Sri Handayani Nasution

Research Report

Improving data governance and personal data protection through ASEAN Digital Masterplan 2025

Policy Paper, No. 46

Provided in Cooperation with:
Center for Indonesian Policy Studies (CIPS), Jakarta

Suggested Citation: Sri Handayani Nasution (2021) : Improving data governance and personal data protection through ASEAN Digital Masterplan 2025, Policy Paper, No. 46, Center for Indonesian Policy Studies (CIPS), Jakarta

This Version is available at:
https://hdl.handle.net/10419/251310

CIPS
Center for Indonesian Policy Studies

Policy Paper No. 46

Improving Data Governance and Personal Data Protection through ASEAN Digital Masterplan 2025

by Sri Handayani Nasution

www.cips-indonesia.org

We would like to thank the Center for International Private Enterprise for their support of this publication

Copy Editor:
Janet Bufton

Acknowledgement:
The authors would like to thank Thomas Dewaranu for his tremendous assistance in this paper.

Cover:
mikeygl/Freepik.com

Policy Paper No. 46

Improving Data Governance and Personal Data Protection through ASEAN Digital Masterplan 2025

Authors:

Sri Handayani Nasution

(Center for Indonesian Policy Studies)

Jakarta, Indonesia

December, 2021

CONTENT

LIST OF TABLES

GLOSSARY

ADM:
ASEAN Digital Masterplan 2025

ADGMIN:
ASEAN Digital Ministries Meeting

AMS:
ASEAN Member States

APEC CBPR:
Asia Pacific Economic Cooperation Cross Border Data Privacy Rules

ASEAN:
The Association of Southeast Asian Nations

ASEAN DDG:
ASEAN Framework on Digital Data Governance

ASEAN PDP:
ASEAN Framework on Personal Data Protection

BCR:
Binding Corporate Rules

CBDF:
ASEAN Cross Border Data Flow Mechanisms

COD:
Cash on Delivery

CIPE:
Center for International Private Enterprise

DO:
Desired Outcomes

DPA:
Data Protection Authority

EA:
Enabling Actions

EU:
European Union

FDI:
Foreign Direct Investment

IoT:
Internet of Things

IRR:
Implementing Rules and Regulations

GDPR:
General Data Protection Regulation

MOCI:
Ministry of Communication and Informatics

MCC:
ASEAN Model Contractual Clauses

NPC:
National Privacy Commission

PDP:
Personal Data Protection

PDPA:
Personal Data Protection Act

EXECUTIVE SUMMARY

The ASEAN Digital Ministries Meeting introduced the ASEAN Digital Masterplan 2025 (ADM) in pursuit of its vision of ASEAN as the leading digital community and digital economic bloc, powered by secure and transformative digital services, technologies, and ecosystems. The ADM complements the ASEAN Framework on Personal Data Protection and ASEAN Framework on Digital Data Governance, specifying eight desired outcomes and associated enabling actions to achieve this vision by 2025.

One of the targets of the ADM is the delivery of trusted digital services and prevention of consumer harm. The ASEAN digital economy is the fastest growing in the world—predicted to reach a value of USD 1 trillion by 2030. Comprehensive regulations, especially regarding data protection and data governance in each ASEAN Member State, are needed to safeguard consumer rights and improve public trust during the digital boom in the region.

Data protection policies vary between ASEAN Member States. Most ASEAN Member States have personal data protection regulations in place, though in some cases these are scattered piecemeal through different laws and regulations (as in Indonesia and Vietnam). States that possess codified personal data protection laws should nonetheless consider improvements, such as providing clear provisions on transnational data transfer (the Philippines) and requiring notification in the event of a data breach (Malaysia).

The lack of a data protection framework is usually accompanied by blurred data categorization, with repercussions for other data-related policies including data localization, unclear provisions on data governance, and cross-border data sharing. Taken together, these issues hinder digital economic growth potential in the region. In the worst case, regulatory gaps may also attract corrosive investment that could hurt consumers in the long term. Two governance gaps are the tendency to enact data localization policies among ASEAN Member States and the lack of a regional regulatory framework on digital infrastructure investment.

To eliminate the identified governance gaps, ASEAN Secretariat should engage in awareness-raising initiatives on the relationship between digital infrastructure investment and data-related regimes through sectoral bodies or meetings, and should formulate a regulatory framework and guiding document for ASEAN digital infrastructure investment.

OVERVIEW OF ASEAN DIGITAL ECONOMY LANDSCAPE: POTENTIALS AND SHORTCOMINGS

Generating around USD 150 billion in 2020 and set to reach USD 1 trillion in 2030, Southeast Asia's digital economy is among the fastest-growing in the world (Kearney, 2021). Rapidly increasing internet penetration and mobile phone use expanded the market for digital services in the region and attracted both domestic and foreign investment to help provide digital solutions for consumers. Electronic commerce (e-commerce), food and transportation, and online media have so far been the main drivers in digital economic growth in the region and are predicted to remain significant.

Policies to ensure data protection and transparent data sharing and processing are needed to safeguard consumers' digital rights without discouraging innovation to support the growth potential of the digital economy in the region. Access to user data is crucial for digital platforms to innovate—it provides insight on how to create services that suit consumer profiles (Chen, 2020). Data sharing between platforms also allows businesses to efficiently develop marketable products and services. It helps to create new business opportunities, increase cross-sector cooperation, such as the integration of the value chain, and increases efficiency through data linkage and integration (OECD, 2019, p.64). Regulations need to carefully balance these benefits with the risks of privacy violations so that interests of businesses and consumers are adequately protected.

Regulatory gaps in ASEAN Member States must be addressed for the digital economy in the region to achieve its full potential. The growing number of digital service users is often not accompanied by robust regulations in areas like personal data protection. While this is apparent in countries like Vietnam and Indonesia, countries with relatively better regulatory frameworks like Malaysia, Singapore, Thailand, and the Philippines also face implementation challenges (World Bank, 2019). The lack of comprehensive personal data access and sharing regulations can negatively affect consumer trust, preventing the digital economy from reaching its full potential.

