

Policy Brief

Shaping Source Code Provision in DEFA: Balancing Innovation Protection and Regulatory Access

by Mahirah Mahusin and Hilmy Prilliadi

Key Messages:

- DEFA should prohibit mandatory source code disclosure as a condition for market access, while clearly preserving regulatory and judicial access for oversight, enforcement, and public interest purposes.
- Any extension of protection to algorithms must not constrain governments' ability to ensure transparency, accountability, and fairness, particularly in high-risk or public-facing digital applications.
- DEFA should explicitly clarify the scope of exclusions, confirming that open-source licensing, voluntary disclosure, commercial contracting, and public procurement fall outside the prohibition on forced disclosure.
- Effective implementation will require strengthened regulatory and enforcement capacity across ASEAN, particularly in data protection, consumer protection, and algorithmic accountability.

Source code underpins digital technologies and is typically protected as commercially sensitive intellectual property. While free trade agreements (FTAs) increasingly prohibit mandatory source code disclosure as a condition for market access, governments continue to require access in specific circumstances, including regulatory oversight of algorithmic systems, conformity assessments, law enforcement, and public procurement.

Across ASEAN, member states have adopted diverse approaches. These include Indonesia's public procurement requirements, Malaysia's provisions allowing access in criminal investigations, and Thailand's safeguards under trade secret law. Recent FTAs reflect a shift from broad, categorical prohibitions towards more nuanced frameworks that permit regulatory exceptions, raise questions regarding the treatment of algorithms, and preserve space for voluntary disclosure.

As ASEAN advances negotiations on the Digital Economy Framework Agreement (DEFA), source code provisions will need to strike a careful balance between protecting innovation and maintaining regulatory and judicial flexibility. This Policy Brief recommends affirming baseline prohibitions on forced disclosure, clearly safeguarding legitimate government access, clarifying the treatment of algorithms, protecting voluntary disclosure, and addressing implications for public procurement.

I. Introduction

Source code refers to the human-readable instructions written by programmers to direct a computer's operations. Typically written in programming languages such as Python, Java, or C++, source code underpins a wide range of digital systems, including messaging applications, hospital information platforms, and e-commerce services. It can range from relatively simple scripts to highly complex systems, such as Google's search engine algorithms.

Because source code often embeds proprietary algorithms that confer a competitive advantage, unauthorised disclosure can enable intellectual property (IP) misappropriation. As a result, source code is generally treated as commercially sensitive information and protected under IP law through a combination of trade secrets, copyright, and patents. Trade secret law safeguards confidential code from disclosure; copyright law protects the expression of a programmer's ideas; and patents may apply to genuinely novel software-related inventions. Each of these mechanisms, however, has limitations. Copyright does not protect the underlying ideas or functional logic of software, patents are time-limited, and certain forms of machine learning may be considered too abstract to be patentable (European Patent Office, n.d.). Consequently, software developers often rely primarily on trade secret protection.

Mahirah Mahusin

Manager for Digital Innovation and
Sustainable Economy, ERIA

Hilmy Prilliadi

Research Associate, ERIA

At the multilateral level, the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) provides baseline IP protection relevant to source code. In parallel, many free trade agreements (FTAs) have introduced provisions prohibiting governments from requiring source code disclosure as a condition for market access (Isono and Prilliadi, 2023). These provisions can be understood as a TRIMS-plus element, designed to shield foreign firms from technology transfer requirements, particularly where domestic suppliers are not subject to equivalent obligations.

While such prohibitions strengthen innovation protection, they have also raised concerns that excessive source code secrecy may constrain governments' ability to regulate digital systems in the public interest. These concerns have become more acute with the growing use of algorithmic decision-making across sectors, including finance, healthcare, and public services. This evolution calls for renewed attention to how source code provisions are framed in existing and future FTAs and digital economy agreements. The resulting policy challenge lies in striking an appropriate balance between safeguarding regulatory interests and maintaining incentives for innovation and cross-border digital trade.

II. Why do Governments Need Access to Source Code?

Governments may require access to source code for several legitimate public policy purposes, most notably regulatory and judicial oversight, as well as public procurement.

First, from a regulatory and judicial perspective, access to source code can be essential for verifying legal and regulatory compliance. Technical examination of code may be necessary to detect anti-competitive conduct, bias or discrimination embedded in automated decision-making systems, unlawful data processing or sharing, and product safety or reliability issues (Mitchell et al., 2023). As digital systems increasingly influence economic transactions and public services, effective oversight often depends on the ability to scrutinise how software operates in practice.

