ERIA Discussion Paper Series

No. 539

Current Status of ASEAN Data Governance and Its Implications for the Digital Economy Framework Agreement

Shota WATANABE
Nomura Research Institute (NRI)

Ema OGURA
Nomura Research Institute (NRI)

Keita OIKAWA
Economic Research Institute for ASEAN and East Asia (ERIA)

January 2025

Abstract: *The transition to data-driven societies has heightened the importance of balancing the free flow of data with robust data protection for privacy, intellectual property, trade secrets, and national security. While different countries have introduced various data governance frameworks, including comprehensive privacy laws, differences in regulations across borders hinder data flow, increasing compliance costs and limiting business expansion, especially for small and medium-sized enterprises. The concept of Data Free Flow with Trust (DFFT), introduced at the G20 in 2019, aims to address this balance by promoting interoperability while respecting national sovereignty. In ASEAN, however, regulatory fragmentation further complicates cross-border data flow. Variations in data localisation policies and personal data governance amongst ASEAN Member States (AMS) create significant challenges for businesses. For instance, differences in requirements for sensitive data, data subject rights, and security measures necessitate additional compliance efforts for companies operating in multiple jurisdictions. Moreover, non-personal data regulations, such as restrictions on supply chain and research and development (R&D) data sharing or mandatory technology transfers, impede global R&D collaboration and discourage investment in certain countries. This study provides a comprehensive analysis of data-related regulations in ASEAN and proposes policy recommendations for the ASEAN Digital Economy Framework Agreement (DEFA), set for 2025. It highlights the need for transparency, regulatory alignment, and various mechanisms to ensure smoother cross-border data flow, ultimately fostering regional digital integration.*

Keywords: ASEAN, data governance, Data Free Flow with Trust (DFFT), ASEAN Digital Economy Framework Agreement (DEFA)

JEL Classification: K2

1. Introduction

The importance of data utilisation in economic development has grown significantly as societies are increasingly transitioning into data-driven ones. In such data-centric societies and economies, supply chains are deeply interconnected; thus, it is necessary to ensure the free flow of data, allowing various stakeholders to access data across borders effectively. While the importance of the free flow of data continues to rise, it is equally imperative to properly protect data for legitimate purposes such as privacy, intellectual property, trade secrets, and national security. To address these concerns, various data governance regulations, including the enactment of comprehensive privacy protection legislation, have been introduced across countries and regions. While the regulatory sovereignty of each country must be respected, the benefits of digitisation cannot be realised without balancing these regulations with the need for the free flow of data.

The international issue of balancing the free flow and protection of data has been discussed in several international forums, such as the G7 and G20, under the concept of Data Free Flow with Trust (DFFT). Proposed by the Government of Japan at the G20 in 2019, DFFT has since gained frequent support at the G7 and G20 summits (Oikawa, 2024). These discussions have been accompanied by studies on data governance conducted by the Organisation for Economic Co-operation and Development (OECD) Secretariat, contributing to a growing body of knowledge on the topic. For example, it has been well documented that basic concepts – such as the definition of data and implementation of data localisation, which mandates that data be processed and stored within national borders – vary between countries. These differences in data governance frameworks have led to situations where companies are unable to transfer necessary data across borders. The resulting compliance costs associated with navigating these disparate regulations are hindering global business development, especially for small and medium-sized enterprises. To address these challenges, previous studies have explored possible solutions, such as trade agreements and certification systems, to enhance interoperability amongst domestic systems. These approaches aim to respect the regulatory sovereignty of each country while maximising the free flow of data.

Balancing the free flow and protection of data is also an important issue within ASEAN. Previous research regarding personal data protection regulations in ASEAN Member States (AMS) indicates that the types of data localisation (EU–ASEAN Business Council, 2020:22–24) and conditionally allowed cross-border transfer restrictions (Liu, Sengstschmid, Ge, 2023:7–9) differ amongst AMS, which results in restricting the free flow of data within

ASEAN. To balance the free flow and protection of data, it is necessary to examine the following two key types of data protection regulations in addition to the aforementioned regulations.

The first type concerns data protection regulations that govern the handling of personal data within a country's jurisdiction. Previous studies have analysed differences amongst AMS regarding such regulations, focussing on specific aspects involving sensitive information such as gender identity, race, personal information on children, and data breach notifications. These domestic variations in managing personal data can pose challenges for businesses operating across multiple countries (Liu, Sengstschmid, Ge, 2023). However, differences in broader personal data governance beyond sensitive information – such as the rights of data subjects[1] and security measures – also affect cross-border data flow (UNCTAD, 2023; Fritz and Giardini, 2023). For example, if a company can process personal data without consent in its home country to fulfil a contract but is required to obtain explicit consent in another country, this discrepancy necessitates additional compliance efforts. Businesses seeking to expand into a new country must notify individuals to obtain consent, revise privacy policies, adjust their legal basis, and modify data-processing practices accordingly. This regulatory fragmentation prevents the region from fully realising its digital potential. Coordinating data protection regulations amongst AMS at a certain level is therefore crucial to enable smoother cross-border data flow and to foster regional digital integration.

The other type of regulation concerns data protection for non-personal data. While previous studies have focussed on personal data, companies also manage large volumes of non-personal data, such as supply chain data and research and development (R&D) data. For example, if the integration or sharing of R&D data across multiple countries is prohibited by data localisation regulations, this could hinder companies' ability to establish global R&D structures, leading to businesses avoiding conducting R&D in countries where such data localisation regulations are enforced. In addition, in cases where governments mandate technology transfer, companies may hesitate to expand their operations into those countries due to concerns about losing the competitive advantage gained from their R&D investment. Thus, regulations affecting the flow of non-personal data also have significant impacts on cross-border data flow.

Considering above issues, based on previous studies on data-related regulations in ASEAN and other countries around the world, this study conducts a more comprehensive

[1] An identified or identifiable natural person with respect to personal data.

analysis of the current state of data-related regulations across the 10 AMS. It also developed policy recommendations for the ASEAN Digital Economy Framework Agreement (DEFA), which is expected to be concluded by 2025, to enhance cross-border data flow. Section 2 analyses current data-related regulations in AMS, exploring challenges that ASEAN faces in realising DFFT. Section 3 proposes potential solutions to address these challenges. Lastly, Section 4 presents policy recommendations for the DEFA based on the findings of this study.

2. Current Status of Data-related Regulations in ASEAN

This section evaluates current data-related regulations in each AMS, focussing on their impacts on companies operating across multiple AMS. When companies enter foreign markets and conduct business, they manage both the personal data of customers and employees as well as non-personal data generated through business activities unrelated to the identification of individuals. Companies must also comply with data protection regulations in foreign countries when acquiring foreign-protected data directly from their home country. Moreover, they need to comply with these regulations when transferring data to their home country once data have been acquired by a customer, supplier, or group company located abroad. When companies transfer data acquired in their home country to entities in foreign countries, they must comply with cross-border data transfer regulations of their home country, which vary depending on the destination country.

As a result, companies incur business costs to scrutinise these data-related regulations and to implement necessary compliance measures. Furthermore, data-related regulations themselves, regardless of cross-border data transfers, are directly linked to business costs. If countries do not carefully consider the impacts of these regulations on business activities before enacting and enforcing them, they may damage their competitiveness as favourable locations for business operations.

To understand how these data-related regulations impact corporate activities, the content and differences of domestic regulations of AMS are analysed below, identifying institutional issues. This analysis includes aspects such as the definition of data and scope of exceptions for restrictions on cross-border data transfers. First, the structure of data protection regulations is reviewed to gain an overall picture. Next, these regulations are categorised into two types: (i) domestic data flow regulations, which govern the handling of data acquired within a country, and (ii) cross-border data flow regulations, which govern the transfer of data to foreign countries.