> "Digital consumer trust is crucial to support the digital economy in ASEAN. The region is among the most vulnerable to cyberattacks and personal data leaks (Microsoft, 2019) which drive down confidence and trust in services such as digital payment."

Digital consumer trust is crucial to support the digital economy in ASEAN. The region is among the most vulnerable to cyberattacks and personal data leaks (Microsoft, 2019) which drive down confidence and trust in services such as digital payment. For instance, many Malaysian and Thai customers prefer cash on delivery (COD) payment (Brewer, 2017 from Ismail & Masud, 2020; Laksanapanyakul, 2020) often out of concern for security and privacy (Ismail & Masud, 2020). If trust issues are left unaddressed, they may translate into low adoption of digital tools and hamper digital economic growth in the region (World Bank, 2019; Kearney, 2020).

The ASEAN Digital Masterplan 2025 (ADM) recognizes these challenges and has included the "delivery of trusted digital services and the prevention of consumer harm" as its third desired

outcome (Desired Outcome 3). Desired Outcome 3 emphasizes that broader adoption of digital services is contingent upon the level of consumer trust and suggests that best practices in cybersecurity and data governance to be broadly implemented. Enabling Action 3.3 from this desired outcome suggests to "Identify Improvements in Legal and Regulatory Measures on the Management of Protection of Data and Other Data-Related Activities that Could Be Harmful".

This paper focuses on Desired Outcome 3 and Enabling Action 3.3 and reviews the data protection and data governance regulations in selected ASEAN Member States: Singapore, Malaysia, the Philippines, Thailand, Indonesia, and Vietnam. These states, excluding Singapore, have been selected due to their status as emerging economies in ASEAN. Singapore has been included because it is an ASEAN Member State with consolidated data protection regulations in place.[1]

Data governance covers a wide range of subjects, but this brief focuses on personal data protection and data sharing and examines how they are regulated in the selected member states. Data protection and data sharing are not always clearly separated and often overlap in policy discussions. In addition to highlighting the benefits that can be achieved through regulatory reform, this brief also shows the risks of corrosive investment in the region if regulatory gaps are left unaddressed.

This paper will perform a general overview on the problem and research gap, a general overview of ADM and review on selected ASEAN Member State regulations, discussion on digital investment in ASEAN and identification of possible governance gaps, and finally it will present conclusions and recommendations.

[1] Discussions on Myanmar, Cambodia, Brunei, and Lao PDR are omitted. There have not been significant efforts to develop comprehensive data protection laws there.

ASEAN DIGITAL MASTERPLAN: ESTABLISHING NORM ON THE REGION'S DATA GOVERNANCE

The ADM presents itself as comprehensive, measurable, and best-practice guidance to boost digital economic growth in the region. It identifies existing barriers and problems in ASEAN digital economic development and provides recommendations to address them. The ADM builds upon the ASEAN Framework on Personal Data Protection (ASEAN PDP) and ASEAN Framework on Digital Data Governance (ASEAN DDG). The ADM recognizes the importance of facilitating cross-border data flows to develop the region's digital economy. It also advocates the development of regulatory measures that build on the Implementing Guidelines for the ASEAN Cross Border Data Flows Mechanism (CBDF) 2021.

The ADM envisions ASEAN to be the leading digital economy with safe and secure transformative digital services, technologies, and ecosystems. To achieve that, it specifies eight desired outcomes, each with enabling actions to achieve the vision by 2025. Desired outcomes are the targeted outcomes, while enabling actions are the suggested actions to achieve them.

Desired Outcome 3 and Enabling Action 3.3 aim to increase the delivery of trusted digital services and prevention of consumer harm (Desired Outcome 3) by improving legal and regulatory measures on the management of protection of data and other data-related activities that could be harmful (Enabling Action 3.3). This can be achieved by addressing key issues, such as establishing ASEAN's position in regulating 'big tech' platforms; developing ASEAN model legislation; harmonizing data protection legislation across ASEAN Member States to promote cross-border data transfer; and developing integrated data protection guidelines.

Outside of Desired Outcome 3 and Enabling Action 3.3, the issue is also discussed in Enabling Action 4.1, which tries to map the regulatory barriers and identify opportunities to harmonize regulations to facilitate the cross-border data flow. To a lesser extent, this paper will also discuss repercussions from the lack of data protection regulations and data governance to cross-border data flow in the region.

The ADM has a measurement system to track the progress of each enabling action to achieve the relevant desired outcomes. The progress of Enabling Action 3.3 will be measured by the publication of a study that addresses key issues mentioned above and emphasizes the promotion of best practices, regulatory approaches, and model legislation for regulation of data-related activities throughout the region. The success indicator of Enabling Action 4.1 will be measured by conducting a study and mapping the barriers to cross-border data flows (Table 1).

Table 1.
Desired Outcomes and Enabling Actions Related to Data Protection and Data Governance

Desired Outcomes	Enabling Actions	Measurement
3. The delivery of trusted digital services and the prevention of consumer harm	3.3 Identify improvements in legal and regulatory measures on the management of protection of data and other data-related activities that could be harmful.	3.3. Publication of a study on regulatory approaches, best practices, and model legislation for regulating big data platforms, exchange of cloud-based data, and ensuring personal data protection.
4. A sustainable competitive market for the supply of digital services	4.1 Continue to identify opportunities to harmonize digital regulation to facilitate cross-border data flows.	4.1 Study and mapping of barriers to cross-border data flows.

