the content of the information; b) does not comply with the rules on access or update information content; c) collecting data illegally through the store information temporarily; d) disclose confidential information.
6	the Law on Protection of Consumer Rights No. 19/2023/QH15	The general rules under the CPL 2023 on consumer information protection are largely compatible with the general rules stipulated in the regulations on personal data protection under other laws, especially the rules regarding notification of data subjects of certain stipulated information in	

		advance; obtaining express opt-in consent of data subjects before collection and processing of consumer information; and ensuring the safety of consumer information.	
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13	Article 18. Updating, alteration and cancellation of personal information 1. Owners of personal information may request personal information-processing organizations and individuals to update, alter or cancel their personal information collected or stored by the latter or to stop providing such personal information to a third party. 2. Upon receiving the request of an owner of personal information for update, alteration or cancellation of personal information or for stoppage of the provision of personal information to a third party, a personal information-processing organization or individual shall: a/ Comply with the request and notify such owner or grant him/her/it the right to access information for the latter to update, alter or delete his/her/its personal information; b/ Take appropriate measures to protect personal information; and notify such owner if it/he/she fails to comply with the request for technical or other reasons. 3. Personal information-processing organizations and individuals shall delete the stored personal information when they have accomplished their use purposes or the	

		storage time has expired and notify such to the owners of such personal information, unless otherwise prescribed by law.	
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information	Article 25. Rights and obligations of organizations and enterprises that establish social networks Organizations and enterprises that establish social networks have the following rights and obligations: 1. To provide social network services for the public, except services banned by law; 2. To publicize the agreements on provision and use of social network services; 3. To take measures for protecting private and personal information of users; to notify users of their rights, obligations and risks when storing, exchanging and sharing information online; 4. To assure the right to make decisions of users when they allow their personal information to be provided for other organizations, enterprises and individuals; 5. Not to provide public information that violates Article 5 of this Decree; 6. To coordinate with competent state management agencies in removing or blocking information that violates Article 5 of this Decree at their request. 7. To provide private and personal information of users relating to terrorism, crime and violations of law at the request of competent state management agencies; 8. To have at least one server system in Vietnam serving the inspection, supervision, storage, and provision of information at the request of competent state management agencies, and	

		settlement of customers' complaints about the service provision according to regulations of the Ministry of Information and Communications; 9. To register, store and manage personal information of the persons that establish private websites and other information providers on social networks according to regulations of the Ministry of Information and Communications. To ensure that only persons who sufficiently and accurately provide their personal information are allowed to establish private websites or provide information on social networks; 10. To make reports according to regulations to and subject to the inspection and supervision by competent state management agencies. Article 26. Rights and obligations of social network users In addition to the rights and obligations of Internet users provided in Article 10 of this Decree, social network users have the following rights and obligations: 1. To use services of social networks, except services banned by law. 2. To have their private and personal information kept confidential in accordance with law. 3. To comply with the Regulation on management, provision and use of social network services. 4. To take responsibility for the information they store, provide and transmit on social networks, or spread via direct links they establish.	
11	Law No. 91/2015/QH13		

12	Law on Inspection No. 56/2010/QH12		

#	Regulation	Right to rectification	Right to erasure
1	Decree No. 13/2023/ND-CP) (PDPD: Personal Data Protection Decree)		5. Right to delete personal data The data subject has the right to delete or request deletion of his/her personal data, unless otherwise provided for by law.
2	Law on Cyber-information Security No.86/2015/QH13	Article 18. Updating, alteration and cancellation of personal information 1. Owners of personal information may request personal informationprocessing organizations and individuals to update, alter or cancel their personal information collected or stored by the latter or to stop providing such personal information to a third party. 2. Upon receiving the request of an owner of personal information for update, alteration or cancellation of personal information or for stoppage of the provision of personal information to a third party, a personal information-processing organization or individual shall: a/ Comply with the request and notify such owner or grant him/her/it the right to access information for the latter to update, alter or delete his/her/its personal information;	Article 18. Updating, alteration and cancellation of personal information 1. Owners of personal information may request personal informationprocessing organizations and individuals to update, alter or cancel their personal information collected or stored by the latter or to stop providing such personal information to a third party. 2. Upon receiving the request of an owner of personal information for update, alteration or cancellation of personal information or for stoppage of the provision of personal information to a third party, a personal information-processing organization or individual shall: a/ Comply with the request and notify such owner or grant him/her/it the right to access information for the latter to update, alter or delete his/her/its personal information;
3	Law on Cybersecurity 24/2018/QH14		
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		

6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13	Article 18. Updating, alteration and cancellation of personal information 1. Owners of personal information may request personal information-processing organizations and individuals to update, alter or cancel their personal information collected or stored by the latter or to stop providing such personal information to a third party. 2. Upon receiving the request of an owner of personal information for update, alteration or cancellation of personal information or for stoppage of the provision of personal information to a third party, a personal information-processing organization or individual shall: a/ Comply with the request and notify such owner or grant him/her/it the right to access information for the latter to update, alter or delete his/her/its personal information; b/ Take appropriate measures to protect personal information; and notify such owner if it/he/she fails to comply with the request for technical or other reasons. 3. Personal information-processing organizations and individuals shall delete the stored personal information when they have accomplished their use purposes or the storage time has expired and	Article 18. Updating, alteration and cancellation of personal information 1. Owners of personal information may request personal information-processing organizations and individuals to update, alter or cancel their personal information collected or stored by the latter or to stop providing such personal information to a third party. 2. Upon receiving the request of an owner of personal information for update, alteration or cancellation of personal information or for stoppage of the provision of personal information to a third party, a personal information-processing organization or individual shall: a/ Comply with the request and notify such owner or grant him/her/it the right to access information for the latter to update, alter or delete his/her/its personal information; b/ Take appropriate measures to protect personal information; and notify such owner if it/he/she fails to comply with the request for technical or other reasons. 3. Personal information-processing organizations and individuals shall delete the stored personal information when they have accomplished their use purposes or the storage time has expired and

