ISEAS YUSOF ISHAK INSTITUTE

ISSUE: 2022 No. 67

ISSN 2335-6677

PERSPECTIVE

RESEARCHERS AT ISEAS – YUSOF ISHAK INSTITUTE ANALYSE CURRENT EVENTS

Singapore | 5 July 2022

Better Safeguards Needed for Trusted Data Use in ASEAN Countries

*Sithanonxay Suvannaphakdy**

The expansion of digital connectivity among businesses, consumers and governments both within and across borders increases the need for data safeguards. Image: Designed by pikisuperstar/Freepik at http://www.freepik.com.

* *Sithanonxay Suvannaphakdy is Lead Researcher at the ASEAN Studies Centre, ISEAS – Yusof Ishak Institute.* *He is grateful for valuable comments and suggestions from Sharon Seah. All remaining errors are his own.*

ISSUE: 2022 No. 67
ISSN 2335-6677

EXECUTIVE SUMMARY

- The expansion of digital connectivity among businesses, consumers and governments both within and across borders increases the need for data safeguards to promote trust in data governance and data management.

- An analysis of 31 regulatory elements using data from the World Bank's Global Data Regulation Diagnostic Survey in 2021 reveals that ASEAN as a group has underregulated data safeguards. It has moderately developed a regulatory framework for safeguarding cybersecurity and non-personal data, while it remains at an early stage in the development of a regulatory framework for protecting personal data.

- The regulatory framework for data safeguards is unevenly developed across ASEAN countries. Measures to safeguard cybersecurity are most advanced in the Philippines and Vietnam, but less so in Cambodia, Indonesia, Malaysia, Myanmar, and Thailand. Personal data protection is most advanced in the Philippines, but is at a basic level in Myanmar and Thailand.

- Although limited regulations imply less restrictions on the movement of data, this may affect the willingness of stakeholders in digital trade (e.g. firms, consumers, and governments) to share their data. This highlights the need for coherent regulations to promote digital economies and trade.

- ASEAN should strengthen data safeguards by adopting sector-wide personal data protection laws; establishing coherent data security measures and cybersecurity requirements for data controllers and processors; and providing capacity-building assistance on data safeguards to its members. This should promote more equitable distribution of the gains from data flows, and address risks and concerns of data flows across countries.