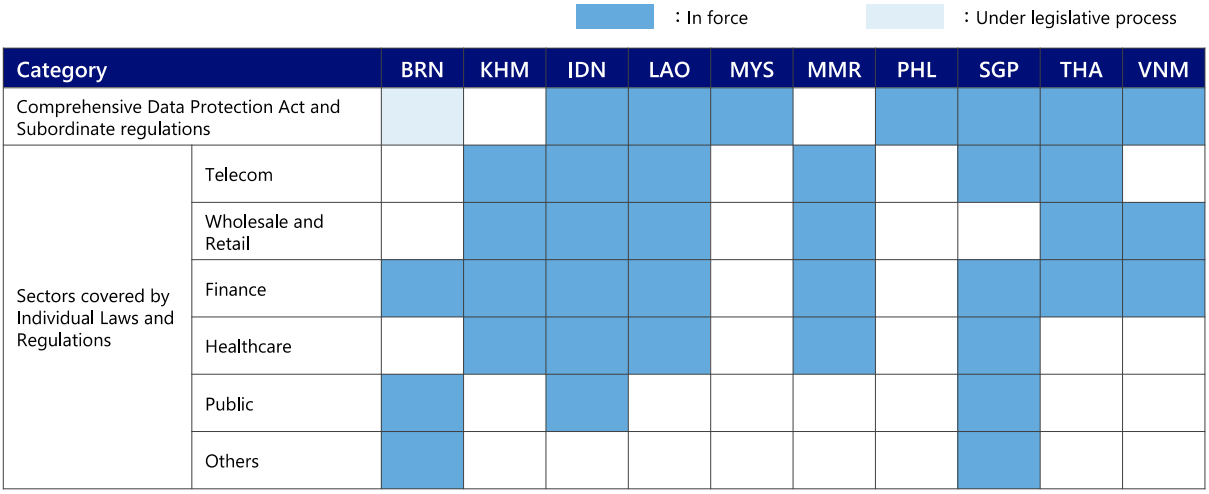
2.1. Structure of Data Protection Regulations

There are two types of legal systems for privacy protection: (i) comprehensive regulations and (ii) sector-specific regulations. Comprehensive regulations apply across all sectors and industries, governing the processing of personal data by companies and other entities. In contrast, sector-specific regulations consist of individual laws that regulate the protection of personal data only within specific sectors and industries. As Table 1 indicates, seven AMS have enacted and implemented comprehensive personal data protection regulations.[2]

Comprehensive regulations provide consistent personal data protection across all industries. Conversely, countries without comprehensive regulations impose personal data protection only in industries where specific laws exist. As a result, in the absence of comprehensive regulations, certain sectors or industries may lack adequate personal data protection. This inconsistency creates challenges for companies transferring personal data across borders. For instance, if the receiving (i.e. foreign) country lacks comprehensive personal data protection regulations, the originating (i.e. home) country's regulations may prohibit the transfer of personal data. Alternatively, the home country may require companies to implement additional protection measures. Even when explicit restrictions are absent in the home country, companies may still face difficulties in ensuring that foreign companies receiving the data comply with the standards of personal data protection required by the home country.

[2] Brunei Darussalam has enacted these regulations, but their implementation is pending.

Table 1: Comprehensive or Sector-specific Regulations for Personal Data Protection across ASEAN



BRN = Brunei Darussalam, IDN = Indonesia, KHM = Cambodia, LAO = Lao People's Democratic Republic, MMR = Myanmar, MYS = Malaysia, PHL = Philippines, SGP = Singapore, THA = Thailand, VNM = Viet Nam.
Source: Authors.

To facilitate seamless data flow within the ASEAN region, it is essential to properly protect both personal and non-personal data. Corporate trade secrets, such as valuable technology and know-how that are managed internally and not publicly available, are examples of non-personal data that require protection. Such information is typically protected by intellectual property laws, granting companies legal rights to protect trade secrets. From a company's perspective, unrestricted government access to non-personal data in certain jurisdictions poses significant risks. Companies may hesitate to transfer sensitive non-personal data to countries with such policies, hindering international business expansion. Furthermore, countries allowing extensive government access may find their attractiveness as business locations diminished.

Overly restrictive regulations on non-personal data can also impede business activities. For example, data generated through the internet of things, supply chain management, and R&D is crucial for digitising corporate value chains, such as manufacturing processes. Modern information and communications technology (ICT) has enabled the unbundling of a company's internal value chain. The ability to optimally position the value chains globally is key for enhancing company's competitiveness. Data localisation measures, as discussed below, can prevent the cross-border flows of such non-personal data. This restriction can damage these global value chains, harming companies' competitiveness. Additionally, from the perspective of companies in other countries, the attractiveness of a country with data localisation

diminishes, leading to a loss of locational competitiveness for that country. To avoid unnecessary restrictions on business activities, regulations on non-personal data should be limited to measures essential for achieving legitimate public policy objectives. Policymakers must carefully identify industries requiring special protection, such as ICT and trade, and the scope of data regulations appropriately.

As shown in Table 2, non-personal data protection approaches vary amongst AMS. Some employ comprehensive regulations, similar to personal data frameworks, offering uniform protection across all industries. Others rely on sector-specific regulations, which target particular sectors or industries for data protection.

Table 2: Comprehensive or Sector-specific Regulations for Non-personal Data Protection across ASEAN

: In force

Category		BRN	KHM	IDN	LAO	MYS	MMR	PHL	SGP	THA	VNM
Comprehensive Data Protection Act and Subordinate regulations of the DPA					■						
Sectors covered by Individual Laws and Regulations	Telecom			■							
	Wholesale and Retail			■						■	
	Finance			■							
	Healthcare			■							
	Public			■							
	Others			■							

BRN = Brunei Darussalam, DPA = Data Protection Act, IDN = Indonesia, KHM = Cambodia, LAO = Lao People's Democratic Republic, MMR = Myanmar, MYS = Malaysia, PHL = Philippines, SGP = Singapore, THA = Thailand, VNM = Viet Nam.
Source: Authors.

For example, the Electronic Data Protection Law of the Lao Democratic People's Republic (Lao PDR) protects national security and trade secrets, such as proprietary technology and know-how, across all industries. The law mandates clear communication about data collection purposes to data owners.[3] Additionally, the data must be managed appropriately. In Indonesia, the Electric Information and Transactions Law protects both personal and non-personal data, including text, voice, images, maps, documents, photographs, electronic data interchange, e-mail, telegrams, telexes, telecopies, and other electronic data. Its scope is limited to data processed within electronic systems.

[3] A data owner is the individual, legal entity, or organisation who/which is the owner of the electronic data.

In contrast, Thailand's Trade Secret Act (2015) provides sector-specific protection. This law protects trade secrets within the trade and commerce sector, requiring companies to ensure that information with commercial value due to its confidentiality is adequately protected. Companies must implement appropriate measures to maintain confidentiality, which may include internal rules of companies, such as work rules. Furthermore, information management systems, including internal training and audits, must be established.

Comprehensive regulations provide a unified framework for ensuring that companies handle data securely within a country. They help prevent the leakage of non-personal data across sectors in the country, thereby offering a low-risk environment for data handling. However, these regulations can impose significant compliance burdens on companies by mandating protection of data that may not be crucial to their businesses. Sector-specific regulations, in contrast, allow for more targeted data protection, imposing obligations tailored to the specific needs of individual industries. For non-personal data, it would be beneficial to design regulations by using a layered approach or sector-specific rules, based on the specific purpose of protection. These purposes could include preventing the leakage of trade secrets or addressing security concerns.

2.2. Classification of Data Protection Regulations

This sub-section analyses current regulatory trends by categorising data protection regulations into domestic and cross-border data flow regulations. Both categories include regulations governing the protection of personal and non-personal data.

2.2.1. Domestic Data Flow Regulations

2.2.1.1.Legal Basis for Personal Data Processing

Table 3 indicates that the six legal bases for processing personal data, which are defined and permitted under the General Data Protection Regulation (GDPR) of the European Union (EU) – 'obtaining consent',[4] 'fulfilling a contract',[5] 'complying with legal obligations',[6]

[4] Obtaining consent entails the data subject giving consent for the handling of data for a specific purpose.

[5] Fulfilling a contract entails processing a data subject's data for the delivery of goods or services purchased by the data subject.

[6] Complying with legal obligations denotes data processing required when complying with legal obligations to which the data controller is subject.

'protecting vital interests',[7] 'protecting public interests',[8] and 'legitimate interests'[9] – are widely recognised in Indonesia, Malaysia, the Philippines, Singapore, and Thailand. However, Myanmar currently recognises only 'obtaining consent' as a lawful basis for processing personal data, imposing a significant burden on data controllers for ensuring lawful data processing. Furthermore, Brunei Darussalam stands out as the only jurisdiction that stipulates opting out[10] as a legal basis. There, data controllers may process personal data after conducting prescribed assessments for adverse effects on the individual, notify the individual of the new purpose, and provide a reasonable period of time for them to opt out.