		notify such to the owners of such personal information, unless otherwise prescribed by law.	notify such to the owners of such personal information, unless otherwise prescribed by law.
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation	Right to restrict processing	Right to data portability
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)	6. Right to obtain restriction on processing a) The data subject has the right to obtain restriction on the processing of his/her personal data, unless otherwise provided for by law. b) The restriction on the processing of personal data shall be implemented within 72 hours after receiving request of the data subject, and all personal data that the data subject requests the restriction, unless otherwise provided for by law.	7. Right to obtain personal data The data subject has the right to request the Personal Data Controller and the Personal Data Controller-cum-Processor to provide him/her with his/her personal data, unless otherwise provided for by law.
2	Law on Cyber-information Security No.86/2015/QH13	Article 18. Updating, alteration and cancellation of personal information 1. Owners of personal information may request personal information processing organizations and individuals to update, alter or cancel their personal information collected or stored by the latter or to stop providing such personal information to a third party. 2. Upon receiving the request of	

		an owner of personal information for update, alteration or cancellation of personal information or for stoppage of the provision of personal information to a third party, a personal information-processing organization or individual shall: a/ Comply with the request and notify such owner or grant him/her/it the right to access information for the latter to update, alter or delete his/her/its personal information;	
3	Law on Cybersecurity 24/2018/QH14		
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		
6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13	Article 18. Updating, alteration and cancellation of personal information 1. Owners of personal information may request personal information-processing organizations and individuals to update, alter or cancel their personal information collected or stored by the latter or to stop providing such personal information to a third party. 2. Upon receiving the request of an owner of personal information for update, alteration or cancellation of personal information or for stoppage of	

		the provision of personal information to a third party, a personal information-processing organization or individual shall: a/ Comply with the request and notify such owner or grant him/her/it the right to access information for the latter to update, alter or delete his/her/its personal information; b/ Take appropriate measures to protect personal information; and notify such owner if it/he/she fails to comply with the request for technical or other reasons. 3. Personal information-processing organizations and individuals shall delete the stored personal information when they have accomplished their use purposes or the storage time has expired and notify such to the owners of such personal information, unless otherwise prescribed by law.	
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation	Right to object	Right not to be subject to a decision based solely on automated processing
1	Decree No. 13/2023/ND-	8. Right to object to processing a) The data subject has the right	

	CP) (PDPD: Personal Data Protection Decree)	to object to the Personal Data Controller and the Personal Data Controller-cum-Processor processing his/her personal data in order to prevent or restrict the disclosure of personal data or the use of personal data for advertising and marketing purposes, unless otherwise provided for by law. b) The Personal Data Controller and the Personal Data Controller-cum-Processor shall comply with the data subject's request within 72 hours after receiving the request, unless otherwise provided for by law. 9. Right to file complaints, denunciations and lawsuits The data subject has the right to file complaints, denunciations and lawsuits as prescribed by law.	
2	Law on Cyber-information Security No.86/2015/QH13		
3	Law on Cybersecurity 24/2018/QH14		
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		
6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		

10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation	Right to withdraw consent	others
1	Decree No. 13/2023/ND-CP) (PDPD: Personal Data Protection Decree)	4. Right to withdraw consent The data subject has the right to withdraw his/her consent, unless otherwise provided for by law.	2. Right to give consent The data subject has the right to give consent to the processing of his/her personal data, other than cases specified in Article 17 of this Decree. 10. Right to claim damage The data subject has the right to claim damage as prescribed by law when there are violations against regulations on protection of his/her personal data, unless otherwise agreed by parties or unless otherwise prescribed by law. 11. Right to self-protection The data subject has the right to self-protection according to regulations in the Civil Code, other relevant laws and this Decree, or request competent agencies and organizations to implement civil right protection methods according to regulations in Article 11 of the Civil Code.
2	Law on Cyber-information Security No.86/2015/QH13		

3	Law on Cybersecurity 24/2018/QH14		Article 29. Child protection in cyberspace 1. Children have the right to be protected; to access information; to participate in social, entertainment and recreational activities; to keep their personal secrets confidential, and other rights when they participate in cyberspace. 2. Information system administrators and cyberspace service providers are responsible to control information on [their] information systems or on services provided by them, in order not to cause harm to or mistreatment of children or infringing children's rights; and to block the sharing of and to delete information the contents of which may cause harm to or mistreat children or infringe their rights; and [are responsible to] promptly notify and co-ordinate with the CTF under the Ministry of Public Security for resolution. 3. Agencies, organizations and individuals participating in activities in cyberspace are responsible to co-ordinate with competent State administrative agencies to guarantee children's rights in cyberspace, and prevent [block] network information with contents causing harm to children, in accordance with this Law and the law on children. 4. Agencies, organizations, parents, teachers, child carers and other relevant individuals are responsible to guarantee children's rights and to protect children in accordance with the law on children when they [the former] participate in cyberspace. 5. Cybersecurity Task Forces and functional agencies are responsible to take measures to