ISSUE: 2022 No. 67
ISSN 2335-6677

INTRODUCTION

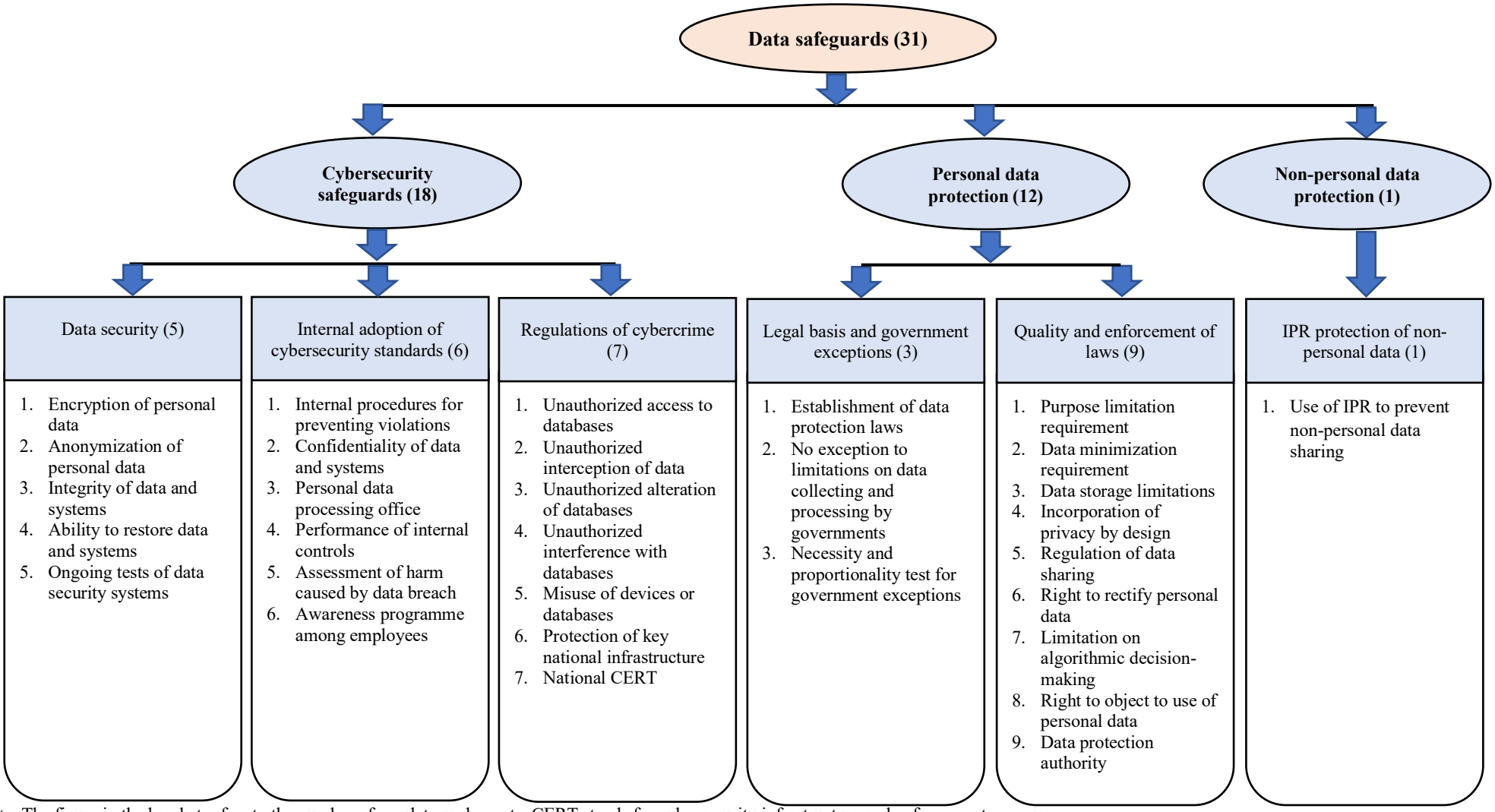
The expansion of digital connectivity among businesses, consumers and governments both within and across borders increases the need for data safeguards. Data safeguards promote trust in the data governance and data management ecosystem by avoiding and limiting harm arising from the misuse of data or breaches affecting its security and integrity. Firms engaging in digital trade usually store customers' bank account and credit card information, email addresses, mailing addresses, and usernames and passwords. One of the key cyber threats to online shoppers in ASEAN in 2020[1] is the e-commerce data interception, which obstructs consumer data transmission to and from the device and remotely alters the messages[2]. This reduces consumer confidence in online payments since cybercriminals may use online data to steal credit card information or use consumers' personal information for identity theft and fraud.

The present study assesses the extent to which ASEAN countries have established national regulatory frameworks for safeguarding data. This is a precondition in the promotion of digital economies and trade in ASEAN. The lack of trust in data use across ASEAN countries could slow cross-border data flows and lead to fragmentation of data, which complicates firms' access to regional supply chains. Cross-border data restrictions and fragmentation could also reduce opportunities for ASEAN governments and firms to strengthen regional collaborations in addressing privacy breaches and cyberattacks.

Following the method used by the World Bank (2021),[3] regulatory frameworks for data safeguards are analysed against 31 regulatory elements; these fall into three broad categories, namely, cybersecurity, personal data protection and nonpersonal data protection (Figure 1). Cybersecurity refers to measures for protecting internet-connected devices, network and data from unauthorized access and criminal use. Cybersecurity safeguards consist of three groups and 18 regulatory elements. These groups include security requirements for automated processing of personal data, cybersecurity requirements for data controllers and processors, and regulation of cybercrime activities for personal data. Safeguards for personal data contain two groups and 12 regulatory elements. These include legal basis and government exceptions in the data protection laws, and the quality and enforcement of data protection laws. The analysis of non-personal data focuses on the use of intellectual property rights (IPR) to prevent data sharing.

