THE CHALLENGE OF HARMONIZING CROSS-BORDER DATA TRANSFER REGULATIONS AMONG ASEAN MEMBER STATES

Jessica Aurelia, Faculty of Law, Tarumanagara University,
e-mail: jessica.205210096@stu.untar.ac.id
Lewiandy, Faculty of Law, Tarumanagara University,
e-mail: lewiandy@fh.untar.ac.id

doi: https://doi.org/10.24843/KS.2025.v13.i03.p01

ABSTRAK

Penelitian ini mengkaji regulasi transfer data lintas batas antar negara anggota ASEAN dan menganalisis tantangan dalam mengimplementasikan ASEAN Model Contractual Clauses (MCCs). Melalui penelitian hukum normatif dan analisis komparatif, studi ini mengungkapkan adanya perbedaan signifikan dalam kerangka perlindungan data di negara-negara ASEAN. Sementara negara-negara seperti Malaysia, Singapura, dan Filipina telah menetapkan undang-undang perlindungan data yang komprehensif, negara lain masih mengandalkan regulasi sektor-spesifik atau sama sekali tidak memiliki kerangka hukum khusus. Penelitian ini mengidentifikasi tiga tantangan utama yang menghambat implementasi efektif ASEAN MCCs: tidak adanya undang-undang privasi data yang seragam antar negara anggota, kurangnya mandat hukum dan mekanisme penegakan, serta standar perlindungan data yang relatif lemah dibandingkan dengan kerangka global seperti GDPR. Penemuan ini menekankan perlunya koordinasi regional yang lebih kuat dan harmonisasi standar perlindungan data untuk memfasilitasi transfer data lintas batas yang aman dan mendorong pertumbuhan ekonomi digital di ASEAN.

Kata Kunci: Transfer Data Lintas Batas, ASEAN MCCs, Harmonisasi Regulasi

ABSTRACT

This research examines the cross-border data transfer regulations among ASEAN member states and analyzes the challenges in implementing the ASEAN Model Contractual Clauses (MCCs). Through normative legal research and comparative analysis, the study reveals significant disparities in data protection frameworks across ASEAN countries. While nations like Malaysia, Singapore, and the Philippines have established comprehensive data protection laws, others rely on sector-specific regulations or lack dedicated frameworks entirely. The research identifies three major challenges hindering the effective implementation of ASEAN MCCs: the absence of uniform data privacy laws across member states, the lack of legal mandate and enforcement mechanisms, and relatively weak data protection standards compared to global frameworks like the GDPR. These findings highlight the need for stronger regional coordination and harmonization of data protection standards to facilitate secure cross-border data transfers and promote digital economic growth within ASEAN.

Keywords: *Cross-Border Data Transfer, ASEAN MCCs, Regulatory Harmonization*

I. INTRODUCTION

1.1 Problem Background

In today's digital age, personal data has become an invaluable asset, often likened to the "new oil" or "digital currency" of the global economy.[1] Its value, however, is

[1] Georgios Yannopoulos, et. al., "Personal Data as the Currency of the Digital Age Having as an Example Art. 3 Par. 1 (and Preamble No. 24) of Directive 2019/770)", *Postgraduate Thesis National and Kapodistrian University of Athens* (2022), p. 12; Marc Van Lieshout, "The Value of Personal

matched by its vulnerability to exploitation, making the protection of personal data a critical issue for governments, businesses, and individuals alike. Numerous cases of data breaches, particularly those involving the misuse of personal information and subsequent criminal activities, underscore the pressing need for comprehensive data protection regulations. Personal data protection is fundamentally linked to the broader concept of privacy, and data leaks typically arise from two main sources: systemic negligence or malicious cyberattacks.[2] These challenges highlight the necessity of effective legal frameworks to safeguard personal information while upholding the right to privacy as a universal principle.[3]

In sectors such as e-commerce, the need for personal data protection is particularly pronounced. Activities like electronic fund transfers, inventory management, and data collection rely heavily on the exchange and storage of personal data, making them vulnerable to unauthorized access and misuse.[4] Effective personal data protection ensures that individuals retain control over their information, including determining who can access it, under what conditions, and for what purposes. This concept aligns with broader notions of confidentiality and privacy, which emphasize the right to restrict or disclose personal information based on the individual's preferences.[5]

The increasing importance of personal data in the digital economy is accompanied by significant risks, particularly in the context of cross-border data transfers. The management of personal data, while inherently an individual matter, becomes more complex when data flows across national boundaries.[6] These cross-border data transfers often involve multiple parties, including data controllers and international organizations, necessitating legal and institutional frameworks to govern their use. Unfortunately, there is no universal convention under the United Nations to regulate cross-border data flows, and the prospect of such a framework emerging in the near future remains unlikely.[7]

In response, regional initiatives have been developed to address these gaps. For instance, the European Union's General Data Protection Regulation (GDPR), the APEC Cross-Border Privacy Rules System, and the ASEAN Framework on Personal Data Protection aim to provide guidance on data protection practices.[8] Established in 2016, the ASEAN Framework on Personal Data Protection seeks to strengthen personal data

---

Data", *Conference Paper in IFIP Advances in Information and Communication Technology* (2015): 11-13.