			preclude, discover, prevent and strictly deal with the use of cyberspace to cause harm to or intrude on children or to infringe their rights.
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		1. organizations or individuals to participate in information technology applications have the following rights: a) search, Exchange and use of information on the network environment, except for the content information prescribed in clause 2 of article 12 of this Law;(Article 12. The prohibited acts) b) required to restore your information or recover the ability to access your information source in case the content of information that do not violate the provisions in paragraph 2 of article 12 of this Law; c) requires that State agencies have jurisdiction under the provisions of the law in the case denied the information recovery or restore the ability to access sources of information; d) distribute the contact address on network environment when the consent of the owner of contacts; DD) refuse to provide or receive on the network environment of products, services, contrary to the provisions of the law and must take responsibility for that. 2. organizations and individuals participate in the development of information technology has the following rights: a) research and development in information technology products; b) producing information technology products; digitized, maintaining and increasing the value of information resources. Article 15. Management and use

			of information 1. The Organization, individuals have the right to freely use the information of legitimate purposes, in accordance with the provisions of the law. 2. the competent State agencies responsible for implementing measures to ensure the access and use of information advantage. 3. The provision, Exchange, give, use, storage of information are guaranteed not to violate prescribed in clause 2 of article 12 of this Law and the provisions of relevant laws. 4. organizations and individuals not be cited content information of the Organization, other individuals in the case of information owners had warned or law regulating the quoted information is not allowed. 5. Cases are allowed to cite information, organizations, individuals are responsible for stating the source of that information. Article 16. Information transmission of 1. organizations and individuals have the right to transmit information of other individual of the Organization, consistent with the provisions of this law. 2. organizations and individuals put some of the information transmission organization, the other individual is not responsible for the content of information to be stored automatically, temporarily, due to the technical requirements if temporary storage activities aim to serve for the transmission of information and the information is stored in the time enough to make the transmission take. 3. organizations and individuals put information transfer of

			responsibility to conduct the necessary measures in time to prevent the access information or remove unlawful information at the request of the competent State bodies. 4. organizations and individuals put information transmission the number of organizations and individuals are not responsible for the content of such information, unless you do one of the following behaviors: a) himself started the transmission of information; b) choose the recipient information was transmitted bringing; c) option and modify the content of the information transmitted. Article 17. The temporary storage of information 1. The Organization, individuals have the right to temporary storage of information of the Organization, the other individual. 2. organizations and individuals, the temporary storage of information of the Organization, the other individual is not responsible for the content of such information, unless you do one of the following behaviors: a) modify the content of the information; b) does not comply with the rules on access or update information content; c) collecting data illegally through the store information temporarily; d) disclose confidential information.
6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		the contract for continuous cross-border supply of services between an offshore trader and a consumer in Vietnam should

			be carefully prepared to comply with new requirements in the Consumer Law 2023.
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		11. To add the following Article 23d: 2. Conditions on information management of social networks: d/ To adopt measures to protect the privacy and personal information of users; dd/ To ensure users' right to permit the collection of his/her personal information or provision of such information to other organizations, enterprises or persons.
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

Extraterritorial application

#	Regulation		
		applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction	applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction
1	Decree No. 13/2023/ND-CP) (PDPD: Personal Data Protection Decree)		
2	Law on Cyber-information		

	Security No.86/2015/QH13		
3	Law on Cybersecurity 24/2018/QH14		
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		
6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP	Decree 85 adds a separate section governing the cross-border e-commerce activities of foreign entities, including those having websites to provide e-commerce services in Vietnam and those selling goods in Vietnam's e-commerce websites. - Foreign traders having websites providing e-commerce services in Vietnam; - Foreign traders selling goods on Vietnamese e-commerce floors; - Foreign investors invest in the business of providing e-commerce services in Vietnam in the form of setting up enterprises or purchasing shares and equity in Vietnamese enterprises.	
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and		

	online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation		
		no express territorial scope, but would require some nexus to the jurisdiction	other
1	Decree No. 13/2023/ND-CP) (PDPD: Personal Data Protection Decree)	Article 1. Scope and regulated entities 1. This Decree provides for personal data protection and responsibilities of relevant agencies, organizations and individuals for protection of personal data. 2. This Decree applies to: a) Vietnamese agencies, organizations and individuals; b) Foreign authorities, entities and individuals in Vietnam; c) Vietnamese agencies, organizations and individuals that operate in foreign countries; d) Foreign agencies, organizations and individuals that directly process or are involved in processing personal data in Vietnam.	
2	Law on Cyber-information Security No.86/2015/QH13	Article 2. Subjects of application This Law applies to Vietnamese agencies, organizations and individuals and foreign organizations and individuals directly involved in or related to cyberinformation security activities in Vietnam.	
3	Law on Cybersecurity 24/2018/QH14		
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		

6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		Article 2. Subjects of application This Decree applies to Vietnamese and foreign organizations and individuals directly engaged in or related to the management, provision and use of Internet services, online information, and online games, and assurance of information safety and security.
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation	Representatives of controllers or processors not established in the country
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)	
2	Law on Cyber-information Security No.86/2015/QH13	
3	Law on Cybersecurity 24/2018/QH14	
4	Decree No. 53/2022/ND-CP	
5	Law on Information	