ISSUE: 2022 No. 67
ISSN 2335-6677

Figure 1: An analytical framework for assessing data safeguards in ASEAN



Note: The figure in the bracket refers to the number of regulatory elements. CERT stands for cybersecurity infrastructure and enforcement agency.
Source: Author's construction based on World Bank (2021).

Table 1: Scores of regulatory frameworks for data safeguards in ASEAN countries

Country	Cybersecurity and cybercrime	Personal data protection	Nonpersonal data protection
Cambodia	33	33	0
Indonesia	39	50	100
Laos	50	50	0
Malaysia	44	67	100
Myanmar	28	8	0
Philippines	94	83	100
Singapore	61	67	0
Thailand	39	17	100
Vietnam	89	42	100
ASEAN	**53**	**46**	**56**

Note: The table shows the score for good-practice governance by regulatory framework as of 2020. Colours refer to the level of the regulatory framework: = advanced level (score of 75-100); = moderate level (scores of 50-75); = evolving level (scores of 25-50); and = basic level (scores below 25).

Source: Author's calculation based on the World Bank's Global Data Regulation Diagnostic Survey in 2021, available at https://microdata.worldbank.org/index.php/catalog/3866. Accessed April 21, 2022.

Using the World Bank's Global Data Regulation Diagnostic Survey from 2021[4], the analysis of regulatory frameworks for data safeguards in this study reveals that ASEAN has underregulated data safeguards. ASEAN as a group has a moderate level of regulatory framework for safeguarding cybersecurity and nonpersonal data, while it remains at an early stage of developing a regulatory framework for protecting personal data (Table 1). While limited regulations on data safeguards imply less restrictions on the movement of data, they may affect the willingness of digital trade's stakeholders (e.g. firms, consumers, and governments) to share their data due to concerns over data privacy or national security.

The study also shows different levels of regulatory framework across aspects of data safeguards and ASEAN countries. This study suggests the need for ASEAN to constitute more coherent regulations for data safeguards to promote the development of digital economies and trade.

SAFEGUARDING CYBERSECURITY

The analysis of cybersecurity measures in Table 2 reveals that none of the ASEAN countries in this study has imposed a full range of cybersecurity measures on data processors and controllers. The Philippines has the most comprehensive regulatory framework for cybersecurity, followed by Vietnam, Singapore, and Laos. The remaining five ASEAN countries have adopted less than half the cybersecurity measures.

ASEAN countries have made much progress in developing safeguard measures to prevent cybercrime activities such as unauthorized access to databases, unauthorized interception of data, unauthorized deletion or alteration of databases, unauthorized interference of databases, and the establishment of national CERT. Most ASEAN countries are still in early

stages in developing data security measures and internal adoption of cybersecurity standards. The less developed data security measures include the anonymization of personal data, the ability to restore data and systems that use or generate personal data after a physical or technical incident, and ongoing tests, assessments and evaluation of security of systems that use or generate personal data. The less developed cybersecurity standards include appointment of a personal data processing office or manager, and assessment of the harm caused by a data breach.

Table 2: Regulatory elements for cybersecurity in ASEAN countries

No.	Regulatory element	CAM	IDN	LAO	MYS	MMR	PHL	SGP	THA	VNM
1.	Encryption of personal data	No	Yes	No	No	No	Yes	No	No	Yes
2.	Anonymization of personal data	No	No	No	No	No	No	No	No	No
3.	Integrity of data and systems	No	No	No	Yes	No	Yes	Yes	No	Yes
4.	Ability to restore data and systems	No	No	No	No	No	Yes	No	No	Yes
5.	Ongoing tests of data security systems	No	No	No	No	No	Yes	No	No	Yes
6.	Adoption of internal procedures for preventing and detecting violations	No	No	No	No	No	Yes	Yes	No	Yes
7.	Confidentiality of data and systems that generate or use personal data	No	No	Yes	No	No	Yes	No	No	Yes
8.	Appointment of a personal data processing office	No	No	No	No	No	Yes	Yes	No	No
9.	Performance of internal controls	No	No	Yes	No	No	Yes	No	No	Yes
10.	Assessment of the harm caused by a data breach	No	No	No	No	No	Yes	No	No	Yes
11.	Awareness programme among employees	No	No	No	No	No	Yes	Yes	No	Yes
12.	Unauthorized access to databases	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
13.	Unauthorized interception of data	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
14.	Unauthorized deletion or alteration of databases	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
15.	Unauthorized interference with databases	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
16.	Misuse of devices or databases	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes
17.	Legal framework to create a cybersecurity plan to protect key national infrastructure	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
18.	Legal framework to establish a national CERT	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Source: See Table 1.