(Source: ASEAN Digital Masterplan 2025)

Improving ASEAN Member State data protection and governance regulations is crucial for building a secure digital environment. Regulations governing personal data protection provide guidance for responsible data collection and processing, hopefully leading to a decrease in data leaks and breaches. Harmonized data protection regulations in ASEAN Member States should endorse cross-border data transfer mechanisms with a clear and explicit division between stakeholders in order to create a conducive and easy-to-navigate environment for business.

"Improving ASEAN Member State data protection and governance regulations is crucial for building a secure digital environment."

However, the ADM is not legally binding, and ASEAN operates with a non-interference principle that makes the development of a regional, legally binding document on this issue unlikely. Fortunately, the first ASEAN Digital Ministries Meeting in January 2021 approved ASEAN Model Contractual Clauses, or MCC (Ministry of Communication and Information Singapore, 2021). The MCC serves as a binding contractual agreement between businesses (or parties) in ASEAN that wish to transfer data across borders.[2] The MCC provides a standard baseline of data protection clauses for businesses which may be modified in accordance with the ASEAN PDP or any other relevant ASEAN Member State regulations. The MCC details obligations of parties to ensure protections through the ASEAN PDP, such as the requirement that parties provide a lawful basis for data collection, use, and disclosure, process data in accordance with the ASEAN PDP, and to notify data subjects in case of data breach.

[2] See ASEAN Model Contractual Clauses for Cross Border Data Flows

ADM can also serve as a set of guiding principles to harmonize data protection and governance regulations across the region, which may increase both consumer trust and the adoption and innovation of digital services in the region. Both ASEAN PDP and ASEAN DDG provide guiding principles and encourage member states to incorporate these principles in their domestic policies. Several principles in the ASEAN PDP are:

- "consent, notification, and purpose," which stresses the urgency of consent in data collection stage;
- "accuracy of personal data," which emphasizes the proportionality of data being collected;
- "security safeguards," which ensures the protection of personal data;
- "access and correction," which gives leverage to individuals over their data;
- "transfers to another country or territory," which re-emphasizes the importance of consent in data transfer;
- "retention," which details the organization's obligation to dispose the personal data when they are no longer necessary; and
- "accountability," which ensures transparency in handling personal data.

Meanwhile, the ASEAN DGD has several strategic priorities related to its respective principles, detailed in Table 2.

Table 2.
ASEAN DDG Strategic Priorities and Principles

Framework	Strategic Priority	Principle
ASEAN Framework on Digital Data Governance (ASEAN DDG)	Data life cycle and ecosystem	Principle on data integrity and trustworthiness
		Principle on data use and access control
		Principle on data security
	Cross Border Data Flows	Principle on cross border data flows
	Digitalisation and Emerging Technologies	Principle on capacity development
	Legal, Regulatory, and Policy	Principle on personal data protection and privacy regulation
		Principle on accountability
		Principle on development and adoption of best practices

(Source: ASEAN Framework on Digital Data Governance)

DATA REGULATIONS IN ASEAN MEMBER STATES

Data protection laws and regulations in ASEAN vary between member states. Although most ASEAN Member States have data protection regulations in place, some exist scattered piecemeal through different laws and regulations while others have a specific law that aims to regulate data use on the internet.

The Philippines, Singapore, Malaysia, and Thailand: Proponents of Digitally Safe ASEAN

"Although most ASEAN Member States have data protection regulations in place, some exist scattered piecemeal through different laws and regulations while others have a specific law that aims to regulate data use on the internet."

Four ASEAN Member States that have enacted specific personal data protection regulations are the Philippines, Singapore, Malaysia, and Thailand. Malaysia's 2010 Personal Data Protection Act (PDPA) was the first data protection act in Southeast Asia, followed by the Philippines' 2012 Data Protection Act, Singapore's 2012 Personal Data Protection Act, and Thailand's Personal Data Protection Act B.E. 2562 (2019) (World Bank, 2019). PDPAs in Singapore and Malaysia focus on data collection and data use mainly by the private sector. The act in the Philippines and Thailand cover data used by both the public and the private sector.

Data processing in Singapore requires consent, contractual safeguards, certifications, and binding corporate rules. Singapore is a part of the Asia Pacific Economic Cooperation Cross Border Privacy Rules system, which facilitates cooperation between states practicing cross-border data transfer in Asia Pacific (Asia Business Law Institute [ABLI], 2020; APEC, n.d.).

The Philippines, because of its extensive trade with the European Union, operates in compliance with the EU General Data Protection Regulation (GDPR) to facilitate trade. However, domestic law in the Philippines lacks guarantees for data protection in cross-border data transfers. The Data Protection Act and its implementing rules and regulations do not make self-assessment a responsibility for organizations that wish to process data transnationally. Instead, the act and its regulations are generally vague about protections for transnational data flows (ABLI, 2020; Disini, 2018).

Malaysia, in addition to passing the PDPA 2010, published the PDPA Standard 2015 and the PDP (Class of Data Users) (Amendment) Order 2016 (Noor Sureani et al., 2021). As in other legal environments governing personal data in the region, it regulates fundamental elements of personal data protection, such as consent and the security obligations of platforms. However, the PDPA does not explicitly include the right to be forgotten nor does it protect user data in social media, despite this being a vulnerable area for personal data in the country (Sureani et al., 2021). PDPA 2010 Article 1 paragraph 2 states the law applies to "...any personal data in respect of commercial transactions" in which "commercial transactions" is understood as "any transaction of a commercial nature...which includes any matters relating to the supply or

exchange of goods...". Overall, Malaysia's PDPA shares similar provisions with the EU GDPR, although in actuality it is based on the EU Data Protection Directive (1995) (Hassan, 2012).

Thailand's newly enacted PDPA B.E. 2562 (2019) is the first explicitly "GDPR-based" data protection regime in Asia (Privacy Laws & Business, 2019). The PDPA B.E. 2562 (2019) regulates both the private and the public sector, although unlike the Philippines, there are several public institutions that are exempted. The regulation is similar with the GDPR but omits some fundamental parts, such as privacy by design[3] and the independence of the Data Protection Authority (Privacy Laws & Business, 2019).