The lack of flexibility in legal bases can lead to higher compliance costs. Companies may avoid receiving personal data from countries with limited legal bases for processing personal data. For example, if a company relies on 'fulfilling a contract' as the legal basis in its home country but processes personal data from a foreign country that does not recognise this basis, such processing would violate the laws of the foreign country.[11] To address this, it is desirable to establish a wider range of legal bases for data processing within the ASEAN region. Providing companies with diverse options would reduce compliance burdens and facilitate operations across the region.

[7] Protecting vital interests represents data processing necessary when protecting data subjects or other human life.

[8] Protecting public interests denotes the processing of data necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

[9] Legitimate interests represent data processing where the processing is necessary for purposes of legitimate interests as required by the data controller or by a third party.

[10] Opting out refers to the practice of providing personal data to third parties without the explicit consent of the individual, as long as the individual has not requested the cessation of such provision.

[11] If legality is recognised solely on the basis of obtaining the person's consent, actions undertaken for fulfilling a contract may not be deemed lawful. For example, a company operating an e-commerce site may process a user's information (e.g. address or telephone number) for the purpose of shipping goods under the legal basis of 'fulfilling a contract'. However, this would not be lawful in countries where 'fulfilling a contract' is not recognised as a valid legal basis for data processing.

Table 3: Legal Bases for Personal Data Processing across ASEAN

: In force : Under legislative process

Category	BRN	KHM	IDN	LAO	MYS	MMR	PHL	SGP	THA	VNM
Consent		▲				▲				
Performance of a contract				▲						
Legal obligation		▲								
Vital interests		▲								
Public interest		▲								
Legitimate interests				▲						
Opt-out										
Others	*1					▲*2				

BRN = Brunei Darussalam, IDN = Indonesia, KHM = Cambodia, LAO = Lao People's Democratic Republic, MMR = Myanmar, MYS = Malaysia, PHL = Philippines, SGP = Singapore, THA = Thailand, VNM = Viet Nam.

Notes:

1. Consent entails the data subject giving consent for the handling of data for a specific purpose.
2. Performance of a contract entails processing a data subject's data for the delivery of goods or services purchased by the data subject.
3. Legal obligation denotes data processing required when complying with legal obligations to which the data controller is subject.
4. Vital interests represents data processing necessary when protecting data subjects or other human life.
5. Public interest denotes the processing of data necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
6. Legitimate interests represent data processing where the processing is necessary for purposes of legitimate interests as required by the data controller or by a third party.
7. Opt-out refers to the practice of providing personal data to third parties without the explicit consent of the individual, as long as the individual has not requested the cessation of such provision.
8. A black triangle indicates that the regulations in question apply only to sectors covered by the individual laws and regulations shown in Table 1.
9. *1 indicates that if the individual, without giving express consent, voluntarily provides personal data for that purpose, it is reasonable to assume that the individual voluntarily provides the data.
10. *2 identifies the person who will collect the data or ensures that the data will not be used for any other improper purpose.

Source: Authors.

2.2.1.2. Rights of the Data Subject

Table 4 shows that the rights granted to data subjects under data protection regulations vary significantly across AMS. Amongst those with comprehensive data protection regulations, the only universally recognised right is the 'right of access to data'.[12]

In countries such as Indonesia,[13] the Philippines, Thailand, and Viet Nam, data subjects are granted rights similar to those under the GDPR. These include the right of access,

[12] The right of access to data is the right of data subjects to request a copy of the contents of personal data held by a data controller if they request to know what personal data are held about them.

[13] After the Personal Data Protection (PDP) Law in October 2022.

rectification, deletion (or the right to be forgotten), discontinuation of data processing, data portability, and to be informed and notified. However, discrepancies in the recognition of these rights create challenges for cross-border data transfer. For example, if a company transfers personal data to a foreign country where the right to delete data is not recognised, data subjects from the home country may be unable to exercise this right in the foreign country. To protect the rights of data subjects, companies need to compare rights of data subjects recognised in their home country with those in the foreign country. They should then establish additional data protection contracts with the receiving company to ensure the preservation of these rights. The necessity of these actions places additional compliance burdens on the private sector.

Table 4: Rights of Data Subjects across ASEAN

: In force : Under legislative process

Category	BRN	KHM	IDN	LAO	MYS	MMR	PHL	SGP	THA	VNM
Right to be informed			■				■		▲	▲
Right of access	□	▲	■	■	■		■	■		▲
Right to rectification	□	▲	■	■	■		■	■	▲	▲
Right to erasure			■	■			■		■	▲
Right to restrict processing		▲	■	■	■		■		■	■
Right to data portability	□		■	■			■	■	■	
Right to object			■	■			■		■	■
Right not to be subject to a decision based solely on automated processing			■							▲
Right to withdraw consent	□		■		■		■	■	■	■
Others				*1					*2	

BRN = Brunei Darussalam, IDN = Indonesia, KHM = Cambodia, LAO = Lao People's Democratic Republic, MMR = Myanmar, MYS = Malaysia, PHL = Philippines, SGP = Singapore, THA = Thailand, VNM = Viet Nam.

Notes:

1. Right to be informed ensures that data subjects are provided with clear and comprehensive information about how their personal data is being collected, used, and processed.
2. Right to access allows data subjects to obtain confirmation about whether their personal data is being processed and to access that data along with supplementary information.
3. Right to rectification gives data subjects the ability to request the correction of inaccurate or incomplete personal data concerning them.
4. Right to erasure, also known as the right to be forgotten, allows data subjects to request the deletion of their personal data under certain circumstances, such as when the data is no longer necessary for the original purposes of processing.
5. Right to restrict processing enables data subjects to limit the processing of their personal data, typically in situations where the accuracy of the data is contested or its processing is unlawful.
6. Right to data protability allows data subjects to receive their personal data and to transmit it to another data controller.
7. Right to object permits data subjects to object to the processing personal data based on legitimate interests, direct marketing, etc.
8. Right not to be subject to a decision based solely on automated processing protects data subjects from being subject to decisions maede entirely by automated means, including profiling, which produce significant legal or similarly impactful effects on them.
9. Right to withdraw consent allows data subjects to revoke their previously given consent for the

processing of their personal data at any time, without affecting the lawfulness of prior processing based on that consent.

10. A black triangle indicates that the regulations in question apply only to sectors covered by the individual laws and regulations shown in Table 1.
11. *1 indicates the right to notify the data administration authority and other relevant sectors to secure electronic data when the data have been damaged or are at risk.
12. *2 indicates the right to obtain a copy of personal data and the right to receive personal data from the data controller. The data controller shall arrange such personal data in a format that is readable or commonly used by automated tools or equipment and can be used or disclosed through automated means.

Source: Authors.

2.2.1.3. Extraterritorial Application of Personal Data Protection Regulations

While the scope of national laws is generally limited to a country's geographical territory, the nature of data flow can lead to situations where these national laws apply regardless of a company's physical location. Extraterritorial application is intended to protect personal data handled by companies outside of a country's borders.

As Table 5 indicates, currently, all AMS have provisions for extraterritorial application in their domestic laws. However, the specific conditions vary depending on the purpose for which the data is handled. For example, Malaysia's law applies only to companies providing goods or services from foreign countries to Malaysia. Indonesia and Thailand extend their laws to companies involved in monitoring the behaviour of data subjects.

Extraterritorial application may subject companies in the home country to the data protection laws of a foreign country, even if they lack a physical presence there. Similarly, foreign companies may also be subject to the home country's data protection laws if they process personal data of individuals residing in the home country. This occurs when companies process personal data obtained outside of their borders for purposes such as providing services, selling goods, or monitoring individuals. In such cases, companies need to comply with the rules of the country in which the data subjects reside and implement the necessary actions to ensure compliance. Without clear communication between regulatory authorities and the private sector, including foreign companies, the compliance costs associated with extraterritorial application may reduce a country's attractiveness as a market.