[2] Gabriel Rodrigues, et. al. "Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review", *Data 2023*, Volume 9 Issue 2 (2023): 2.

[3] Oluwatosin Reis, et. al., "Privacy Law Challenges in the Digital Age: A Global Review of Legislation and Enforcement", *International Journal of Applied Research in Social Sciences*, Volume 6 Issue 1 (2024): 74.

[4] Rahmi Ayunda, "Personal Data Protection to E-Commerce Consumer: What are the Legal Challenges and Certainties?", *Law Reform*, Volume 18 Issue 2 (2022): 145.

[5] Merlita Yuli Safitri and Mahfud, "The ASEAN Cross-Border Personal Data Transfer Instrument: Has Indonesian's Personal Data Protection Law Followed it?", *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)* Volume 12 Number 3 (2023): 554.

[6] Lingjie Kong, "Data Protection and Transborder Data Flow in the European and Global Context", *European Journal of International Law*, Volume 21 Issue 2 (2010): 441-442.

[7] United Nations Capital Development Fund, "The Role of Cross-Border Data Flows in the Digital Economy", *Policy Accelerator* (2022): 4.

[8] GSMA, "Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation" (2018): 20.

protection across Southeast Asia while facilitating collaboration among member states to enhance trade and data flows.[9] However, the framework's non-binding nature raises questions about its effectiveness in creating a cohesive regional approach to data protection.

ASEAN member states face several challenges in achieving a harmonized personal data protection system.[10] While countries like Malaysia, Singapore, the Philippines, Laos, Thailand, and Indonesia have enacted dedicated personal data protection laws, others continue to rely on sector-specific regulations. Cambodia, for example, addresses data protection through laws governing telecommunications and e-commerce, while Vietnam employs a fragmented approach across various domains, including civil law and cyber information security.[11] These disparities in legal frameworks create inconsistencies in data security practices and complicate the seamless transfer of data across borders.

Despite these differences, there is a growing recognition within ASEAN of the need for a compatible personal data protection system to address emerging risks such as cybercrime and to promote regional economic integration. In response, ASEAN has introduced the ASEAN Model Contractual Clauses (ASEAN MCCs) as a framework for facilitating cross-border data transfers. However, challenges remain in its implementation due to the lack of harmonization among member states' legal frameworks. Therefore, this paper delves into a comparative analysis of cross-border data transfer regulations among ASEAN member states, examining the obstacles posed by regulatory disparities and exploring potential pathways for aligning personal data protection standards.

1.2 Research Problem

1. What are the key features and frameworks of cross-border data transfer regulations among ASEAN member states?
2. What are the challenges of implementing the ASEAN MCCs amidst the lack of harmonization in cross-border data transfer regulations among ASEAN member states?

1.3 Purpose of Writing

1. To identify the key features and frameworks of cross-border data transfer regulations among ASEAN member states.
2. To analyze the challenges of implementing the ASEAN MCCs amidst the lack of harmonization in cross-border data transfer regulations among ASEAN member states.

2. METHOD

The research adopts a normative legal research approach, focusing on the analysis and interpretation of legal norms, including legislation, books, previous studies,

[9] ASEAN Framework on Personal Data Protection (2022).

[10] Salsabila Siliwangi Surtiwa and Christian Jeremia Gultom, "ASEAN for Data Protection: Remarks on 2016 ASEAN Framework on Personal Data Protection and the Impact Towards Regional Peer to Peer Lending", *Atlantis Press: Advances in Social Sciences, Education and Humanities Research*, Volume 558 (2021): 720.