	Technology No.67/2006/QH11	
6	the Law on Protection of Consumer Rights No. 19/2023/QH15	
7	Decree regarding e-commerce, No.85/2021/NDCP	
8	Law on 86/2015/QH13	
9	Decree 27/2018/ND-CP	
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information	
11	Law No. 91/2015/QH13	
12	Law on Inspection No. 56/2010/QH12	

Notification Obligation

#	Regulation		
		Data breach notification to authorities	Data breach notification to affected individuals
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)	Article 23. Notification of violations against regulations on protection of personal data 1. In case of detection of a violation against regulations on protection of personal data, the Personal Data Controller or the Personal Data Controller-cum-Processor shall notify the Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) within 72 hours after such violation is committed according to Form No. 03 in the Appendix	

		to this Decree. If the notification is given after 72 hours, the reason for the late notification shall be provided. 2. The Personal Data Processor shall notify the Personal Data Controller as quickly as possible after detecting the violation against regulations on protection of personal data. 3. Notification contents: a) Description of the nature of the violation, including: time, place, violation, organization, individual, types of personal data and the amount of relevant data; b) Contact details of the employee (s) assigned to protect the data or organizations or individuals that are responsible for protecting personal data; c) Description of consequences and damage that may occur; d) Description of measures for handling and minimizing the harm caused by the violation. 4. If it is impossible to notify all the information specified in Clause 3 of this Article, the notification may be given every time a piece of information is available.	
2	Law on Cyber-information Security No.86/2015/QH13		
3	Law on Cybersecurity 24/2018/QH14		
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		
6	the Law on Protection of Consumer Rights No. 19/2023/QH15	In addition, the Consumer Law 2023 imposes stricter requirements concerning the time limit to notify responsible government authorities in case	

		of detecting a violation against customer data safety. Under Article 19.3 of the Consumer Law 2023, traders and parties who store customer data must notify the responsible authority within 24 hours (which is significantly shorter than the 72 hours in Decree 13/2023) upon detecting the incident or attack against customer's data safety.	
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

Obligations of Data Fiduciaries

#	Regulation	external	external
		Notification of data processing	registration of database
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)	Article 28. Sensitive personal data protection 1. Adopt measures mentioned in Clause 2 Article 26 and Article 27 of this Decree. 2. Appoint a department with the function of protecting personal data and personnel in charge of protection of personal data, and exchange information about the department and individual in charge of protection of personal data with the personal data	

		protection authority. Exchange information about the individual in charge of protection in case the Personal Data Controller, the Personal Data Controller-cum-Processor, the Personal Data Processor or the Third Party is an individual. 3. Notify the data subject of the processing of his/her sensitive personal data, except for cases specified in Clause 4, Article 13, Article 17 and Article 18 of this Decree. Article 11. Consent of a data subject 1. The consent of the data subject shall be granted to all activities in the processing of his/her personal data, unless otherwise provided for by law. 2. The consent is only valid when the data subject voluntarily consents and clearly knows the following contents: a) Type of personal data; b) Purposes; c) Organization or individual permitted to process personal data; d) Rights and obligations of the data subject. 3. The consent of the data subject shall be expressed in a clear and specific manner in writing, by voice, by ticking the consent box, by consent syntax via message, by selecting consent settings or by other forms. 4. The consent must be bound to the same purpose. In case of multiple purposes, the Personal Data Controller and the Personal Data Controller-cum-Processor shall list these purposes so that the data subject consents to one or several purposes that have been set out. 5. The consent of the data subject shall be expressed in a	

		format that can be printed and reproduced in writing, including in electronic or verifiable format. 6. Silence or non-response is not considered as consent. 7. The data subject may give partial or conditional consent. 8. In case of the processing of sensitive personal data, the data subject shall receive notification of thereof. 9. The consent of the data subject is valid until the data subject has other decisions or the competent authority makes written request. 10. In case of a dispute, the Personal Data Controller and the Personal Data Controller-cum-Processor shall prove consent of the data subject. 11. Via the authorization in accordance with regulations of the Civil Code, an organization or individual may act on behalf of the data subject to carry out procedures related to the processing of his/her personal data with the Personal Data Controller and the Personal Data Controller-cum-Processor in case the data subject knows and consents as prescribed in Clause 3 of this Article, unless otherwise provided for by law.	
2	Law on Cyber-information Security No.86/2015/QH13		
3	Law on Cybersecurity 24/2018/QH14		
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		
6	the Law on Protection of		

	Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation	external	external
		Data protection impact assessment	Others
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)	Article 24. Assessment of impact of personal data processing 1. The Personal Data Controller and the Personal Data Controller-cum-Processor shall make and store their dossiers on assessment of impact of personal data processing from the time of starting to process personal data. A dossier on assessment of impact of personal data processing includes: a) Contact information and details of the Personal Data Controller and the Personal Data Controller-cum-Processor; b) Name and contact details of the organization or employee assigned to protect personal data of the Personal Data Controller and the Personal Data	