The regulations in these four member states follow the general principle of the ASEAN PDP to varying degrees. On consent, notification, and data collection purposes, they all require data controllers to obtain explicit consent from data owners prior to using their data. Controllers must also notify users that their data is being collected and specify the reason and purpose for data collection. Data owners may also ask for access to their data, make corrections, and even withdraw their consent. However, in the case of a data breach, Malaysia's PDPA is the outlier—it does not require notification to the data owner in the event of a data breach among the four member states, although discussions are in process to amend the law in order to remedy this (Data Guidance, 2021).

Another notable difference is in the creation of data protection authorities. Among the four member states, only the Philippines has created an independent data protection authority, the National Privacy Commission (NPC). Both Malaysia and Singapore have data protection agencies housed under a government ministry, though they are administratively separated from it (Data Guidance, n.d.). Meanwhile, Thailand does not specify the status of its Personal Data Protection Committee (Data Guidance, n.d.). In Thailand, the committee's role is to be the primary body enforcing the law but it does not have financially or legislatively guaranteed independence (Privacy Laws & Business, 2019).

"The four member states mostly fulfill the data protection and governance principles provided by ASEAN, but varying degree of implementation might hamper cross-border data transfer."

The four member states mostly fulfill the data protection and governance principles provided by ASEAN, but varying degree of implementation might hamper cross-border data transfer, since some provisions might affect the assessment of adequacy decision[4] of other states. Further harmonization is desirable for this reason.

[3] "Privacy by design" and "privacy by default" are two principles adopted in GDPR Art 25. Privacy by design and by default urges the data controller to incorporate safeguards that guarantee personal data protection and privacy in their early stage of product, infrastructure, or feature development.

[4] Adequacy decision refers to the ability of a state to assess whether a country outside its jurisdiction offers the same level of protection for personal data. The EU requires adequacy assessments before allowing transfers of data belonging to EU citizens. ASEAN Member States such as Singapore, Thailand, and Malaysia possess similar provisions in their data protection regulations (ABLI, 2020)

Vietnam and Indonesia: Data Protection in Development

Vietnam and Indonesia are among the member states that do not possess a single, comprehensive set of data protection and governance regulations. As of 2020, Vietnam governed privacy and personal data protection through several regulations, such as the Law on Cybersecurity, Law on Cyber Information Security, and Law on Electronic Transaction, (World Bank, 2019; DLA Piper, 2020b). Similarly, provisions for personal data protection in Indonesia are scattered among at least 32 regulations (Ministry of Communication and Informatics [MOCI], n.d.; Riyadi, 2021). Despite Indonesia's status as the largest digital economy in Southeast Asia, the country is still discussing its PDP bill.

As it stands, Indonesia's scattered data protection regulations fall short of the principles in ASEAN PDP and ASEAN DDG, but its PDP bill does show a degree of consistency with the ADM and ASEAN PDP principles. The PDP bill upholds the principle of consent in important data cycle stages and provides greater control of individuals over their personal data.[5] Indonesian lawmakers are also debating the status of its DPA (Schweitzer-Caput, 2021). If Indonesia opts for a non-independent body, it might affect the adequacy decision by the EU or other countries with similar provisions to the GDPR.

Meanwhile, Vietnam's data protection law exists piecemeal across at least 12 regulations and guiding documents (DLA Piper, 2021a). The most important data protection regulations in the Vietnam might be the Law on Network Information Security (2015), Law on Cyber Information Security (2015) and Law on Cyber Security (2018). However, these regulations emphasize the state's power to control data and flow of information rather than focusing on empowering individuals to control their data (DLA Piper, 2021a). Law on Network Information Security (2015) regulates the protection of "personal information" in Article 16, Article 17, Article 18, Article 19, and Article 20 but limits its scope for commercial purposes only.[6] The Law on Cyber Security (2018) briefly mentions personal data protection processing by service providers (Art 26.3), without further details.

> "Loopholes and patchwork regulations in both Indonesia and Vietnam create issues for data governance: unclear data categorization, restrictive cross-border data sharing provisions, and data localization obligations."

Loopholes and patchwork regulations in both Indonesia and Vietnam create issues for data governance: unclear data categorization, restrictive cross-border data sharing provisions, and data localization obligations. Indonesia's Ministry of Communication and Informatics (MOCI), though in agreement with the ADM, is reluctant to endorse cross-border data flow practices due to its concern over citizens' personal data protection (MOCI, 2021). Similarly, Vietnam supports a data localization policy in its Law on Cybersecurity (2018)[7] and is in the process of formulating a draft decree which includes the implementation guidelines on data localization (DLA Piper, 2021a). Unsurprisingly, both countries fall short in data classification.

[5] See the draft of Indonesia's Personal Data Protection Bill
[6] See Article 16 of Law on Network Information Security (2015)
[7] See Article 26 paragraph (3) of Law on Cybersecurity (2018) Vietnam

These shortcomings will hamper the region's digital economic growth and may even limit potential opportunities if states with relatively more robust data protection regulations refuse to conduct data transfer to states that do not possess equivalent or higher standards than their own (Disini, 2018; Chia, 2018; Munir 2018; ABLI, 2020).

While neither Indonesia nor Vietnam possess consolidated personal data protection regulations, a bill and a decree on PDP are currently being discussed in Indonesia and Vietnam, respectively.

Vietnam's regulations also fall short of ADM and ASEAN PDP principles and do not possess an adequate data protection mechanism. In the principles of consent, for instance, explicit consent from the data subject is only required in the collection stage of personal data but not in other stages of the data cycle (DLA Piper, 2021a). Vietnam's regulations also fail to fulfill the "access and correction," "accuracy of personal data," and "transfer to another country or territory" principles provided by the ASEAN PDP as well as failing to fulfill most principles in ASEAN DDG.