Note: CAM = Cambodia, IDN = Indonesia, LAO = Laos, MYS = Malaysia, MMR = Myanmar, PHL = Philippines, SGP = Singapore, THA = Thailand, VNM = Vietnam.

Data security measures

Data security measures include security requirements for automated processing of personal data used by data controllers and processors. In ASEAN, the Philippines and Vietnam have the most comprehensive regulatory framework for data security, but they still need to create a data security measure on the anonymization of personal data. Malaysia and Singapore have not yet established four data security measures, namely, the encryption of personal data, anonymization of personal data, ability to restore data and systems, and ongoing tests

of data security systems. Indonesia has not yet created data security measures on anonymization of personal data, integrity of data and systems, ability to restore data and systems, and ongoing tests of data security systems. Cambodia, Laos, Myanmar, and Thailand have not yet adopted any data security measures (Table 2).

Internal adoption of cybersecurity standards

Internal adoption of cybersecurity standards refers to the adoption of cybersecurity requirements by data controllers and processors. This is uneven across ASEAN countries. Only the Philippines has adopted all cybersecurity standards for data controllers and processors. Data controllers and processors in Vietnam are not required to comply with a cybersecurity standard for appointing a personal data processing office or manager, while those in Singapore are not required to comply with cybersecurity requirements on confidentiality of data and systems, performance of internal controls, and assessment of the harm caused by a data breach. Data controllers and processors in Cambodia, Indonesia, Malaysia, Myanmar and Thailand are not required to comply with any cybersecurity standards (Table 2). This suggests the fragmentation of cybersecurity standards in ASEAN. Harmonizing these standards is needed to reduce the compliance costs for firms engaging in digital trade.

Regulation of cybercrime activities for personal data

Regulatory measures to prevent cybercrime – criminal acts committed online by using electronic communications networks and information systems[5] – have been widely adopted by ASEAN countries. These measures include unauthorized access to systems or other databases holding personal data; unauthorized interception of data from systems or other databases holding personal data; unauthorized damaging deletion, deterioration, alteration or suppression of data collected or stored as part of databases holding personal data; unauthorized interference with databases holding personal data; and misuse of devices or data for the purpose of committing any of the above criminal behaviour (Table 2).

Establishment of cybersecurity infrastructure and enforcement agency (CERT)

All nine ASEAN countries in this study have established a legal framework to establish their national CERT. Seven out of these nine ASEAN countries also have a legal framework to create a cybersecurity plan to protect key national infrastructure. These include Indonesia, Laos, Malaysia, the Philippines, Singapore, Thailand, and Vietnam (Table 2).

In Singapore, for example, the Cyber Security Agency of Singapore (CSA) was established in 2015 and is managed by the Ministry of Communications and Information. CSA aims to protect critical information infrastructure to ensure the continuous delivery of essential services such as telecommunication, energy, healthcare, and banking; create a vibrant cybersecurity ecosystem comprising skilled professionals, strong research and development expertise, and companies with deep cybersecurity capabilities to promote a digital economy; and conduct outreach programmes to raise awareness and promote adoption of

good cyber hygiene practices by the public.[6] These goals are further elaborated in its cybersecurity strategy 2021, which was first launched in 2016.[7]

SAFEGUARDING PERSONAL DATA

Measures to protect personal data are based on individuals' substantive and procedural rights. Substantive rights include measures that prevent the unauthorized disclosure of personal data and the use of personal data for unfair treatment as well as measures that require purpose specification, data minimization, and storage limitations. Procedural rights include measures that allow individuals to receive notice about and to object to the use of their personal data as well as measures that allow them to correct and erase their data.