[11] Drew Network Asia, "DNA ASEAN Guide to: Data Protection and Cybersecurity Regulation in Southeast Asia" (2024): 5-7.

scientific articles, journals, and other credible literature related to cross-border data transfer regulations.[12] This study also employs a comparative approach by examining laws and regulations relevant to the topic across ASEAN member states. The research analyzes legal issues using legislative texts, scholarly literature, and other reference materials. Data collection is conducted through a library study, a method commonly used in normative legal research, by reading, quoting, and analyzing laws, regulations, and related materials to provide a comprehensive understanding of cross-border data transfer regulations and their alignment within ASEAN.[13]

3. RESULTS AND DISCUSSION

3.1 Cross-border data transfer regulations among ASEAN member states

Southeast Asia is a vibrant and diverse region that is home to more than 680 million people, spread across 10 nations: Brunei Darussalam, Cambodia, Indonesia, Lao People's Democratic Republic, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam. Of these, all but Timor-Leste are members of ASEAN, a regional organization dedicated to fostering economic growth, social progress, cultural exchange, and regional stability. Timor-Leste is currently on the path to becoming ASEAN's eleventh member, following an agreement in principle by existing member states in November 2022.[14]

Geographically, Southeast Asia stretches over 5,000 kilometers from east to west, covering an area of more than 4.5 million square kilometers. This expanse is home to the world's two largest archipelagic nations, Indonesia and the Philippines, alongside one of the smallest sovereign states, Singapore. Each Southeast Asian country has unique cultural and social characteristics, though shared influences often blur borders, creating a rich tapestry of interconnected traditions and customs across the region.[15]

In recent years, data protection and cybersecurity have gained prominence among ASEAN member states. Prior to 2010, the region lacked comprehensive data protection laws. However, significant progress has been made in the past decade.[16] Malaysia, the Philippines, and Singapore were the first to introduce general data protection laws in the early 2010s, paving the way for other nations. Subsequent years saw the introduction of similar laws in Laos (focusing on electronic data), Thailand, Indonesia, and Vietnam between 2017 and 2023.

Countries like Brunei Darussalam and Cambodia have also initiated steps toward enacting comprehensive data protection regulations, conducting public consultations on proposed frameworks. Meanwhile, others, including Cambodia and Myanmar, have implemented sector-specific rules, particularly in e-commerce. These developments underscore the growing importance of harmonized data protection

---

[12] Efendi, Jonaedi dan Ibrahim, Johny. *Metode Penelitian Hukum: Normatif dan Empiris* (Depok, Prenada Media Group, 2018), 132-136.

[13] Sigit Sapto Nugroho, et. al. *Metodologi Riset Hukum*, (Surakarta: Oase Pustaka, 2020), 93.

[14] Drew Network Asia, "DNA ASEAN Guide to: Data Protection and Cybersecurity Regulation in Southeast Asia" (2024): 5.

[15] Michael G. Plummer, et. al. *Connecting Asia: Infrastructure for Integrating South and Southeast Asia*, (Northampton: Edward Elgar Publishing, 2016), 71.

[16] Syafri Haariansah, et. al., "Personal Data Protection in ASEAN: Indonesia's Role in Developing ASEAN's Personal Data Protection Legal Framework", *Novateur Publication India, Proceedings of International Seminar on Indonesian Lecturer is Born to Report Regularly* (2023): 455.

measures across ASEAN to address the complexities of cross-border data transfers in today's digital economy.[17]

Table 1. Comparison of each ASEAN member states handles cross border data transfers.

Country	Comprehensive Data Protection Law	Sector-Specific Regulations	Cross-Border Transfer Restrictions	Key Authority
Brunei	No (PDPO under development)	Yes (telecom sector)	Expected under PDPO	Authority for Info-communications Technology Industry (AITI)
Cambodia	No (draft in progress)	Yes (e-commerce, banking laws)	Not explicitly regulated	Ministry of Post and Telecommunication (MPTC)
Indonesia	Yes (PDP Law)	Yes (banking sector)	MOCI notification and reporting required	Ministry of Communications and Informatics (MOCI)
Laos	No (focused on electronic data)	Yes (cybercrime, e-commerce laws)	Not explicitly regulated	Ministry of Technology and Communications
Malaysia	Yes (PDPA)	Yes (sector-specific banking laws)	Allowed only to White List countries with consent/contract	Department of Personal Data Protection (JPDP)
Myanmar	No (laws on telecom, privacy)	Yes (financial, electronic transactions laws)	Not explicitly regulated	Ministry of Transport and Communications
Philippines	Yes (Data Privacy Act)	Yes (banking sectors)	Controllers liable for cross-border data transfers	National Privacy Commission (NPC)
Singapore	Yes (PDPA)	Yes (telecom, financial sectors)	Transfers allowed only with compliance to Singaporean standards	Personal Data Protection Commission (PDPC)
Thailand	Yes (PDPA)	Yes (sector-specific rules apply)	Allowed if destination country meets adequacy standards	Personal Data Protection Commission

[17] Prapanpong Khumon, "Cross-Border Data Privacy Regulation in ASEAN: Overcoming Institutional Challenge", *Research Paper of University of the Thai Chamber of Commerce* (2020): 8.