MINIMIZING GOVERNANCE GAPS: DIGITAL INFRASTRUCTURE AND DATA PROTECTION AND GOVERNANCE

There are different ways that national or regional data regulations bring extraterritorial influence to other jurisdictions. The Philippines provides an example of how a close economic relationship with the EU shapes the country's PDPA as they strive to be in compliance with GDPR. Big technology companies could also play a central role—when the GDPR came into effect, Facebook responded by moving its non-European data out of GDPR jurisdictions. It later changed its position, endorsing GDPR principles and pushing for GDPR-like standards to its non-European consumers (Erie & Streinz, 2021, p.11).

Infrastructure development can also influence data regulations beyond national borders. Wider adoption of digital technology requires sufficient digital and non-digital infrastructure. Data centers, fiber-optic and/or undersea cables, base transceiver towers, routers, and antennas are all required for digital services to run smoothly. These physical components are often costly to build for and so in developing economies, foreign investment is often needed. As providers of critical infrastructure, investors can bargain with the host countries to allow for conditions such as policy change or reform to secure the investment.

"Infrastructure development can also influence data regulations beyond national borders. Wider adoption of digital technology requires sufficient digital and non-digital infrastructure."

The opportunity for large technology companies to shape policy is especially strong in the case of new technologies such as 5G that require specific technical and practical standards in both digital and non-digital infrastructure. When 5G developers export their research and development activities overseas, the standards required to undertake these activities are naturally bundled with the investment and host countries may need to make policy changes and to grant particular market access and operational freedom to enable the investment to take place (Erie & Streinz, 2021, p.16).

5G is the next generation of wireless infrastructure with new and improved capabilities, such as lower latency, higher capacity, and support for a larger number of connections (Brake, 2020). In short, it offers advanced connections where more Internet of Things (IoT) devices (and not just tablets and smartphones) can be connected (Brake, 2020). However, advanced connection is a double-edged sword that illustrates another challenge. Advanced connection promises superior digital service with higher internet speed and integrated AI systems, but may compromise user privacy. On the one hand, as 5G could connect various devices and IoT–personal smartphones, smart home appliances, and even self-driving vehicles–all at once, citizens' lives are more connected to the internet than ever. On the other hand, concern has been raised about surveillance of citizens, especially in the development of smart cities (Erie & Streinz, 2021, p.28). In this case, although digital infrastructure regulation is important, it may not be sufficient to ensure adequate protection for the data that are being used and transferred across different tools and platforms. (EIT Digital, 2021). Robust data protection and data governance are required to ensure that the delivery of advanced connection does not come at the cost of consumer privacy.

5G investments are thriving in Southeast Asia. Leading players in 5G infrastructure in the region are Huawei & ZTE, Ericsson, Nokia, and Ooredoo (ASEAN Secretariat & UNCTAD, 2021). As of 2020, Chinese (Huawei and ZTE) and European (Ericsson and Nokia) players dominate the region's 5G infrastructure market (Martinus, 2020).

There is growing public concern surrounding a lack of trust in Chinese companies. Espionage allegations were made against Huawei in the Philippines but no wrongdoing was proven (Martinus, 2020). Despite these concerns, China remains a significant presence in regional digital infrastructure, as shown by a stable inflow of Chinese foreign direct investment (FDI) into ASEAN (Table 3), stable commercial capital inflow, and increasing interest from Chinese companies in the region (Table 4).

Table 3.
FDI Inflow by Source Country in the Information and Communication Sector in million US$[8]

No	Source Country	2015	2016	2017	2018	2019	2020
1	China	163.90	185.65	149.43	2,135.39	229.77	210.42
2	EU	1,768.31	-460.44	0.00	3,300.05	-370.49	259.20
3	United States	110.39	-404.43	1,348.36	44.85	278.89	634.24

Source: (ASEANStats)

[8] According to the OECD, FDI inflow can be negative because of disinvestment; the direct investor pays off loans from the investment enterprise, or if the reinvestment earnings are negative. ASEANStats do not provide data on each state's FDI inflow, therefore it is difficult to determine which state(s) contribute to this negative. However, from the table we can observe that FDI inflow from China never suffers from the negative FDI.

Table 4.
Major Chinese Private Companies in ASEAN

No	Company	Industry/Deal Type	Product	Recipients/Signatories	Countries
1	Alibaba Group	E-commerce, e-finance, cloud computing	Aliexpress, Aliyun, UC browser, Alipay	USD 1 billion for 51% stake in Lazada Group	Singapore
				USD 206 million for undisclosed equity stake in Singpost	
				USD 22 million for undisclosed stake in M-daq	
				20% stake of Ascend Money (sum undisclosed)	Thailand
				Joint Venture with Emtek (Sum Undisclosed)	Indonesia
2	Huawei	Services	CloudAIR 2.0 Solution	Investing in Telkomsel (sum undisclosed)	Indonesia
		Infrastructure & Services	MoU to develop Cloud, 5G, and AI	In cooperation with Indonesia Agency for the Assessment and Application of Technology	
		Infrastructure	DANAWA Malaysia Smart Modular Data Center	DANAWA Malaysia (sum undisclosed)	Malaysia
		Infrastructure	Prime Minister's Department Malaysia smart modular data center	Malaysia Department of the Prime Minister	
		Infrastructure	Huawei Eastern Economic Corridor Data Center (first)	Thailand Ministry of Digital Economy and Society	Thailand
3	Jingdong	E-commerce	Jd.com	none	Indonesia

excerpt from (Lewis, 2019) and (CSIS, 2021). Compiled by the author.

While authoritarian regimes such as the Russian Federation and People's Republic of China have been associated with corrosive investments, it does not follow that all investments from these countries are inherently corrosive.