Table 5: Extraterritorial Application of Personal Data Protection Regulations across ASEAN

: In force : Under legislative process

Category		BRN	KHM	IDN	LAO	MYS	MMR	PHL	SGP	THA	VNM
Extraterritorial application	Foreign companies offering goods or services to data subjects in the jurisdiction		▲		▲						▲
	Foreign companies engaged in the monitoring of the behaviour of data subjects located in the jurisdiction				▲						
	Others	*1	▲*2*3		*1	*4	▲*5	*6	*1		
Requirement for foreign companies to establish representatives for controllers or processors in the jurisdiction											

BRN = Brunei Darussalam, IDN = Indonesia, KHM = Cambodia, LAO = Lao PDR, MMR = Myanmar, MYS = Malaysia, PHL = Philippines, SGP = Singapore, THA = Thailand, VNM = Viet Nam.
Notes:

1. A black triangle indicates that the regulations in question apply only to sectors covered by the individual laws and regulations shown in Table 1.
2. *1 applies to organisations that collect, use, or disclose personal data within the country, whether they are formed or recognised under the country's laws, or if they are residents or have an office or place of business in the country.
3. *2 applies to legal and natural persons or interests of Cambodia.
4. *3 applies to foreign companies registered with the National Bank of Cambodia as institutions handling credit information. They are obligated to accept requests for corrections or other amendments to consumers' credit information (i.e. personal data) due to the regulatory requirements under the regulations on credit information overseen by the National Bank of Cambodia.
5. *4 applies to a person who is not established in Malaysia but uses equipment in Malaysia for processing personal data, other than for the purposes of transit through Malaysia.
6. *5 applies to Myanmar citizens who are anywhere beyond the physical limits of Myanmar.
7. *6 applies to the act, practice, or processing relating to personal information about a Philippines citizen or a resident; a contract is entered into in the Philippines.

Source: Authors.

2.2.1.4. Data Controller's Obligations Associated with Data Security

Table 6 shows that some AMS, such as Cambodia, Indonesia, and Malaysia, require companies to register with regulators when processing personal data, ensuring that such data are handled securely. In Cambodia and Indonesia, this registration applies universally across industries, while in Malaysia, it is limited to specific industries designated by ministerial order. Singapore's regulator, meanwhile, recommends that companies conduct data protection impact

assessments[14] on personal data and perform risk assessments[15] to strengthen data security.

Regulations stipulate both technical measures (e.g. access control to information systems, countermeasures against unauthorised access, and system monitoring) and organisational measures (e.g. appointing a data protection officer [DPO] to oversee the company's internal systems to be implemented for security). While technical measures are widely required, organisational measures vary across AMS. Some AMS require the appointment of DPOs, while others do not. In countries that mandate the appointment of DPOs, companies must establish an organised data protection system. In jurisdictions lacking such requirements, the establishment of these systems is not guaranteed. Consequently, companies from countries with DPO requirements may consider transferring personal data to companies in countries without such obligations as a data protection risk.

Countries that do not explicitly mandate technical and organisational measures may risk losing business opportunities for domestic companies. Foreign companies may view the transferring of personal data to such jurisdictions as a compliance risk. In the context of ASEAN businesses expanding to other regions – such as an e-commerce provider targeting non-ASEAN customers – it is crucial to demonstrate their adherence to robust data protection standards. Measures such as conducting data protection impact assessments and appointing DPOs can reassure individuals and companies outside of ASEAN that data transfer risks within ASEAN are minimal. Accordingly, prioritising technical and organisational measures for data protection would establish high expectations of ASEAN companies for handling data securely, stimulating data flow within and outside of ASEAN and fostering the development of the digital economy.

Conversely, obligations to register data processing are often considered unnecessary and overly burdensome for businesses. While registration may help identify high-risk companies in advance, its significance diminishes if applied indiscriminately across all industries. Even in high-risk sectors, such as ICT and finance, mandatory registration offers limited benefits; instead, a risk-based approach to data protection is more effective. Companies could implement voluntary data protection impact assessments, with additional protections imposed through industry-specific laws and regulations as necessary. This approach reduces unnecessary

[14] A data protection impact assessment is a process designed to describe data-processing activities, assess their necessity and proportionality, and assist in managing risks regarding the rights and freedoms of natural persons. It involves risk assessment and identifying measures to mitigate the risks associated with the processing of personal data.

[15] Risk assessments include evaluations of the content and purpose of the data processing, necessity of the processing, and risk to the data subject's rights and freedoms.

administrative burdens while ensuring effective safeguards for high-risk data.

Table 6: Data Controller Obligations Associated with Data Security across ASEAN

: In force : Under legislative process

Category		BRN	KHM	IDN	LAO	MYS	MMR	PHL	SGP	THA	VNM
External	Notification for data subject		▲				▲				
	Registration of database/service		▲	*2							
	Data protection impact assessment								*4		
	Others		▲*1				▲*3				
Internal	Technical and organisational measures		▲				▲				
	Purpose Limitation		▲								
	Accuracy		▲				▲				
	Retention Limitation		▲				▲				
	Drawing up of codes of conduct		▲		▲						
	Record of processing activities										
	Designation of the data protection officer										

BRN = Brunei Darussalam, IDN = Indonesia, KHM = Cambodia, LAO = Lao People's Democratic Republic, MMR = Myanmar, MYS = Malaysia, PHL = Philippines, SGP = Singapore, THA = Thailand, VNM = Viet Nam.

Notes:

1. A black triangle indicates that the regulations in question apply only to sectors covered by the individual laws and regulations shown in Table 1.
2. *1 indicates that if an intermediary or an electronic commerce service provider becomes aware that information in an electronic record gives rise to civil or criminal liability, the intermediary or service provider must immediately take appropriate measures.
3. *2 notes that Indonesia's Personal Data Protection Law does not require organisations to register or to notify any governmental body regarding the processing of personal data. However, if an organisation (whether Indonesian or offshore) processes personal data through an electronic system (e.g. a website or app), it may be classified as an electronic system operator (ESO). Consequently, the organisation is required to obtain an ESO registration certificate. The ESO registration process is conducted through the online single submission system, an integrated electronic platform for managing licensing in Indonesia.
4. *3 notes that organisations must submit a cybersecurity report to the relevant ministries and organisations at least once per year.
5. *4 indicates that conducting a data protection impact assessment is not mandatory, but organisations are advised to perform them as a best practice.

Source: Authors.

2.2.1.5. Mandatory Personal Data Breach Notification

As Table 7 indicates, in the event of a data breach, all AMS require data controllers[16] to report the incident to regulatory authorities and/or to notify the affected data subjects.[17] However, the specific requirements – such as the deadline for notification, relevant authority, and content of the report – vary across AMS. Consequently, companies must ensure compliance with the specific regulations of the countries where they operate.

Table 7: Mandatory Personal Data Breach Notification across ASEAN

: In force : Under legislative process

Category	BRN	KHM	IDN	LAO	MYS	MMR	PHL	SGP	THA	VNM
Data breach notification to authorities		▲								
Data breach notification to affected individuals		▲				▲				

BRN = Brunei Darussalam, IDN = Indonesia, KHM = Cambodia, LAO = Lao People's Democratic Republic, MMR = Myanmar, MYS = Malaysia, PHL = Philippines, SGP = Singapore, THA = Thailand, VNM = Viet Nam.
Note: A black triangle indicates that the regulations in question apply only to sectors covered by the individual laws and regulations shown in Table 1.
Source: Authors.

2.2.1.6. Government Access to Personal and Non-personal Data Held by Private Entities

As indicated in Table 8, all AMS have legal provisions allowing public authorities to access information held by companies under certain conditions. However, unlike the EU and United States frameworks, AMS lack explicit safeguards to minimise infringements on data subjects' rights or to prevent industrial espionage. For example, under the Minister of Communications and Information's Regulation on Private Sector Electronic System Providers, the regulatory authority of Indonesia can request access to data from private electronic system operators (ESOs),[18] including foreign ESOs. The Ministry of Communications and Information is authorised to grant access to electronic systems and data related to Indonesian citizens or legal entities. This access extends to both personal and non-personal data.

There is a concern that governmental access to confidential business and technical data,

[16] The data controller is the entity that determines why the data are needed, how the data will be used, and how long they will be kept and processed (or instructs on how to process the data) according to these purposes and means. The data controller is responsible for and legally accountable for the user's data.

[17] In response to a major personal data breach in 2017, the July 2024 amendment to the law also stipulates Malaysia's obligation to report data breaches to the Personal Data Protection Department in the event of a data breach.