Such access typically arises in two distinct regulatory contexts: *ex ante* and *ex post* (Katyal, 2019). *Ex ante* access refers to situations in which regulators need to review source code before a product or system is placed on the market. This commonly occurs in conformity assessments or approval procedures for high-risk applications, such as medical devices or safety-critical software, where authorities must verify compliance with technical, safety, or sector-specific standards prior to deployment. *Ex post* access, by contrast, is required after a system has been deployed, including during investigations, enforcement actions,

audits, or judicial proceedings. In these cases, source code examination may be necessary to determine whether a system has caused harm, malfunctioned, or violated applicable laws.

Second, in the context of public procurement, access to source code can help governments mitigate the risks of vendor lock-in and ensure long-term interoperability and sustainability of digital systems. Compared with proprietary software, open-source licensing models allow public agencies to reuse, modify, and maintain software independently, while enabling third-party audits and improvements. This can promote transparency, explainability, and trust, particularly in the procurement of artificial intelligence and algorithmic systems (WTO, 2024).

III. Source Code Disclosure Policies in ASEAN

Several ASEAN Member States (AMS) already maintain legal frameworks that permit or require access to source code for specific public policy purposes, particularly for *ex post* regulatory enforcement and public procurement. A critical distinction in these frameworks is between *access* and *disclosure*. Access typically allows competent authorities to examine or review source code under controlled conditions – such as within secure government systems, through on-site inspections, or via escrow arrangements – without transferring ownership or making the code publicly available. Disclosure, by contrast, implies wider sharing or public release of source code, which may expose proprietary information and compromise trade secrets or other intellectual property rights.

Importantly, these access mechanisms are not designed as trade barriers. Rather, they support national authorities in ensuring compliance with laws and regulations related to safety, security, competition, and public interest objectives. In general, such requirements apply in a non-discriminatory manner to both domestic and foreign providers, though their existence is relevant when considering the scope and exceptions of source code provisions in trade and digital economy agreements.

In Indonesia, Government Regulation No. 71/2019 requires providers of customised software for public sector systems to provide source code or place it in escrow in the context of public procurement. This requirement enables government oversight, system continuity, and maintenance, particularly where software is developed specifically for public use. In Malaysia, access to encrypted data – including, where necessary, source code – may be compelled to support criminal investigations under Section 116B of the Criminal Procedure Code, subject to a magistrate's warrant. In Thailand, the Trade Secrets Act allows government agencies to disclose trade secrets, including source code, when necessary to

protect public health, safety, or the broader public interest. Such disclosures must not be for commercial purposes and must follow procedures designed to prevent unfair use or competitive harm.

IV. Source Code Disclosure in Trade Agreements

Source code provisions in free trade agreements (FTAs) were initially introduced to address concerns over trade secret misappropriation and forced technology transfer. Over time, however, governments have increasingly recognised the need to regulate digital technologies in the public interest. This has prompted a more nuanced approach that seeks to protect source code while preserving sufficient regulatory space. Four elements illustrate how FTAs have approached this balance.

A. General Prohibitions and Scope

The core feature of most FTAs is a prohibition on requiring the transfer of, or access to, source code of software as a condition for market access. These provisions generally apply to mass-market software and typically exclude software developed for critical infrastructure or customised for government use. Such language appears in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the Indonesia–Australia Comprehensive Economic Partnership Agreement (IA–CEPA), the Singapore–Australia Digital Economy Agreement (SADEA), the UK–Singapore Digital Economy Agreement (UKSDEA), and the Korea–Singapore Digital Partnership Agreement (KSDPA).

It is worth noting that forward-looking agreements do not uniformly include binding source code provisions. The Digital Economy Partnership Agreement (DEPA), often regarded as a benchmark, the upgraded ASEAN–Australia–New Zealand Free Trade Area (AANZFTA), and the stabilised text of the WTO Joint Statement Initiative on Electronic Commerce (WTO JSI) do not contain binding source code obligations. The withdrawal by the United States of its proposed source code text further signals a reassessment of how to balance innovation protection with governments' ability to regulate and pursue legitimate public policy objectives.

B. Exceptions for Regulatory and Judicial Needs

Alongside general prohibitions, some FTAs explicitly recognise that governments may legitimately require access to source code for regulatory or judicial purposes. SADEA, UKSDEA, and KSDPA allow authorities to access source code for investigations, enforcement actions, or legal proceedings, subject to safeguards against unauthorised disclosure. By contrast, earlier agreements such as CPTPP and IA–CEPA permit source code *modification* for compliance

with laws and regulations but do not explicitly guarantee access. This distinction is significant: allowing modification without access may constrain effective oversight and enforcement.

The EU–Singapore Digital Trade Agreement (EU–SG DTA) goes further by explicitly permitting regulatory, enforcement, and competition authorities to access source code in both ex ante and ex post contexts, including for conformity assessments and to ensure digital market fairness. These provisions reflect a growing recognition that broad prohibitions must be balanced with regulatory flexibility.