Table 3: Regulatory elements to protect personal data in ASEAN countries

No.	Regulatory element	CAM	IDN	LAO	MYS	MMR	PHL	SGP	THA	VNM
1.	Establishment of data protection law across sectors	No	No	No	Yes	No	Yes	Yes	No	No
2.	No exception to limitations on data collecting and processing by governments	Yes	No	Yes	No	Yes	No	No	Yes	No
3.	Necessity and proportionality test for government exceptions	No	No	No	No	No	No	No	No	No
4.	Purpose limitation requirement	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes
5.	Data minimization requirement	Yes	Yes	No	Yes	No	Yes	Yes	No	No
6.	Data storage limitations	No	Yes	No	Yes	No	Yes	Yes	No	Yes
7.	Requirements to incorporate privacy by design	No	No	No	No	No	Yes	No	No	No
8.	Regulation of data sharing with third parties	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
9.	Individual right to challenge accuracy and rectify personal data	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes
10.	Regulatory limitation on algorithmic decision-making	No	No	No	No	No	Yes	No	No	No
11.	Individual right of redress to object to use of personal data	No	Yes	Yes	Yes	No	Yes	Yes	No	Yes
12.	Data protection authority	No	No	Yes	Yes	No	Yes	Yes	No	No

Source: See Table 1.

The analysis of personal data protection in Table 3 reveals that the Philippines has the most comprehensive regulatory framework for the protection of personal data, but it still needs to adopt a regulatory measure that requires the necessity and proportionality test for the use of personal data by public authorities. Malaysia and Singapore need to establish regulatory measures for the necessity and proportionality test for government exceptions, incorporation of privacy by design, and limitation on algorithmic decision-making. The regulatory frameworks for safeguarding personal data in the remaining six ASEAN countries are significantly lagging behind the Philippines, Malaysia, and Singapore, especially in the adoption of data protection law across sectors, the imposition of limitations on data storage, and the establishment of national personal data protection authority.

Establishment of personal data protection laws

Laws on personal data protection – the protection of data about an individual who can be identified from those data, or from those data and other information to which a data controller or processor has or is likely to have access to – provide a baseline standard of protecting personal data. Such a law comprises various requirements governing the collection, use, disclosure and care of personal data in a country. It aims to protect individuals' personal data, while enabling the public and private sectors to collect, use or disclose personal data for legitimate and reasonable purposes.

Three out of the nine ASEAN countries have constituted a data protection or privacy law of general application to govern the use, collection and processing of personal data across sectors. These are Malaysia, the Philippines, and Singapore (Table 3). The remaining six countries have only sector-specific personal data protection law. Different scopes of regulatory framework on data protection may impede the transfer and sharing of data for digital trade in ASEAN.

Government exceptions to limitations on data collection and processing

The collection and processing of personal data by ASEAN governments should be subject to the necessity and proportionality test to enhance transparency and trust in data use. Limitations on the use of personal data should apply to both the private and public sectors which processes or controls personal data. Four out of the nine ASEAN governments have created exceptions to limitations for data processing by public authorities. These are Indonesia, Malaysia, Singapore, and Vietnam. These exceptions should be limited to specific data uses such as ensuring national security and performing lawful government functions.

However, ASEAN governments have not yet constituted a legal provision to regularly review the efficiency and effectiveness of the established government exceptions. This may result in the lack of transparency and a monitoring mechanism in the implementation of government exceptions on personal data, and hence undermines trust in data use.

Quality of data protection laws

The quality of data protection laws is also uneven across ASEAN countries. These laws should allow individuals to challenge the accuracy and object to the use of personal data, while requiring data processors to limit the purpose of data use, the volume of data collection, and timeframe for data storage. The Philippines is the only ASEAN country that incorporates all of these legal provisions. Indonesia, Malaysia, Singapore, and Vietnam have not yet included legal provisions on privacy by design and automated decision. A legal provision on the privacy by design requires data processors to incorporate technical and organizational privacy-by-design or use privacy enhancing technologies in the design and implementation of processing systems. A legal provision on the automated decision limits decision making about individuals due to automated processing of personal data such as the use of artificial intelligence and machine learning.

Legal provisions on the quality of data protection laws are much less prevalent in Cambodia, Laos, Myanmar and Thailand. Cambodia has incorporated only a provision on individual rights to challenge the accuracy and rectify personal data. Thailand has included only a provision on limitations on data sharing, while Laos has incorporated provisions on limitations on data sharing, individual rights to challenge the accuracy and rectify personal data, and redress. A provision on redress allows individuals to object to the use of personal data about them, file complaints and seek redress.