[18] An ESO is a manager or technician who controls and operates electronic systems to ensure that they are operating properly.

unrelated to national security, could be perceived as a threat akin to industrial espionage. This perception may deter businesses and reduce the competitiveness of countries that lack restrictions on governmental access.

Table 8: Government Access to Personal and Non-personal Data Held by Private Entities across ASEAN

: In force : Under legislative process

Category		BRN	KHM	IDN	LAO	MYS	MMR	PHL	SGP	THA	VNM
Comprehensive (computer systems, cybersecurity, etc.)				#							
Sector Specific	Telecom										
	Finance (Banking, Credit information, etc)										
	Public										

BRN = Brunei Darussalam, IDN = Indonesia, KHM = Cambodia, LAO = Lao People's Democratic Republic, MMR = Myanmar, MYS = Malaysia, PHL = Philippines, SGP = Singapore, THA = Thailand, VNM = Viet Nam.
Note: # applies to electric system operators.
Source: Authors.

2.2.2. Cross-border Data Flow Regulations

As shown below, in AMS, cross-border personal data transfer regulations are in place to protect domestic personal data in a business environment where data are transferred across borders. These regulations generally prohibit the transfer of personal data from their home country to other countries that have not been granted adequacy status, meaning that their data protection regulations are not recognised as equivalent to those of the home country. To transfer personal data to countries without adequacy status, it is necessary to operate a certification system for companies or to use cross-border transfer mechanisms approved by the home country such as model contractual clauses (MCCs).[19] The costs associated with these measures are considered a challenge for ASEAN in promoting the digital economy.

Some AMS have also introduced restrictions on cross-border data transfers and localisation regulations that impact non-personal data transfers. For example, Cambodia's Prakas on Credit Reporting (dated 26 June 2020) regulates the cross-border transfer of consumer credit and overdue information. These regulations were implemented to mitigate the

[19] MCCs are standardised contractual terms and conditions that businesses can voluntarily adopt for cross-border transfer of personal data.

risk of data breaches, particularly concerning the cross-border transfer of data by financial institutions and the exchange of data between companies in different countries. Similarly, the Law on Information and Communication Technology in the Lao PDR prohibits the cross-border transfer of non-personal data held by governmental agencies for security reasons, with no exceptions. No such regulations exist in Brunei Darussalam, Malaysia, Myanmar, the Philippines, or Singapore.

This section elaborates on the regulatory status of AMS regarding two key topics concerning cross-border data transfers: (i) measures for interoperability across jurisdictions and (ii) data localisation.

2.2.2.1. Measures for Interoperability across Jurisdictions

Table 9 illustrates that all AMS have established regulations for cross-border personal data transfers to safeguard domestic personal data in a business environment involving cross-border data flow. One approach to achieving interoperability across jurisdictions involves establishing exceptions to the prohibition on cross-border transfer of personal data, allowing data transfer under specific conditions. As mentioned above, granting adequacy status to foreign countries is one mechanism for providing these exceptions. While some countries permit data transfer through adequacy status, the lack of harmonised and detailed provisions in data flow regulations has led to the addition of varied and fragmented requirements by individual countries.

For example, in Malaysia, in addition to an adequacy decision from the Personal Data Protection Committee, approval from the Malaysian Communications and Multimedia Commission is also required. Consequently, companies must comply with these specific provisions, making the operational hurdles for cross-border data transfer based on adequacy certification both high and costly.

In Viet Nam, in addition to adequacy status, exceptions to the cross-border transfer of personal data require that all of the following conditions be met: (i) obtaining the consent of the data subject, (ii) ensuring domestic storage of the original data in Viet Nam (i.e. data localisation), and (iii) securing written consent from the Personal Data Protection Commission. As a result, even companies in countries granted adequacy status by Viet Nam face high compliance costs for cross-border personal data transfer.

Another measure to enhance interoperability is the development of mechanisms involving the private sector. ASEAN has made progress in developing such mechanisms to facilitate cross-border personal data flow amongst AMS. In January 2021, ASEAN endorsed

the ASEAN MCCs, which align with the ASEAN *Framework on Personal Data Protection*, a non-binding guideline established in 2016. Additionally, Singapore, in collaboration with ASEAN and the European Commission Directorate-General for Justice and Consumers, has published a joint guide to the ASEAN MCCs (ASEAN, 2021) and the European Union Standard Contract Clauses (ASEAN and European Commission, 2024). While not all AMS are participants, the Philippines and Singapore have joined the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System, which allows certified companies to ensure that personal data are protected according to established privacy standards across participating jurisdictions (APEC, 2023).

Despite these advancements, the need for harmonisation of the detailed provisions in domestic data flow regulations remains. This includes standardising definitions of terms, like 'data subject', and breach notification obligations. Additionally, it is essential to provide clear operational guidance to clarify the relationship of regulations between countries.

In contrast, the cross-border transfer of non-personal data is not generally regulated through prohibitions or exceptions in AMS. Instead, cross-border transfers of non-personal data are regulated only for specific purposes, such as cybersecurity; regulatory enforcement, including the right of access to data; and national security.

Table 9: Measures for Interoperability across Jurisdictions for Personal Data Cross-border Transfers amongst ASEAN Member States

: In force : Under legislative process

Category		BRN	KHM	IDN	LAO	MYS	MMR	PHL	SGP	THA	VNM
Cross-border data transfer restriction											
Exceptions	Adequacy decision										A
	Contractual relationship (SCC/MCC/BCR, etc)										
	Certification (CBPR etc)										
	Approval from authority		A								A
	Consent of data subject		A								A
	Performance of contractual obligation										
	Legality of domestic regulations						A				
	Others						A				A

BCR = binding corporate rule, BRN = Brunei Darussalam, CBPR = cross-border privacy rule, IDN = Indonesia, KHM = Cambodia, LAO = Lao People's Democratic Republic, MCC = model contractual clause, MMR = Myanmar, MYS = Malaysia, PHL = Philippines, SCC = standard contractual clause, SGP = Singapore, THA = Thailand, VNM = Viet Nam.
Note: All requirements must be met for a company to qualify for exceptions to cross-border data transfer restrictions.
Source: Authors.

2.2.2.2. Data Localisation

An increasing number of countries are implementing data localisation requirements. As shown in Table 10, four AMS have some form of data localisation regulations. These regulations mandate that data – whether personal or non-personal – be processed or stored within the country of origin. The primary purposes of these requirements are to protect and to promote domestic industries, ensure national security, and facilitate regulatory enforcement.

For personal data, data localisation provisions generally prevent companies from transferring personal data abroad, even if they have implemented measures to protect them. For non-personal data, certain laws mandate the domestic storage of data related to national strategies in certain industrial sectors, such as finance, ICT, national administration, and defence. For example, in Viet Nam, Decree No. 53/2022/ND-CP, which outlines implementing regulations of the Cyber Security Law, stipulates that from October 2022, both domestic and foreign businesses – including e-commerce platforms – providing online services in Viet Nam must store both personal and non-personal data within the country. This includes data related to service user relationships and data generated by service users. The Lao PDR has also introduced data localisation for both personal and non-personal data.

Even when addressing the same objective, regulations on non-personal data differ considerably amongst AMS. While one AMS imposes data localisation requirements, another may allow the free flow of such data. For instance, in the context of cybersecurity, some AMS consider self-regulation by companies or civil compensation in the event of an incident to be a sufficient incentive for compliance, while other AMS may consider state regulations necessary and have introduced data localisation requirements accordingly.

Companies face significant costs related to constructing data centres for storing personal data, renting servers, and managing data. As barriers to the free flow of data, these requirements pose a significant challenge to companies engaged in digital economic activities.