The Center for International Private Enterprise [CIPE] (n.d.) outlines the characteristics of what they termed "constructive capital" and "corrosive capital." Constructive capital refers to flows of investment backed by transparent and market-oriented objectives both at the origin and destination of the funds. The word "constructive" emphasizes that when such capital is attracted it generates positive spill-over effects. Constructive capital can spur a cycle of good quality investments in the community and encourage good governance practices (Hontz, 2019).

Corrosive capital refers to flows of investment with vague motives that are often not transparent, politically driven, and sourced from authoritarian regimes into new or transitioning economies with the aim of influencing the recipient economy (Morrell et al., 2018). An originator of corrosive capital could use their financial power to influence a recipient country for the investor's own economic, social, or political agenda instead of the recipient country's best interests (James, 1930).

Because investments can direct policy, host countries, especially those without robust data regulations, must be cautious of corrosive investment capital. In policy formulation and objectives, the dilemma between enabling market-oriented or social benefit centered policy formulation is inherent, especially when regulating the digital economy (EIT Digital, 2021). Due to the complex relationships involved, such as between public and private sectors, and the rapid development of technology, regulations on digital issues may result in over-regulation or under-regulation, both of which are bad for data-driven innovations (EIT Digital, 2021). Governance gaps, including in the digital sector, create vulnerabilities to corrosive capital. There is growing corrosive capital investment in the ASEAN region that exploits such regulatory gaps. Some examples include payday lending through fintech in Indonesia and online gambling in the Philippines (Hanemann & Seiden, 2020; Suleiman et al., 2019).

> "In the case of digital data governance and digital infrastructure, corrosive investments may exploit governance gaps by promoting data localization."

In the case of digital data governance and digital infrastructure, corrosive investments may exploit governance gaps by promoting data localization (Erie & Streinz, 2021, pp.7-8). Data localization is usually politically popular. In ASEAN, states with data localization often do not possess adequate data protection and data governance regulations (as in Indonesia and Vietnam). Citizens are led to believe that their data is safe so long as it stays within their borders, and so fail to address data protection in transfers within the country, where their data may be collected, processed, and used without sufficient protection (Cheney, 2019, p.5; pp.18-19).

Although ADM is supportive of digital infrastructure development, it lacks guiding documents for digital infrastructure investments. Digital infrastructure investments are discussed in Desired Outcome 2–"Increase in the quality and coverage of fixed and mobile broadband infrastructure"–but none of the enabling actions mention the relationship between digital infrastructure and data protection and governance. Enabling Action 2.1–"Encourage inward investment in Digital and ICT"–endorses investments between ASEAN Member States, but it does not detail the mechanisms to differentiate between constructive and corrosive investment. Neither does it provide guidelines for preventing investment inflows that may be harmful to the development of adequate legal and regulatory protections for digital consumers. Overall, the focus on the digital infrastructure issues in Desired Outcome 2 is limited to fostering wider adoption of digital technology or digital transformation, not on promoting best practices for securing trusted digital infrastructure investment.

Further, although the ASEAN DDG mandates storage centres, platforms, and systems that manage data to take technical, procedural and physical measures, mitigate security risks and to ensure the confidentiality, integrity and availability of any data in their possession, common guidelines on these measures are yet to be developed. Therefore, dialogues and knowledge sharing between private and public organizations between ASEAN Member States on this matter are encouraged. This is all while also encouraging compliance with general principles for data transfer in the ASEAN PDP to safeguard consumer data during data collection and processing.

CONCLUSION AND RECOMMENDATION

Conclusion

Regulatory and governance gaps in and variance between regulations and governance across ASEAN Member States on the subject of data protection may increase the risk of corrosive capital inflow to the region as well as complicate data flow between member states. ADM can bridge these gaps by encouraging ASEAN Member States to adopt robust data protection policies on a national level and to harmonize these policies at the regional level. However, since it is not legally binding, ASEAN also uses other documents with stronger enforcement mechanisms such as the ASEAN Model Contractual Clauses, which aims for a safe cross-border data transfer in the region.

The identified governance gaps are the tendency to data localization among ASEAN Member States and the lack of a regional regulatory framework on digital infrastructure investment. These gaps must be eliminated.

Recommendations

Corrosive investment may exploit governance gaps in ASEAN Member States, especially those without robust personal data protection and data governance regulations. To address this problem, the ASEAN Secretariat should:

a. **Include the issue of digital infrastructure investment and its effects on data protection and data governance in the agendas of major ASEAN sectoral bodies and/or meetings.**
   There is an apparent lack of awareness about the potentially harmful relationship between the need for investment to develop digital infrastructure and the laws and regulations governing personal data protection in the region. By neglecting this relationship, ASEAN Member States may be exposed to corrosive investment as they develop their digital economy. The ASEAN secretariat needs to increase the awareness of this issue, especially among high-ranking officials, to create necessary agenda-setting for the next ASEAN Digital Ministries Meeting or other sectoral bodies or committees to address this gap.

b. **Formulate a regulatory framework and guiding document on digital and non-digital infrastructure investment.**
   Improving both digital and non-digital infrastructure is vital to developing the region's digital economy. In addition to providing best practices and an overview of each state's data regulation, this guiding document should present the possible harms from digital infrastructure investment when states lack adequate data protection and governance regulations. This regulatory framework and guiding documents should also provide a practical, risk-based analysis tool for ASEAN Member States that wish to engage with foreign entities to develop their digital infrastructure.

REFERENCES

APEC. (n.d.). APEC Cross Border Privacy Rules System Policies Rules and Guidelines.

Asian Business Law Institute. (2020). Transferring Personal Data in Asia: a Path to Legal Certainty and Regional Convergence.

Brake, D. (2020). Report: A U.S. National Strategy for 5G and Future Wireless Innovation.