Enforcement of data protection laws

The enforcement of data protection laws has been undermined by the lack of a national data protection authority. Only four out of the nine ASEAN countries have established such a national data protection authority. Malaysia, the Philippines and Singapore have adopted sector-wide personal data protection laws, and created the authorities for their enforcement. Laos has constituted a sector-specific personal data protection law, and established the institution to enforce it. Cambodia, Indonesia, Myanmar, Thailand, and Vietnam have constituted sector-specific personal data protection laws, but they have not yet created any institutions to enforce such laws.

SAFEGUARDING NON-PERSONAL DATA

Safeguards for the use and reuse of non-personal data produced by the private sector may be covered by the IPR. Five out of the nine ASEAN countries have constituted the IPR that can be used to prevent the sharing of nonpersonal data. These include Indonesia, Malaysia, the Philippines, Thailand and Vietnam. The remaining ASEAN countries have not yet done so.

However, the IPR protection of non-personal data contradicts other policies that encourage the interoperability of data systems and the free reuse of data. In this case, governments should create rules for the private sector to set reasonable prices for the use of licensed data-driven products and services generated using public sector data. One way to do this is to mandate firms to license those products on fair, reasonable and non-discriminatory (FRAND) terms.

In ASEAN, only Malaysia (e.g. standard-setting organizations) has mandated IPR holders to provide voluntary licensing access to critical data or applications based on FRAND terms.[8]

CONCLUSION AND POLICY IMPLICATIONS

The development of a regulatory framework for data safeguards is uneven across ASEAN countries. On average, safeguards for cybersecurity and non-personal data in ASEAN are

moderately developed, while safeguards for personal data are the weakest area of performance. The level of regulatory framework for safeguarding cybersecurity is most advanced in the Philippines and Vietnam, while it is less developed in five of the ASEAN countries, namely, Cambodia, Indonesia, Malaysia, Myanmar, and Thailand. The level of regulatory framework for protecting personal data is most advanced in the Philippines, while it is at the basic level in Myanmar and Thailand. Indonesia, Malaysia, the Philippines, Thailand and Vietnam have used the IPR to prevent the sharing of nonpersonal data, while other ASEAN countries have not yet done so.

Strengthening data safeguards in ASEAN should focus on three aspects. First, ASEAN countries that lack a sector-wide personal data protection law should accelerate the process of adopting and implementing it. The personal data protection law plays an important role in enhancing trust for data use in digital economies and trade. Without it, individuals may not be willing to share their personal data; and policymakers would impose restrictions on data flows. Although the existing consumer protection and competition laws in ASEAN can be helpful to address certain manifestations of the misuse of personal data, their scopes of application are limited. These laws are complements, but not substitutes for the personal data protection law.

The development of personal data protection law in ASEAN should follow good regulatory practices, which consist of impact assessment of proposed law, stakeholder consultations, and ex-post evaluation of the law. These practices should enhance the quality of personal data protection law, and avoid unnecessary, duplicative or inefficient provisions in such a law. ASEAN countries should also promote the interoperability of data privacy approaches and reference to international standards, principles, guidelines and criteria when developing their national personal data protection laws. This is essential to facilitate cross-border data flows and protect personal data in the region.

Second, ASEAN countries should accelerate the adoption of coherent data security measures and cybersecurity requirements for data controllers and processors. Under-regulation of cybersecurity increases the risks of cyber threats and reduces trust in digital economies and trade. ASEAN countries should use the existing regional trade agreements such as the Regional Comprehensive Economic Partnership (RCEP) and the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) to reinforce the role of consensus-based standards with commitments to develop international standards and to use international standards where they exist as a basis for developing their domestic regulations on data security and cybersecurity requirements for data controllers and processors. This should support the implementation of the ASEAN Cybersecurity Cooperation Strategy 2021-2025[9] to enhance regional cybersecurity cooperation. Also, this should also promote the development of globally consistent and least trade-restrictive approaches to cybersecurity, while reducing concerns over the use of cybersecurity measures as a disguised restriction on trade aimed at supporting domestic industry.