Table 10: Data Localisation Requirements for Personal and Non-Personal Data across ASEAN

: In force

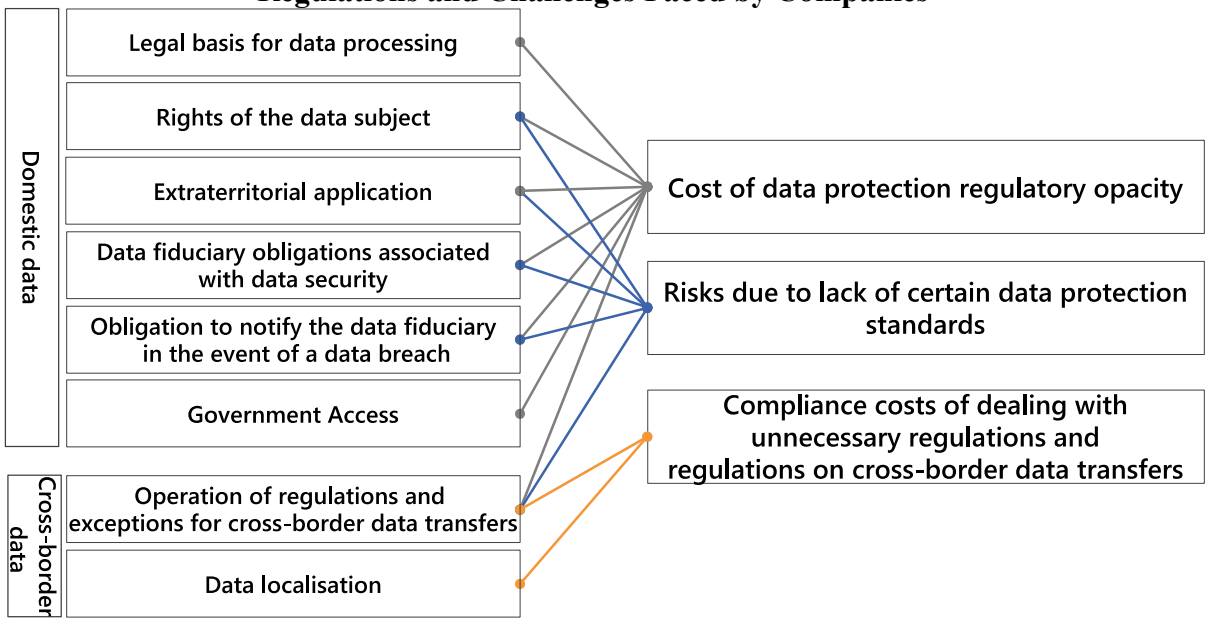
Category			BRN	KHM	IDN	LAO	MYS	MMR	PHL	SGP	THA	VNM
Data localisation	Public data											
	Private data	Telecom										
		Wholesale and Retail										
		Finance (Credit information)										
		Healthcare										
		Public										

BRN = Brunei Darussalam, CBPR = cross-border privacy rule, IDN = Indonesia, KHM = Cambodia, LAO = Lao People's Democratic Republic, MCC = model contractual clause, MMR = Myanmar, MYS = Malaysia, PHL = Philippines, SCC = standard contractual clause, SGP = Singapore, THA = Thailand, VNM = Viet Nam.
Source: Authors.

3. ASEAN's Data Governance Challenges

Based on the above discussion, the current data-related regulations of AMS present three key challenges: (i) the cost of regulatory opacity in data protection, (ii) risks arising from the lack of standardised data protection measures, and (iii) compliance costs associated with unnecessary regulations and cross-border data transfer restrictions. Figure 1 below illustrates the relationship between the discussion points on domestic and cross-border data protection regulations and the three identified challenges.

Figure 1: Relationship between Domestic and Cross-border Data Protection Regulations and Challenges Faced by Companies



Source: Author.

12.1. Challenge 1: Cost of Regulatory Opacity in Data Protection

The lack of uniformity in data protection regulations amongst AMS creates significant challenges for businesses. Companies engaging in cross-border data transfers must assess their compliance with the regulations of multiple countries. The absence of a comprehensive and accessible service that outlines these regulatory differences leaves businesses without clear guidance. From a practical perspective, this lack of transparency in AMS regulations forces companies to either build internal systems or to rely on external professional services to stay updated on regulatory changes and new requirements, imposing considerable burdens on businesses.

12.2. Challenge 2: Risks Due to Lack of a Certain Level of Data Protection Standards

Establishing clear and reasonable data protection standards – and excluding unreasonable and excessive ones – helps institutionalise appropriate data management practices and reduces data protection risks within a country. The absence of such standards heightens risks for companies engaging in entrepreneurial activities. For instance, if a company handles data received from a foreign country with lower standards or transfers data to a country with higher standards, the data protection risks would remain manageable under an established regulatory regime. However, transferring data to countries with lower protection standards increases the risks of data breaches or improper handling, including risks to customers' personal data.

Moreover, companies may hesitate to enter countries where unlimited governmental access to data is permitted. Such environments expose businesses to risks such as industrial espionage, threatening the confidentiality of critical business and technical data. These challenges deter companies from expanding into potentially lucrative but uncertain markets, resulting in missed opportunities.

12.3. Challenge 3: Compliance Costs of Unnecessary Regulations and Cross-border Data Transfer Regulations

Prohibitions on cross-border transfers of personal data and data localisation requirements increase the costs of intra-company data transfers across borders. These measures directly impede the global operations of companies. While each country has regulatory sovereignty, some countries have adopted data localisation measures to enforce cybersecurity or tax collection measures, creating excessive constraints for businesses.

Even with the introduction of adequate status systems designed to facilitate cross-border data transfer, challenges persist. For example, some countries impose additional conditions on cross-border data transfer beyond adequacy standards, increasing compliance complexity and costs. These differences in national data protection laws exacerbate the burden on businesses operating across multiple jurisdictions.

12.4. Key Directions to Address Challenges

12.4.1. Direction 1: Improve the Transparency of National Data Regulations

Currently, no systematic service organises information on data protection regulations across the ASEAN region. As a result, company representatives must individually navigate websites of various ministries and agencies, often encountering language barriers. To address this issue and to reduce the costs associated with researching regulatory updates, a centralised and publicly accessible data regulation repository should be developed. This repository would provide comprehensive information on each country's data protection regulations, allowing users to compare these regulations across AMS. The repository would also help users identify key data protection issues that need to be addressed.

Such a repository would reduce the costs associated with researching regulatory updates, supporting businesses in streamlining operations in the ASEAN region and contributing to the expansion of the ASEAN digital economy. Furthermore, given the rapid evolution of data-related technologies, frequent regulatory changes are inevitable. An up-to-date and comprehensive data regulation repository is essential for enabling companies to stay informed

and to adapt swiftly to technological innovation.

12.4.2. Direction 2: Establish Minimum Standards for Data Protection Regulations

Minimum standards refer to common baseline requirements that must be met when establishing regulations in each country. Rather than relying on a comparison of existing data protection regulations, established privacy guidelines should be used, such as those developed by OECD, as a reference for defining these standards across AMS. This approach ensures that data protection standards in any given country do not fall significantly below those of others.

Minimum standards can be achieved through a combination of comprehensive, sector-wide regulations and flexible, sector-specific regulations tailored to address national priorities and technological innovation. Sectors such as finance, ICT, and health care – and particularly those involving national security concerns – require tailored approaches. Ensuring such standards will support the expansion of the ASEAN digital economy and foster the free flow of data.

Additionally, to address concerns about governmental access, regulations should include safeguards to limit disclosure to essential purposes, such as search warrants or legitimate public need. High standards of data protection, even within data localisation provisions, can help prevent excessive or unnecessary restrictions while maintaining trust.

12.4.3. Direction 3: Reduce Unnecessary Regulations and Ensure Regulatory Interoperability for Cross-border Data Flow

To address the compliance costs associated with cross-border data transfer regulations, two strategies can be pursued: (i) reduce unnecessary regulations, and (ii) enhance the interoperability of legitimate regulations.

First, ensuring transparency, as outlined in Direction 1, can be instrumental in removing unnecessary regulations. By enhancing transparency, the current state of cross-border data transfer restrictions and data localisation requirements in each country will become clearer. This will reveal situations where one country mandates data localisation for a specific purpose while another does not. For instance, some countries may require critical data, such as financial data, to be stored domestically for cybersecurity purposes, or tax-related data to be kept within the country for tax collection purposes. In contrast, other countries may adopt less burdensome approaches for businesses, such as requiring companies to obtain international certifications for cybersecurity (e.g. an international security management system) or establishing systems that allow timely data submission even if the data

are stored overseas (e.g. granting local offices access to cloud data). Encouraging dialogue amongst AMS should be encouraged to assess whether cross-border transfer restrictions and data localisation are genuinely necessary for achieving their intended objectives. Such dialogue should aim to identify and to rectify unnecessary regulations, fostering mutual efforts to streamline the regulatory environment.