		Controller-cum-Processor; c) Processing purposes; d) Types of personal data to be processed; dd) Data-receiving organization or individual, including the organization or individual that is located or lives outside the territory of the Socialist Republic of Vietnam; e) Cases of outbound transfer of personal data; g) Duration of processing of personal data; estimated duration of deletion or destruction of personal data (if any); h) Description of measures for protecting personal data; i) Assessment of impact of personal data processing; undesirable consequences and damage that may occur, measures for reducing or removing such consequences and damage. 2. The Personal Data Processor shall make and store the dossier on the assessment of impact of personal data processing in case the Personal Data Processor executes a contract with the Personal Data Controller. A dossier on assessment of impact of personal data processing of the Personal Data Processor includes: a) Contact information and details of the Personal Data Processor; b) Name and contact details of the organization or employee assigned to protect personal data of the Personal Data Processor; c) Description of processing of personal data and types of personal data to be processed under a contract with the Personal Data Controller; d) Duration of processing of	

		personal data; estimated duration of deletion or destruction of personal data (if any); dd) Cases of outbound transfer of personal data; e) General description of measures for protecting personal data; g) Undesirable consequences and damage that may occur, measures for reducing or removing such consequences and damage. 3. The dossier on assessment of impact of personal data processing of the Personal Data Controller, the Personal Data Controller-cum-Processor or the Personal Data Processor specified in Clause 1 and Clause 2 of this Article shall be made in writing that is valid. 4. The dossier on assessment of impact of personal data processing shall be always available in order to serve inspection and assessment by the Ministry of Public Security and the Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) shall receive 01 authentic copy according to Form No. 04 in the Appendix of this Decree within 60 days from the date of processing of personal data.	
2	Law on Cyber-information Security No.86/2015/QH13		
3	Law on Cybersecurity 24/2018/QH14	Article 11. Evaluation of cybersecurity of information systems critical for national security 1. Evaluation of cybersecurity means the activity of reviewing and assessing cybersecurity contents/items in order to provide the basis for a decision	

		on constructing or upgrading an information system. 2. Items subject to an evaluation of cybersecurity of an information system critical for national security comprise: (a) The pre-feasibility study report and design file for construction/building of the works of an investment project for construction of an information system prior to their approval; (b) The plan on upgrading an information system prior to its approval. 3. Items to be evaluated regarding cybersecurity of an information system critical for national security comprise: (a) Compliance with regulations and conditions for cybersecurity set out in the design; (b) Conformity with plans on protection, response to and remedying any incident and on deployment of human resources protecting cybersecurity. 4. Authority to evaluate cybersecurity of an information system critical for national security is regulated as follows: (a) The Cybersecurity Task Force [CTF] under the Ministry of Public Security shall evaluate cybersecurity of information systems critical for national security, except in the cases prescribed in sub-clauses (b) and (c) below; (b) The CTF under the Ministry of National Defence shall evaluate cybersecurity of military information systems; (c) The Government Cipher Committee shall evaluate cybersecurity of cipher information systems under the Government Cipher Committee.	
4	Decree No. 53/2022/ND-CP		

5	Law on Information Technology No.67/2006/QH11		
6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation	internal	internal
		technical and organisational measures	Purpose Limitation
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)	Article 3. Rules for protection of personal data 1. The personal data shall be processed as prescribed by law. 2. The data subject shall be entitled to receive information related to the processing of his/her personal data, unless otherwise provided for by law. 3. The personal data shall be processed for the purposes that have been registered and declared by the Personal Data Controller, the Personal Data Processor, the Personal Data	Article 3. Rules for protection of personal data 1. The personal data shall be processed as prescribed by law. 2. The data subject shall be entitled to receive information related to the processing of his/her personal data, unless otherwise provided for by law. 3. The personal data shall be processed for the purposes that have been registered and declared by the Personal Data Controller, the Personal Data Processor, the Personal Data

		Controller-cum-Processor and the Third Party. 4. The collected personal data shall be appropriate for the scope and purposes of processing. The purchase or sale of personal data shall be prohibited in any form, unless otherwise provided for by law. 5. The personal data shall be updated and added for the processing purposes. 6. The personal data shall be protected and secured throughout the processing. To be specific, the personal data shall be protected from violations against regulations on protection of personal data and prevention of loss, destruction or damage caused by incidents and use of technical measures. 7. The personal data shall be stored within a period of time that is appropriate for the processing purposes, unless otherwise provided for by law. 8. The Personal Data Controller and the Personal Data Controller-cum-Processor shall comply with the rules for data processing specified in Clauses 1 through 7 of this Article and prove their compliance.	Controller-cum-Processor and the Third Party. 4. The collected personal data shall be appropriate for the scope and purposes of processing. The purchase or sale of personal data shall be prohibited in any form, unless otherwise provided for by law. 5. The personal data shall be updated and added for the processing purposes. 6. The personal data shall be protected and secured throughout the processing. To be specific, the personal data shall be protected from violations against regulations on protection of personal data and prevention of loss, destruction or damage caused by incidents and use of technical measures. 7. The personal data shall be stored within a period of time that is appropriate for the processing purposes, unless otherwise provided for by law. 8. The Personal Data Controller and the Personal Data Controller-cum-Processor shall comply with the rules for data processing specified in Clauses 1 through 7 of this Article and prove their compliance.
2	Law on Cyber-information Security No.86/2015/QH13		
3	Law on Cybersecurity 24/2018/QH14	Article 23. Implementation of cybersecurity protective activities in State agencies and political organizations at the central and local levels 1. Contents of implementation of cybersecurity protective activities comprise: (a) Formulating and completing rules and regulations on use of local area networks and Internetconnected computer networks; plans for ensuring	