Finally, ASEAN as a group should pledge capacity-building assistance on data safeguards for its members, especially emerging economies such as Cambodia, Laos, Myanmar and Vietnam. Such assistance should aim at raising awareness and understanding of the importance of data safeguards that meet international standards, principles and guidelines

as well as supporting them to implement national regulatory reforms for developing or aligning their laws. This should ensure more equitable distribution of the gains from data flows, while addressing risks and concerns across countries. Without such technical assistance, ASEAN countries that have limited technical capacity may not be able to undertake regulatory reforms for data safeguards, which result in regulatory divergence in ASEAN. Such regulatory divergence impedes cross-border data flows, and limits the benefits of digital economies and trade in the region.

Efforts to strengthen regional data safeguards should be driven by the existing sectoral bodies in ASEAN. These include the ASEAN Network Security Action Council (ANSAC), Working Group on Digital Data Governance (WG-DDG), and ASEAN Coordinating Committee on Electronic Commerce (ACCEC). The ANSAC is in charge of coordination on ASEAN cybersecurity cooperation activities, while the WG-DDG is responsible for developing and implementing the ASEAN Framework on Digital Data Governance in the digital sector.[10]

These two working groups should play an important role in translating the existing commitments on regional data safeguards into national action plans, or proposing new ones. Meanwhile, engaging the ACCEC in the establishment of regional data safeguard measures should be helpful in providing feedback on the potential impacts of the proposed data safeguard measures on cross-border e-commerce transactions, and hence reducing the compliance costs for traders. The ACCEC aims to enhance the coordination of initiatives on ASEAN e-commerce, and consists of representatives from trade-related government agencies (e.g., trade, customs, transport facilitation, consumer protection, standards and conformance, and micro, small, and medium enterprises) from all ASEAN countries.[11]

ENDNOTES

[1] ASEAN Cyberthreat Assessment 2021: https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf
[2] IGI Global: https://www.igi-global.com/dictionary/data-interception/63971
[3] World Bank. 2021. *World Development Report 2021: Data for Better Lives*. Washington, DC: World Bank.
[4] World Bank, Global Data Regulation Diagnostic Survey Dataset 2021: https://microdata.worldbank.org/index.php/catalog/3866. Accessed April 12, 2022. This study does not include Brunei due to data unavailability; that country was not included in the survey either.
[5] European Commission: https://ec.europa.eu/home-affairs/cybercrime_en
[6] Cyber Security Agency of Singapore: https://www.csa.gov.sg/Who-We-Are/Our-Organisation
[7] The Singapore Cybersecurity Strategy 2021: https://www.csa.gov.sg/News/Publications/singapore-cybersecurity-strategy-2021
[8] ISES Perspective: https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-32-enabling-domestic-data-flows-for-e-commerce-in-asean-countries-by-sithanonxay-suvannaphakdy/

[9] ASEAN Cybersecurity Cooperation Strategy: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf
[10] ASEAN digital sector: https://asean.org/our-communities/economic-community/asean-digital-sector. Accessed June 16, 2022.
[11] ASEAN e-commerce: https://asean.org/our-communities/economic-community/asean-e-commerce. Accessed June 16, 2022.

ISEAS Perspective is published electronically by: **ISEAS - Yusof Ishak Institute** 30 Heng Mui Keng Terrace Singapore 119614 Main Tel: (65) 6778 0955 Main Fax: (65) 6778 1735 Get Involved with ISEAS. Please click here: https://www.iseas.edu.sg/support/get-involved-with-iseas/	ISEAS - Yusof Ishak Institute accepts no responsibility for facts presented and views expressed. Responsibility rests exclusively with the individual author or authors. No part of this publication may be reproduced in any form without permission. © Copyright is held by the author or authors of each article.	Editorial Chairman: Choi Shing Kwok Editorial Advisor: Tan Chin Tiong Editorial Committee: Terence Chong, Cassey Lee, Norshahril Saat, and Hoang Thi Ha. Managing Editor: Ooi Kee Beng Editors: William Choong, Lee Poh Onn, Lee Sue-Ann, and Ng Kah Meng Comments are welcome and may be sent to the author(s).