Next, to ensure interoperability, it is necessary to promote mutual compatibility by coordinating the detailed provisions of national laws and regulations, such as unifying the definitions of terms and the rights of data subjects. At the same time, the introduction of interoperability mechanisms, including MCCs and adequacy certifications, should be actively pursued. As previously mentioned, ASEAN introduced its MCCs in 2021, enabling companies to reduce the number of contracts that they need to sign and easing the burden of complying with complex legal frameworks for cross-border data transfer. To further enhance the effectiveness of interoperability mechanisms, several implementation strategies can be considered. These include incorporating specific data transfer tools, such as the aforementioned MCCs, into national legislation or mandating reliance on these tools through trade agreements.

4. Implications for the Digital Economic Framework Agreement

Negotiations are underway to conclude the DEFA by 2025, with the goal of realising a single ASEAN digital market. This section examines the essential elements that the DEFA should stipulate to address current data regulatory issues in AMS in line with the three directions identified in Section 3: (i) increasing the transparency of national data regulations, (ii) ensuring a minimum level of data protection regulations, and (iii) reducing unnecessary regulations while ensuring regulatory interoperability in cross-border data flow. Specifically, provisions are proposed that should be included as well as actions that ASEAN or AMS should take to implement these provisions, drawing on existing studies and digital trade rules. It should be noted that while the DEFA covers a broad range of topics, the recommendations focus on cross-border data flow and data protection.

4.1. Recommendation 1: Establish and maintain a comprehensive data regulation repository for ASEAN with a mechanism for continuous updates.

As noted in Section 3, there is currently no service that systematically organises data protection regulations amongst AMS. This lack of organisation imposes significant costs on companies to check the data regulations of each AMS. A comprehensive data regulation repository should be created that can be used by a variety of companies. The Economic

Research Institute for ASEAN and East Asia (ERIA) is already working on creating a data regulation repository for AMS in line with the specifications outlined in the Appendix, and leveraging this repository could be a viable option.

In addition to the data regulation repository, a mechanism should be incorporated into the DEFA to ensure that the regulations are regularly updated. Given the rapid evolution of technology, society, and the economy, data regulations will need to be revised continuously even after the DEFA is concluded. Using the proposed data regulation repository, stakeholders can monitor the state of regulatory development in each country in a timely manner and compare regulatory frameworks to facilitate harmonisation and interoperability.

4.2. Recommendation 2: Specify minimum standards for the protection of personal data in the DEFA

Second, the DEFA should establish specific rules on minimum standards for the protection of personal data. The *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (CPTPP), which includes 11 countries such as Brunei Darussalam, Malaysia, Singapore, and Viet Nam, mandates that national laws comply with the OECD Privacy Guidelines[20] to protect personal data. Similarly, *Digital Economic Partnership Agreement* (DEPA) provisions are largely aligned with the OECD Privacy Guidelines (Government of Chile et al., 2020). ASEAN has already adopted the ASEAN *Framework on Personal Data Protection* (AFPDP), which also adheres to the OECD Privacy Guidelines (ASEAN, 2016). It is conceivable that the provisions of the AFPDP could be incorporated into the domestic laws of AMS. DEFA provisions could also build on the language of the DEPA by explicitly listing the key elements that must be ensured.

Regarding issues beyond the AFPDP, such as the obligation to appoint a DPO, or the right to data portability as a data subject, there is no consensus amongst AMS. While these topics could be included in future discussions, reaching agreement on them at this stage would be challenging. Although such elements are part of the GDPR and similar legislation, they lack global consensus. Introducing them into DEFA negotiations at this point may yield limited benefits. For now, efforts should focus on reducing compliance costs by enhancing regulatory transparency.

Additionally, the DEFA should address the issue of governmental access to personal data. The OECD *Declaration on Government Access to Personal Data Held by Private Sector*

[20] OECD, Privacy and Data Protection, https://www.oecd.org/en/topics/policy-issues/privacy-and-data-protection.html

Entities highlights the importance of adhering to the higher-order principles to ensure a minimum level of personal data protection (OECD, 2022). Indeed, the *EU-Japan Economic Partnership Agreement*'s e-commerce chapter, amended in 2023, acknowledges the role of these principles in fostering trust in the digital economy.[21] Incorporating similar provisions into the DEFA could promote disciplined practices for governmental access. While extending these measures to non-personal data could be considered in the future, this action should remain a longer-term objective. Since OECD's higher-order principles currently address only personal data, prioritising personal data protection within DEFA provisions is the most practical step.

4.3. Recommendation 3: Pursue digital economy rules aiming for the CPTPP level and ensure substantive interoperability amongst national systems

The DEFA should focus on two objectives: (i) revising measures that are overly restrictive to ensure alignment with reasonable objectives, and (ii) ensuring interoperability amongst national regulatory systems.

Regarding the first objective, DEFA negotiations should aim to achieve standards comparable to those of the CPTPP, particularly concerning data localisation and restrictions on cross-border data transfers. Rules on digital trade already exist in the CPTPP, which includes four AMS, and in the *Regional Comprehensive Economic Partnership* (RCEP) agreement, which includes 10 AMS.

The CPTPP and RCEP have differing levels of regulatory ambition. While the RCEP adopts a more flexible approach due to self-judging exception clauses,[22] the CPTPP provides

---

[21] Article 8.82: Protection of Personal Data (emphasis added)

3. Each Party shall adopt or maintain a legal framework that provides for the protection of personal data related to electronic commerce. In the development of its legal framework for the protection of personal data and privacy, each Party should take into account the principles and guidelines of relevant international bodies. *The Parties also recognise that high standards of privacy and data protection as regards government access to privately held data, such as those outlined in the OECD Principles for Government Access to Personal Data held by Private Sector Entities, contribute to trust in the digital economy* (EC and Government of Japan, 2019).

[22] Article 12.14: Location of Computing Facilities (emphasis added)

1. The Parties recognise that each Party may have its own measures regarding the use or location of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.
2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that Party's territory.
3. Nothing in this Article shall prevent a Party from adopting or maintaining

(a) any measure inconsistent with paragraph 2 *that it considers necessary to* achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or

(b) any measure that it considers necessary for the protection of its essential security interests. *Such measures shall not be disputed by other Parties* (Government of Australia et al., 2022).

more objective description in its exceptions.[23] The RCEP-type clauses grant AMS significant discretion, potentially undermining the enforcement of minimum protections, such as those related to data localisation and other disciplines, as noted in Section 3. To create a single digital market in ASEAN, the DEFA should thus aim for higher-level rules and strive to meet the standards set by the CPTPP.[24]

The CPTPP rules on digital trade include exceptions that permit measures necessary for legitimate public policy objectives. While these exceptions provide AMS with regulatory discretion, this discretion is bounded; that is, measures cannot result in arbitrary or unjustifiable discrimination or impose restrictions that are more burdensome than necessary to achieve the legitimate public policy objectives.[25] These conditions make the CPTPP an effective foundation for future discussions amongst AMS and can help clarify legitimate policy objectives and identify acceptable measures to achieve them.

To advance these discussions, it would be effective to visualise the measures each AMS has introduced for similar policy objectives using the repository proposed in Direction 1. This allows identification of commonalities and facilitates dialogue on aligning regulatory approaches. For example, Section 2 highlighted differing regulatory measures amongst AMS, such as obligations to notify authorities when personal data are transferred across borders or requirements for data localisation in specific sectors like finance. These differences indicate divergent views that must be reconciled to support the formation of a digital single market in ASEAN. Discussions should assess whether these measures are necessary and appropriate for achieving integration.

For the second objective, ensuring interoperability, the initial step is to identify and to map the common denominators across AMS with the aim of unifying the definition of terms,

---

[23] Article 14.13: Location of Computing Facilities

1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.
2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.
3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective (Government of Australia et al., 2018).

[24] Note that all of the DEPA's original members are CPTPP members, and DEPA's obligations related to cross-border flow confirm those of the CPTPP.