		cybersecurity of information systems; and plans for responding to and remedying cybersecurity incidents; (b) Applying and implementing plans, measures and technology to protect cybersecurity of information systems and of information and data archived, drafted and transmitted on information systems within the scope of their managerial authority [managed by such State agencies and political organizations]; (c) Organizing retraining on cybersecurity knowledge for cadres [senior officials], other officials and employees; increasing the capability of Cybersecurity Task Forces [CTF] to protect cybersecurity; (d) Protecting cybersecurity in the following activities: providing public services in cyberspace; providing information to, exchanging information with and collecting information from agencies, organizations and individuals; sharing information internally and with other agencies or during other activities in accordance with Government regulations; (dd) Conducting investment in and building physical infrastructure in conformity with conditions for ensuring implementation of cybersecurity protective activities for information systems; (e) Inspecting cybersecurity of information systems; preventing and combating breaches of the law on cybersecurity; responding to and remedying cybersecurity incidents. 2. Heads of agencies and organizations are responsible to carry out cybersecurity protective activities [for	

		networks] within the scope of their managerial authority.	
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		
6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation	internal	internal
		Accuracy	Retention Limitation
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)	Article 3. Rules for protection of personal data 1. The personal data shall be processed as prescribed by law. 2. The data subject shall be entitled to receive information related to the processing of his/her personal data, unless otherwise provided for by law. 3. The personal data shall be processed for the purposes that have been registered and	Article 3. Rules for protection of personal data 1. The personal data shall be processed as prescribed by law. 2. The data subject shall be entitled to receive information related to the processing of his/her personal data, unless otherwise provided for by law. 3. The personal data shall be processed for the purposes that have been registered and

		declared by the Personal Data Controller, the Personal Data Processor, the Personal Data Controller-cum-Processor and the Third Party. 4. The collected personal data shall be appropriate for the scope and purposes of processing. The purchase or sale of personal data shall be prohibited in any form, unless otherwise provided for by law. 5. The personal data shall be updated and added for the processing purposes. 6. The personal data shall be protected and secured throughout the processing. To be specific, the personal data shall be protected from violations against regulations on protection of personal data and prevention of loss, destruction or damage caused by incidents and use of technical measures. 7. The personal data shall be stored within a period of time that is appropriate for the processing purposes, unless otherwise provided for by law. 8. The Personal Data Controller and the Personal Data Controller-cum-Processor shall comply with the rules for data processing specified in Clauses 1 through 7 of this Article and prove their compliance. Article 42. Responsibilities of relevant organizations and individuals 1. Adopt measures for protecting their personal data, take responsibility for the accuracy of the personal data provided.	declared by the Personal Data Controller, the Personal Data Processor, the Personal Data Controller-cum-Processor and the Third Party. 4. The collected personal data shall be appropriate for the scope and purposes of processing. The purchase or sale of personal data shall be prohibited in any form, unless otherwise provided for by law. 5. The personal data shall be updated and added for the processing purposes. 6. The personal data shall be protected and secured throughout the processing. To be specific, the personal data shall be protected from violations against regulations on protection of personal data and prevention of loss, destruction or damage caused by incidents and use of technical measures. 7. The personal data shall be stored within a period of time that is appropriate for the processing purposes, unless otherwise provided for by law. 8. The Personal Data Controller and the Personal Data Controller-cum-Processor shall comply with the rules for data processing specified in Clauses 1 through 7 of this Article and prove their compliance.
2	Law on Cyber-information Security No.86/2015/QH13		

3	Law on Cybersecurity 24/2018/QH14		
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		
6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation	internal	internal
		drawing up of codes of conduct	record of processing activities
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)		Article 38. Responsibility of Personal Data Controllers 1. Implement organizational and technical measures and appropriate safety and security measures to prove that the personal data is processed in accordance with regulations of the law on protection of personal data, review and update these measures when necessary.

			2. Record and store log of the processing of personal data. 3. Notify violations against regulations on protection of personal data according to regulations in Article 23 of this Decree. 4. Select an appropriate Personal Data Processor with specific tasks and only work with the Personal Data Processor that has appropriate measures for protecting personal data. 5. Protect the rights of data subjects according to regulations in Article 9 of this Decree. 6. Be responsible to the data subject for damage caused by the processing of personal data. 7. Cooperate with the Ministry of Public Security and competent authorities in protecting personal data and providing information serving investigation and handling of violations against the law on protection of personal data. ---
2	Law on Cyber-information Security No.86/2015/QH13		
3	Law on Cybersecurity 24/2018/QH14	Article 23. Implementation of cybersecurity protective activities in State agencies and political organizations at the central and local levels 1. Contents of implementation of cybersecurity protective activities comprise: (a) Formulating and completing rules and regulations on use of local area networks and Internetconnected computer networks; plans for ensuring cybersecurity of information systems; and plans for responding to and remedying cybersecurity incidents; (b) Applying and implementing plans, measures and technology	

		to protect cybersecurity of information systems and of information and data archived, drafted and transmitted on information systems within the scope of their managerial authority [managed by such State agencies and political organizations]; (c) Organizing retraining on cybersecurity knowledge for cadres [senior officials], other officials and employees; increasing the capability of Cybersecurity Task Forces [CTF] to protect cybersecurity; (d) Protecting cybersecurity in the following activities: providing public services in cyberspace; providing information to, exchanging information with and collecting information from agencies, organizations and individuals; sharing information internally and with other agencies or during other activities in accordance with Government regulations; (dd) Conducting investment in and building physical infrastructure in conformity with conditions for ensuring implementation of cybersecurity protective activities for information systems; (e) Inspecting cybersecurity of information systems; preventing and combating breaches of the law on cybersecurity; responding to and remedying cybersecurity incidents. 2. Heads of agencies and organizations are responsible to carry out cybersecurity protective activities [for networks] within the scope of their managerial authority.	
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology		