C. Protection of Algorithms

Earlier agreements, such as CPTPP, are silent on algorithms. More recent agreements, including UKSDEA and KSDPA, extend protection to algorithms 'expressed in that source code.' This reflects concern that explicit reference may be necessary to prevent compelled disclosure of proprietary logic embedded in software systems. However, this approach is not universal: the recently concluded EU–SG DTA does not explicitly mention algorithms.

As machine learning and algorithmic systems are increasingly deployed in sectors such as finance, healthcare, and public services, calls for greater transparency and accountability have intensified. Policymakers therefore face a delicate balance. While protecting the commercial value of algorithms remains important, overly restrictive secrecy provisions may limit regulatory access and undermine public accountability, particularly in high-risk or sensitive applications. A clearer understanding amongst DEFA negotiators of the implications of extending algorithm protection will be essential to avoid unintended constraints on future oversight.

D. Commercial and Voluntary Disclosure

Most FTAs preserve the ability of parties to agree on source code access through voluntary or commercially negotiated arrangements. SADEA and UKSDEA explicitly clarify that open-source licensing remains unaffected, while the EU–SG DTA allows voluntary transfers of, or access to, source code on a commercial basis. These provisions preserve contractual flexibility while maintaining incentives for innovation and the protection of confidential business information.

V. Policy Recommendations

The Digital Economy Framework Agreement (DEFA) presents an opportunity to design source code provisions that reflect a more nuanced understanding of how to protect legitimate commercial interests in

innovation while ensuring that governments retain sufficient oversight to pursue legitimate public policy objectives. The following recommendations outline a balanced and practical approach for DEFA negotiators:

- **Affirm a baseline prohibition** on mandatory source code disclosure as a condition for market access, in line with prevailing global digital trade norms and the protection of intellectual property rights. DEFA should draw on language from recent FTAs to ensure consistency and international benchmarking.
- **Explicitly allow regulatory and judicial access** to source code for both ex ante purposes (such as conformity assessments for high-risk systems) and ex post purposes (such as investigations, enforcement actions, and legal proceedings), subject to appropriate safeguards against unauthorised disclosure. This would preserve regulatory space should ASEAN Member States establish or strengthen accountability frameworks in the future.
- **Clarify the treatment of algorithms** where they are brought within the scope of source code protection, ensuring that such provisions do not impede legitimate regulatory oversight in an evolving technological and regulatory landscape. Where copyright or patent law offers limited protection, trade agreement provisions should not be treated as a substitute for domestic IP regimes.
- **Avoid overly broad or rigid language** that could restrict voluntary source code disclosure through open-source licensing, commercial contracts, or collaborative development arrangements.
- **Address public procurement explicitly** by assessing whether procurement-related source code access should be carved out, either through clearly defined exceptions or within the main source code provision itself, to prevent unintended constraints on government purchasing practices.
- **Strengthen regulatory and enforcement capacity** in areas such as data protection, consumer protection, and algorithmic accountability, to enable effective oversight and to mitigate both intentional and unintentional harms arising from opaque or biased automated systems.

References

- European Patent Office (n.d.), *3.3.1 Artificial Intelligence and Machine Learning*. Retrieved 2 September 2025, from https://www.epo.org/en/legal/guidelines-epc/2023/g_ii_3_3_1.html
- Isono, I. and H. Prilliadi (2023), *ASEAN's Digital Integration: Evolution of Framework Documents*. Economic Research Institute for ASEAN and East Asia (ERIA). <https://www.eria.org/uploads/media/Books/2023-ASEAN-Digital/ASEAN-Digital-Integration-ERIA-23Aug.pdf>
- Mitchell, A.D., D. Let, and L. Tang (2023), 'AI Regulation and the Protection of Source Code', *International Journal of Law and Information Technology*, 31(4), pp.283–301. <https://doi.org/10.1093/ijlit/eaad026>
- WTO (2024), *Trading with Intelligence: How AI Shapes and Is Shaped by International Trade*. https://www.wto.org/english/res_e/booksp_e/trading_with_intelligence_e.pdf

©ERIA, 2025.

DISCLAIMER:

The findings, interpretations, and conclusions expressed herein do not necessarily reflect the views and policies of the Economic Research Institute for ASEAN and East Asia, its Governing Board, Academic Advisory Council, or the Institutions and governments they represent. All rights reserved. Material in this publication may be freely quoted or reprinted with proper acknowledgement.



Sentral Senayan II, 5th, 6th, 15th floors
Jalan Asia Afrika No. 8
Senayan, Central Jakarta 10270, Indonesia
Tel: (62-21) 57974460
E-mail: contactus@eria.org