[25] For example, refer CPTPP Article 14.13, Section 3 (footnote 18).

rights of data subjects, and similar foundational elements. Subsequently, the DEFA should work towards recognising and establishing specific tools that facilitate cross-border data transfers within each country's regulatory framework. One such tool is the ASEAN MCCs, which have been introduced in Singapore and Thailand. However, many AMS have yet to officially recognise them as a basis for cross-border data transfers under their national laws. To ensure interoperability, it is important to explicitly incorporate the MCCs into domestic legislation or guidelines. Additionally, harmonising the content of MCCs across countries is desirable. Where differences exist, they should be clearly documented and made accessible. This approach would enable companies to compare the MCCs of countries where they already comply with those of new markets that they wish to enter. This clarity would allow businesses to understand any additional measures required, thereby reducing regulatory complexity and facilitating smoother cross-border operations.

References

Asia Pacific Economic Cooperation (2023), *APEC Cross-Border Privacy Rules System Program Requirements,* https://www.apec.org/docs/default-source/Groups/ECSG/CBPR/CBPR-ProgramRequirements.pdf

Association of Southeast Asian Nations (ASEAN) (2016), *Framework on Personal Data Protection,* Bandar Seri Begawan, 25 November.

——— (2021), *ASEAN Model Contract Clauses for Cross Border Data Flows*, https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

ASEAN and European Commission (2024), *Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractural Clauses*, https://asean.org/book/joint-guide-to-asean-model-contractual-clauses-and-eu-standard-contractual-clauses/

EU–ASEAN Business Council (2020), *Data Governance in ASEAN: From Retoric to Reality*, https://www.eu-asean.eu/wp-content/uploads/2022/02/DATA-GOVERNANCE-IN-ASEAN-FROM-RHETORIC-TO-REALITY-2020.pdf

European Commission (EC) and Government of Japan (2019), *EU-Japan Economic Partnership Agreement,* https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/japan/eu-japan-agreement_en

Fritz, J. and T. Giardini (2023), *Data Governance Regulation in the G20: A Systematic Comparison of Rules and Their Effect on Digital Fragmentation*, Digital Policy Alert, https://digitalpolicyalert.org/report/fragmentation-risk-in-g20-data-governance-regulation

Government of Australia et al. (2018), *Comprehensive and Progressive Agreement for Trans-Pacific Partnership,* https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/cptpp

Government of Australia et al. (2022), *Regional Comprehensive Economic Partnership Agreement,* https://www.dfat.gov.au/trade/agreements/in-force/rcep

Government of Chile, Government of New Zealand, Government of Singapore, and Government of South Korea (2020), *Digital Economy Partnership Agreement,* https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa

Liu, J., U. Sengstschmid, and Y. Ge (2023), 'Facilitating Data Flows across ASEAN: Challenges and Policy Directions', *Asia Competitiveness Institute Research Paper Series,* No. 19-2023, Singapore: Lee Kuan Yew School of Public Policy

Oikawa, K. (2024), 'Future of Data Governance in Asia and Operationalisation of "Data Free Flow with Trust"', *Economic Research Institute for ASEAN and East Asia (ERIA) Policy Briefs,* No. 2024-01, Jakarta: ERIA.

Organisation for Economic Co-operation and Development (OECD), Privacy and Data Protection, https://www.oecd.org/en/topics/policy-issues/privacy-and-data-protection.html

——— (2022), *Declaration on Government Access to Personal Data Held by Private Sector Entities,* Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

United Nations Conference on Trade and Development (UNCTAD) (2023), *G20 Members' Regulations of Cross-border Data Flows,* Geneva, https://unctad.org/publication/g20-members-regulations-cross-border-data-flows

World Trade Organization (WTO) Secretariat (2024), *Transparency Concerns Remain at Centre During Discussions at SCM Committee Meeting*, https://www.wto.org/english/news_e/news24_e/scm_23apr24_e.htm

Appendix: ASEAN Data Governance Hub

As discussed in this paper, access to information on data-related regulations is crucial for businesses to operate effectively. Visualising the current state of data governance in each country is also essential for fostering informed policy discussions and facilitating cross-border collaboration. Existing initiatives, such as those by Digital Policy Alert, suggest that creating a comprehensive repository of data-related regulations for each country can significantly improve transparency. Similarly, establishing a repository of data-related regulations in ASEAN would serve as a powerful tool for improving transparency across the region. The findings from this paper provide a foundational step towards realising such a repository in the future.

To explore the practicalities of creating and maintaining such a repository, several operational models were analysed. The key to success lies in ensuring that the repository's information is both accurate and up to date. Three potential approaches were considered:

(i) **Operator-driven research.** The repository operator conducts all necessary research.

(ii) **ASEAN Member State (AMS) contribution.** Each country provides the information, and the operator aggregates it.

(iii) **External third-party research.** Independent entities, such as law firms within each AMS, conduct the research.

Each approach has distinct advantages and challenges. Option (ii) seems most promising as it leverages the direct involvement of AMS, ensuring accuracy and timeliness. However, the capacity and willingness of AMS to consistently update the repository can vary, making voluntary cooperation a critical factor. For instance, a similar reliance on voluntary reporting has posed challenges under the subsidy rules of the World Trade Organization (WTO), which also rely on a similar voluntary reporting system (WTO Secretariat, 2024). In contrast, Options (i) and (iii) are less dependent on AMS engagement, which can help mitigate risks associated with inconsistent report risks associated with inconsistent reporting. However, these approaches may struggle to achieve the sufficient level of accuracy. Digital Policy Alert's method, which combines automated notifications (e.g. through web crawling) with rigorous internal verification processes, offers a valuable model in this regard.

A combined approach may provide the best solution. For example, information could initially be gathered through Option (i) or (iii) using Digital Policy Alert-like mechanisms, with AMS verifying and updating the data as in Option (ii). This would reduce the burden on AMS,

as they would not need to provide information entirely from scratch.

In addition, the repository's user interface and user experience of databases are critical. The database should be user-friendly, especially for micro, small, and medium-sized enterprises and governmental officials in AMS, with regulations presented in clear, understandable language. Functional features, such as comparative tools, are also essential. For example, users who are planning to expand their businesses into other countries should be able to compare the target country's regulations with those of their home country.

Based on the points above, the Economic Research Institute for ASEAN and East Asia (ERIA) created a mock-up of the ASEAN Data Governance Hub, which would serve as the foundation for a data-related regulatory repository for ASEAN. A video or PPT developed by Digital Policy Alert is included in the main part of the report. It is recommended that this mock-up be used as a reference to establish a framework for future operations.

ERIA Discussion Paper Series

No.	Author(s)	Title	Year
2024-31 (No. 538)	Tadashi Ito	Trump Tariffs and Roundabout Trade	November 2024
2024-30 (No. 537)	Prabir De, Komal Biswal, and Venkatachalam Anbumozhi	Securing Regional Solar Supply Chains: Determinants and Preparedness of the Northeastern Region of India and ASEAN	November 2024
2024-29 (No. 536)	Phouphet Kyophilavong, Shandre Thangavelu, Inpaeng Sayvaya, and Phongsili Soukchalern	Determinant Factors of Tourist Expenditure in the Lao People's Democratic Republic	November 2024
2024-28 (No. 535)	Cassey Lee	Urban Amenities and Trade Resilience During the Covid-19 Pandemic in Malaysia	November 2024
2024-27 (No. 534)	Sebastiao Oliveira, Jay Rafi, and Pedro Simon	The Effect of United States Monetary Policy on Foreign Firms: Does Debt Maturity Matter?	September 2024
2024-26 (No. 533)	Kazunobu Hayakawa and Sasatra Sudsawasd	Impacts of Trade Diversion from China in the United States Market on Wages in a Third Country: Evidence from Thailand	September 2024
2024-25 (No. 532)	Jung Hur and Chin Hee Hahn	Examining the Impact of the 2011 Japanese Earthquake on Japanese Production Networks in the Republic of Korea: A Firm-level Data Analysis	September 2024
2024-24 (No. 531)	Nobuaki Yamashita and Doan Thi Thanh Ha	The Third-country Effect of the United States-China Trade War on Viet Nam	September 2024
2024-23 (No. 530)	Ketan Reddy, Subash Sasidharan, and Shandre Mugan Thangavelu	Does Economic Policy Uncertainty Impact Firm GVC Participation? Microdata Evidence from India	September 2024
2024-22 (No. 529)	Kuriko Otsuka and Keita Oikawa	Economics of Happiness and ASEAN's People-Centric Smart City	July 2024

ERIA discussion papers from previous years can be found at:

http://www.eria.org/publications/category/discussion-papers