	No.67/2006/QH11		
6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation	internal	internal
		Designation of the data protection officer	Others
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)		
2	Law on Cyber-information Security No.86/2015/QH13		
3	Law on Cybersecurity 24/2018/QH14		
4	Decree No. 53/2022/ND-CP		

5	Law on Information Technology No.67/2006/QH11		
6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

Data Cross Boarder Dist

#	Regulation	Cross-border data transfer & Exceptions	Data localization
		Provisions for Transborder Data Transfer. What are the exceptions?(e.g., sufficient authorization, transfers based on contracts equivalent to Standard Contract Clauses (SCC) or Binding Corporate Rules (BCR), transfers based on corporate certification, etc.), Transborder transfer assessment (TIA)	Presence or absence of provisions, stipulations regarding the types of data that must be stored in the country
		Provisions for cross boarder data transfer	Provisions on requirement of localization; and

			Type of data required for localization
1	Decree No. 13/2023/ND-CP) (PDPD : Personal Data Protection Decree)	Article 2. Definition of terms 14. "Outbound transfer of personal data" refers to an act of using cyberspace, electronic devices, equipment, or other forms to transfer personal data of a Vietnamese citizen to a location outside the territory of the Socialist Republic of Vietnam or using a location outside the territory of the Socialist Republic of Vietnam to process personal data of a Vietnamese citizen. To be specific: a) An organization, enterprise or individual transfers personal data of a Vietnamese citizen to an overseas organization, enterprise or management department in order to process the data for the purposes agreed upon by the data subject; b) The personal data of a Vietnamese citizen is processed by automatic systems outside the territory of the Socialist Republic of Vietnam of the Personal Data Controller, Personal Data Controller-cum-Processor, Personal Data Processor for the purposes agreed upon by the data subject. Article 25. Outbound transfer of personal data 1. A Vietnamese citizen's personal data shall be transferred abroad in case where the Sender makes a dossier on assessment of impact of outbound transfer of personal data and carries out the procedures specified in Clauses 3, 4 and 5 of this Article. The senders include the Personal Data Controller, the Personal Data Controller-cum-Processor, the Personal Data Processor and the Third Party. 2. A dossier on assessment of impact of outbound transfer of	

		personal data includes: a) Contact information and details of the Sender and the Receiver; b) Full name and contact details of an organization or individual under the Sender involved in sending and receiving a Vietnamese citizen's personal data; c) Description and explanation about objectives of the processing of a Vietnamese Citizen's personal data after the personal data is transferred abroad; d) Description and clarification of type of personal data to be transferred abroad; dd) Description and explanation about the observance of regulations on protection of personal data in this Decree, detailed measures for protecting personal data; e) Assessment of impact of personal data processing; undesirable consequences and damage that may occur, measures for reducing or removing such consequences and damage. g) Consent of the data subject according to regulations in Article 11 of this Decree when he/she is informed of the mechanism for feedback and complaint in case of arising problems or requests; h) Document that shows obligations and responsibilities between the Senders and the Receivers for processing of a Vietnamese Citizen's personal data. 3. A dossier on assessment of impact of outbound transfer of personal data shall be always available in order to serve inspection and assessment by the Ministry of Public Security. The Sender shall send 01	

		authentic copy of the assessment to the Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) according to Form No. 06 in the Appendix of this Decree within 60 days from the date of processing of personal data. 4. The Sender shall notify the Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) of information about the data transfer and contact details of the organization or individual in charge of such transfer in writing after the personal data is successfully transferred. 5. The Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) shall make assessment and request the Sender to complete the dossier on assessment of impact of outbound transfer of personal data in case the assessment is not complete and accurate according to regulations. 6. The Sender shall update and amend the dossier on assessment of impact of outbound transfer of personal data when there is any change of contents submitted to the Ministry of Public Security (Department of Cybersecurity and Hi-tech Crime Prevention) according to Form No. 05 in the Appendix of this Decree. The duration for completion of the dossier on assessment for the Sender is 10 days from the date of request. 7. According to specific situation, the Ministry of Public Security shall decide to inspect the outbound transfer of personal data once a year, unless it detects violations against the law on protection of personal data in	

		this Decree or a Vietnamese citizen's personal data is leaked or lost. 8. The Ministry of Public Security shall decide to request the Sender to stop transferring personal data abroad in the following cases: a) It is detected that the transferred personal data is used for activities that violate the interests and national security of the Socialist Republic of Vietnam. b) The Sender does not comply with regulations in Clause 5 and Clause 6 of this Article; c) A Vietnamese citizen's personal data is leaked or lost.	
2	Law on Cyber-information Security No.86/2015/QH13	Article 34. Export and import of civil cryptographic products 1. If wishing to export and import civil cryptographic products on the list of civil cryptographic products subject to export and import permit, an enterprise must obtain a permit for export and import of civil cryptographic products from a competent state agency.	
3	Law on Cybersecurity 24/2018/QH14		Article 26. Guarantees relating to information security in cyberspace 3. Domestic and foreign service providers on telecom networks and on the Internet and other value added services in cyberspace in Vietnam [cyberspace service providers] carrying out Unofficial Translation. For Reference only 24 www.economica.vn activities of collecting, exploiting [using], analysing and processing data [being] personal information, data about service users' relationships and data generated by service users in Vietnam must store such data in Vietnam for a [specified] period [to be] stipulated by the Government. Foreign enterprises