Brewer, C. (2017). All Eyes on Malaysia for The Next E-commerce Boom. https://

logisticsofthings.dhl/article/all-eyes-malaysia-next-e-commerce-boom

Center for International Private Enterprise. (2018). Channeling the Tide: Protecting Democracies Amid A Flood of Corrosive Capital.

Chen, Y. (2020). Improving Market Performance in the Digital Economy. *China Economic Review*, 62, 1-8.

Cheney, C. (2019). China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism. *Issues & Insights Working Paper*, 19 (8).

Data Guidance. (n.d.). Comparing Privacy Laws: GDPR v. Singapore's PDPA.

Data Guidance. (n.d.). Comparing Privacy Laws: GDPR v. Thai Personal Data Protection Act.

Data Guidance. (2021, June). *Malaysia – Data protection Overview*. Accessed on September 15, 2021. https://www.dataguidance.com/notes/malaysia-data-protection-overview

Disini, J.J. (2018). Jurisdiction Report: Republic of the Philippines. *Regulation of Cross Border Data Transfer of Personal Data in Asia*. Asian Business Law Institute, 278-314.

DLA Piper. (2021a). Data Protection Laws of The World, Vietnam.

DLA Piper. (2020). Data Protection Laws of The World, Malaysia.

DLA Piper. (2020). Data Protection Laws of The World, Vietnam.

Duncan, D. (2018). Jurisdictional Report: Kingdom of Thailand. *Regulation of Cross Border Data Transfer of Personal Data in Asia*. Asian Business Law Institute, 383-393

Erie, M.S. & Streinz, T. (2021). The Beijing Effect: China's Digital Silk Road As Transnational Data Governance. *New York University Journal of International Law and Politics (forthcoming)*.

EIT Digital. (2021). Report: European Digital Infrastructure and Data Sovereignty, A Policy Perspectives.

Google, Temasek Foundation & Bain & Company. (2020). Report: economy SEA 2020, At full Velocity: Resilient and Racing Ahead

Hanemann, T. & Seiden, S. (2020). Chinese Investment in Southeast Asia: Making Sense of Data. In A Study of Chinese Capital Flows to Six Countries: Overview, Mitigating Governance Risks from Investment in Southeast Asia. Center for International Private Enterprise.

Hemming, J. (2020). Reconstructing Order: The Geopolitical Risks in China's Digital Silk Road. Asia Policy 15 (1), 5-21.

Hontz, E. (2019). *Building a market for everyone: How emerging markets can attract constructive capital and foster inclusive growth. Center for International Private Enterprise (CIPE)*. https://www.cipe.org/newsroom/building-a-market-for-everyone-how-emerging-markets-can-attract-constructive-capital-and-foster-inclusive-growth/

Human Rights Watch. (2021, March). *Myanmar: Facial Recognition System Threatens Rights Camera Surveillance, Mass Data Collection Bolsters Abusive Junta*. https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights

Ismail, N. A. & Masud, M.M. (2020). Prospects and Challenges in Improving E-Commerce Connectivity in Malaysia. In L. Chen & F. Kimura (Eds). E-Commerce Connectivity in ASEAN (pp.78-98)

James, F. C. (1930). Benefits and dangers of foreign investments. *The Annals of the American Academy of Political and Social Science*, 150, 76–84. http://www.jstor.org/stable/1017061

Jia Hao, C. & Rawat, D. (2019). China's Digital Silk Road: The Integration of Myanmar. RSIS Commentary.

Kateifides, A., Potter, A., Highams, H., Young, A., Kazmi, T., Campbell, C., Ashcroft, V., Campbell, K., Kerpauskaite, K., Dampster, E., Filis, A., Formichella, J.P., Jamallsawat, N., McNair, B., & Brikshari, A. (2019). *Report: Comparing Privacy Laws: GDPR v. Thai Personal Data Protection Act*.

Kearney. (2020). Report: The ASEAN Digital Revolution.

Ken, C. (2018). Jurisdictional Report: Singapore. *Regulation of Cross Border Data Transfer of Personal Data in Asia*. Asian Business Law Institute, 315-342

Kendall-Taylor, A., Frantz, E., & Wright, J. (2020). The Digital Dictators How Technology Strengthen Autocracy. Foreign Affair 99 (103), 103.

Kennedy, G., Doyle, S., Lui, B. (2009). Data Protection in the Asia Pacific Region. *Computer & Law Security Review* 25, 59-68.

Khatri, V & Brown, C.V. (2010). Designing Data Governance. *Communication of the ACM*, 53 (1), 148-152. doi: 10.1145/1629175.1629210

Laksanapanyakul, N. (2020). How Can E-marketplaces Turn Thailand into a Distributive Economy. In L. Chen & F. Kimura (Eds). *E-Commerce Connectivity in ASEAN* (pp.99-119)

Lewis, D. (2017). China's Global Ambitions: Finding Roots in ASEAN. *Occasional Paper. Institute of Chinese Studies*, Delhi

Lodean, N.N. (2016). The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law. *Journal of Internet Law* 19 (8).

Martinus, M. (2020). The Intricacies of 5G Development in Southeast Asia. *ISEAS Yusof Ishak Institute, Perspectives* (130).

Microsoft. (2019). Microsoft Security Endpoint Threat Report 2019.

Ministry of Communication and Informatics. (n.d.) Existing Regulations Regarding Personal Data Protection in Indonesia [infographic].

Ministry of Communication and Informatics. (2021, January 21). *Temu Kementerian Digital se-ASEAN, Indonesia Tekankan PDP di ADGSOM*. https://aptika.kominfo.go.id/2021/01/temu-kementerian-digital-se-asean-indonesia-tekankan-pdp-di-adgsom/

Ministry of Communications and Information Singapore. (2021, January 21). *1st ASEAN Digital Ministers' Meeting approves Singapore-led initiatives on ASEAN Data Management Framework, ASEAN Model Contractual Clauses for Cross Border Data Flows and ASEAN CERT Information Exchange Mechanism*. https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2021/1/1st-asean-digital-ministers-meeting

Munir, A.B. (2018). Jurisdictional Report: Malaysia. *Regulation of Cross Border Data Transfer of Personal Data in Asia*. Asian Business Law Institute, 215-246

Naughton, B. (2020). Chinese Industrial Policy and The Digital Silk Road: The Case of Alibaba in Malaysia. Asia Policy 15 (1), 23-39. Noor Sureani, N., Awis Qurni, A. S., Azman, A. H., Othman, M.B., & Zahari, H.S. (2021). The Adequacy of Data Protection Laws in Protecting Personal Data in Malaysia. *Malaysian Journal of Sciences and Humanities (MJSSH)*, 6 (10). https://doi.org/10.47405/mjssh.v6i10.1087

OECD. (2019). Enhancing Access to and Sharing of Data, Reconciling Risks and Benefits for Data Re-Use across Societies. https://doi.org/10.1787/276aaca8-en

OECD. (2019a). Going Digital: Shaping Policies, Improving Lives. https://doi.org/10.1787/9789264312012-en.

OECD. (n.d.). Foreign Direct Investment Statistics, Explanatory Notes.

Paul, T., Allison, K., Brown, C., & Broderick, K. (2020). The Digital Silk Road: Expanding China's Digital Footprint. Eurasia Group.

Privacy Law & Business. (2019). Data Protection & Privacy Information Worldwide. *International Report* (161).

Riyadi, G. A. (2021). Data Privacy in the Indonesia Personal Data Protection Legislation. *Center for Indonesian Policy Studies Policy Brief Series*.

Schwaizer-Chaput, A. (2021, June 8). *Independent data protection authority matters*. The Jakarta Post. https://www.thejakartapost.com/academia/2021/06/08/independent-data-protection-authority-matters.html

Shahbaz, A. (2018). The Rise of Digital Authoritarianism, Fake News, Data Collection, and The Challenge to Democracy. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Stalla-Bourdillon, S., Thuermer, G., Walker, J., Carmichael, L., & Simperl, E. (2020). Data Protection by Design: Building the Foundations of Trustworthy Data Sharing. Data & Policy 2 (4), 1-40. 10.1017/dap.2020.1

Suleiman, A., Kosijungan, P. A., & Octania, G. (2019). Chinese Investment in Indonesia's Fintech Sector: Their interaction with Indonesia's Evolving Regulatory Governance.

Tai Dong, Z. & Qi, X. (2019). The Digital Silk Road and Southeast Asian Countries. In A. Mulakala (Ed). *The Fourth Industrial Revolution and The Future of Work. KDI School of Public Policy and Management & The Asia Foundation*. 132-163

Voss, W.G. (2020). Cross Border Data Flows, the GDPR, and Data Governance. *Washington International Law Journal 29* (3), 485-532.

World Bank. (2019). Report: The Digital Economy in Southeast Asia: Strengthening the Foundations for the Future Growth.

Yayboke, E. & Brannen, S. (2020). Promote and Build A Strategic Approach to Digital Authoritarianism. Center for Strategic and International Studies.

Yu, P.K. (2010). The Political Economy of Data Protection. *Chi Kent Law Review*, 84 777-801.

ABOUT THE AUTHOR

Sri Handayani Nasution or Bolby graduated with a bachelor's degree from the Faculty of Social and Political Sciences at Universitas Gadjah Mada in Yogyakarta. When she began her career in a think tank of her university she specialized on matters regarding the digital sphere. After successfully finishing the CIPS Emerging Policy Leaders Program (EPLP) 2021, she joined the CIPS research team with a focus on digital rights and the digital economy.

JOIN OUR SUPPORTERS CIRCLES

Through our Supporters Circles, you, alongside hundreds of others, enable us to conduct our policy research and advocacy work to bring greater prosperity to millions in Indonesia.

Those in our Supporters Circles get the opportunity to engage in the work of CIPS on a deeper level. Supporters enjoy:

- Invitation to CIPS' annual Gala Dinner
- Exclusive Supporters-only briefings by CIPS leadership
- Priority booking at CIPS-hosted events
- Personal (Monthly/Quarterly) Supporters-only update emails and videos
- Free hard copy of any CIPS publication upon request

For more info, please contact anthea.haryoko@cips-indonesia.org.

Scan to join

ABOUT THE CENTER FOR INDONESIAN POLICY STUDIES

Center for Indonesian Policy Studies (CIPS) is a strictly non-partisan and non-profit think tank providing policy analysis and practical policy recommendations to decision-makers within Indonesia's legislative and executive branches of government.

CIPS promotes social and economic reforms that are based on the belief that only civil, political, and economic freedom allows Indonesia to prosper. We are financially supported by donors and philanthropists who appreciate the independence of our analysis.

KEY FOCUS AREAS:

Food Security & Agriculture: To enable low-income Indonesian consumers to access more affordable and quality staple food items, CIPS advocates for policies that break down the barriers for the private sector to openly operate in the food and agriculture sector.

Education Policy: The future of Indonesia's human capital need to be prepared with skills and knowledge relevant to the 21st century. CIPS advocates for policies that drive a climate of healthy competition amongst education providers. Such competition will drive providers to constantly strive to innovate and improve education quality for the children and parents they serve. In particular, CIPS focuses on the improvement of operational and financial sustainability of low-cost private schools who serve the poor.

Community Livelihood: CIPS believes that strong communities provide a nurturing environment for individuals and their families. They must have the rights and capacities to own and manage their local resources and to ensure healthy and sound living conditions for the development and prosperity of the community.

www.cips-indonesia.org

facebook.com/cips.indonesia
@cips_id
@cips_id
Center for Indonesian Policy Studies
Center for Indonesian Policy Studies

Jalan Terogong Raya No. 6B
Cilandak, Jakarta Selatan 12430
Indonesia