			referred to in this clause must have branches or representative offices in Vietnam.
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		
6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP	Cross-border e-commerce activities of foreign entities are now in scope of Decree 85 Decree 85 adds a separate section governing the cross-border e-commerce activities of foreign entities, including those having websites to provide e-commerce services in Vietnam and those selling goods in Vietnam's e-commerce websites. A foreign entity is considered as having a website to provide e-commerce services in Vietnam if its website is either (i) set up under a Vietnam's domain name (.vn) or (ii) displayed in Vietnamese language or (iii) having over 100,000 transactions from Vietnam per year. Accordingly, the foreign entity must register its e-commerce activities in Vietnam with the Ministry of Trade and Industry ("MOIT") and must establish its representative office in Vietnam or appoint someone to act as their authorized representative in Vietnam. This requirement must be done within 12 months from 1 January 2022. Whilst, a foreign entity selling goods in Vietnam's e-commerce websites must (i) have a trading (import) permit granted by the MOIT or (ii) arrange for the import of goods as entrusted by the buyers or (iii)	

		appoint its commercial agents in Vietnam for the import of goods into Vietnam. The Vietnam's e-commerce website providers shall be responsible for verifying the foreign entity's identity and its satisfaction of one of these requirements.	
8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP	Cross-border data transfers In addition, the draft Decree details obligations for foreign organizations and individuals providing services on a cross-border basis and using data storage leasing services in Vietnam, or that have 100,000 total visits for six consecutive months from Vietnam. These include, among other things: notifying the MIC within 60 days of reaching the number of visitors stipulated above; preventing and removing illegal content, services, and applications at the request of the MIC; storing the personal information of Vietnamese users, and providing such personal information to competent State authorities on request; only allowing users in Vietnam over the age of 16 years or older to register for an account; having a specialized department for receiving, processing, and responding to requests from competent authorities, and resolving and responding to complaints from Vietnamese users; and within 48 hours of receiving complaints from Vietnamese users, handling complaints by blocking content.	
10	Decree No. 72/2013/ND-CP of July 15, 2013,		

	on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		

#	Regulation	Governent Access
		National Security Law, Cybersecurity Law Provisions
		Provision allowed govt to access regulated data/to not comply to data regulation
1	Decree No. 13/2023/ND-CP) (PDPD：Personal Data Protection Decree)	
2	Law on Cyber-information Security No.86/2015/QH13	
3	Law on Cybersecurity 24/2018/QH14	
4	Decree No. 53/2022/ND-CP	
5	Law on Information Technology No.67/2006/QH11	
6	the Law on Protection of Consumer Rights No. 19/2023/QH15	
7	Decree regarding e-commerce, No.85/2021/NDCP	
8	Law on 86/2015/QH13	
9	Decree 27/2018/ND-CP	

10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information	
11	Law No. 91/2015/QH13	
12	Law on Inspection No. 56/2010/QH12	

Penalties

#	Regulation	Corporate Punishments	Individual Punishments
		Forms of penalties (e.g., recommendations for corrective action, public penalties, fines, confiscation of assets and income, data deletion, data processing, business suspension, etc.)	Penalties (penalties, fines, demotion, etc.)
		Forms of penalties on corporate	Forms of penalties on individual
1	Decree No. 13/2023/ND-CP) (PDPD: Personal Data Protection Decree)	Penalties for violations of this decree will be set forth in a separate decree (Cybersecurity Administrative Sanctions Decree). It should be noted that many fines related to PDPD violations have been reduced compared to the previous draft. However, the maximum fixed monetary fine remains VND 1 billion (approx. US$39,285), and severe violations can incur penalties up to 5 percent of the violating enterprise's turnover in the previous fiscal year in Vietnam. **** Article 4. Handling violations against regulations on protection of personal data Agencies, organizations and individuals that commit violations against regulations on protection of personal data, depending on the severity of	

		their violations, may be disciplined, or face administrative penalties or criminal prosecution according to regulations. Article 8. Prohibited acts 1. Processing personal data in contravention of regulations of law on protection of personal data. 2. Processing personal data in order to provide information and data against regulations of the Socialist Republic of Vietnam 3. Processing personal data in order to provide information and data that affect national security, social order and safety, and legitimate rights and interests of other organizations and individuals. 4. Obstructing protection of personal data by competent authorities. 5. Taking advantage of protection of personal data to commit violations of law.	
2	Law on Cyber-information Security No.86/2015/QH13		
3	Law on Cybersecurity 24/2018/QH14		
4	Decree No. 53/2022/ND-CP		
5	Law on Information Technology No.67/2006/QH11		
6	the Law on Protection of Consumer Rights No. 19/2023/QH15		
7	Decree regarding e-commerce, No.85/2021/NDCP		

8	Law on 86/2015/QH13		
9	Decree 27/2018/ND-CP		
10	Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information		
11	Law No. 91/2015/QH13		
12	Law on Inspection No. 56/2010/QH12		