Vietnam	No (sectoral laws apply)	Yes (telecom, banking, e-commerce)	Banking data requires encryption and consent	Ministry of Information and Communications

3.1.1 Brunei Darussalam

Currently, Brunei does not have a general data protection law. In May 2021, the Authority for Info-communications Technology Industry (AITI) issued a public consultation paper proposing a framework for personal data protection in the private sector. Following this, AITI released a response to public feedback in December 2021 and has since conducted industry engagement sessions. A new law, the Personal Data Protection Order (PDPO), is anticipated to be enacted later this year. Key requirements of the PDPO are expected to align with AITI's proposals in the consultation paper and response, although the final provisions will only be confirmed upon the law's enactment.

In addition to a general data protection law, there are sector-specific frameworks that include personal data protection measures, albeit with a narrower scope of obligations. For instance, in the telecommunications sector, end-user subscriber information (EUSI) is protected under the Code of Practice for Competition in the Telecommunications Sector (Competition Code), issued by AITI under the Telecommunications Order, 2001. EUSI encompasses details such as a user's billing name, identification number, address, telephone number, IP address, location data, and usage patterns. The Competition Code prohibits telecommunications entities (referred to as "Market Players") from using or disclosing EUSI, except for purposes outlined in the code or with the explicit consent of the end-user.

3.1.2 Cambodia

Cambodia has not yet implemented comprehensive cybersecurity or data protection laws. In 2021, the Ministry of Post and Telecommunication (MPTC) announced plans to draft a Personal Data Protection Law following the completion of the draft Cybersecurity Law. However, as of mid-June 2024, both drafts remain under discussion and development.

Currently, data protection and privacy issues are broadly addressed through the constitutional right to privacy and provisions in the Civil Code, Criminal Code, and specific laws such as the Law on Electronic Commerce (E-commerce Law) and the Law on Banking and Financial Institutions. These laws generally safeguard the right to privacy, which may extend to the protection of personal data.

3.1.3 Indonesia

The main law governing personal data protection in Indonesia is Law No. 27 of 2022 on Protection of Personal Data ("PDP Law"), which was enacted on 17 October 2022. A draft bill on the Protection of Private Personal Data is under discussion but has not yet been enacted. Meanwhile, existing regulations, such as Regulation 82 on electronic systems and transactions and the Ministry of Communications and Informatics (MOCI) Regulation on personal data protection in electronic systems, mandate that overseas personal data transfers be handled by electronic system operators.[18] These operators are required to coordinate and report transfer details to MOCI and comply with laws

[18] Article 22 (1) of the Indonesia's Minister of Communications & Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System (MOCI Regulation).

governing cross-border data exchanges. Enforcement measures include fines and imprisonment for violations of data privacy or non-compliance with MOCI regulations. Authorities may also issue verbal or written warnings, temporarily suspend activities, or make public announcements on their website to ensure compliance. Additionally, Indonesia has a distinct data privacy regulation for the banking sector, requiring prior approval from Bank Indonesia for overseas transfers of bank customer data, as outlined in Bank Indonesia Regulation No. 9/15/PBI/2007 on Risk Management in the Use of Information Technology by Banks.

3.1.4 Laos

In Laos, the regulatory framework for data privacy primarily focuses on electronic data, with key laws and regulations governing cross-border data transactions and electronic data protection. These include the Law on Electronic Transactions (2012), the Law on Cyber Crime (2015), the Decision on the Penalties of the Law on Cyber Crime (2017), the Law on Electronic Data Protection (2017), the Penal Code (2017), and the Instructions on the Implementation of the Law on Cyber Crime and the Law on Electronic Data Protection (both issued in 2018). Together, these laws and regulations provide guidelines and penalties to safeguard electronic data. Additionally, authorities have issued guidelines outlining best practices for using software, hardware, and social media platforms to enhance electronic data protection. Among these, the primary regulations for data privacy in Laos are the Law on Electronic Data Protection and its implementing instructions.

3.1.5 Malaysia

The Personal Data Protection Act 2010 (PDPA) restricts cross-border data transfers unless the destination country has been approved by the Minister of Information, Culture, and Communications (MIC) as having an adequate level of protection comparable to Malaysian law.[19] The Public Consultation Paper No. 1/2017 on the Personal Data Protection (Transfer of Personal Data to Places Outside Malaysia) Order 2017 introduced a proposed "White List," allowing data transfers to specific countries.

Regardless of inclusion on the White List, cross-border data transfers may still be permitted under specific conditions, such as obtaining the data owner's consent, the necessity of the transfer for contract performance, legal proceedings, obtaining legal advice, defending legal rights, or protecting the vital interests of the data subject. Additionally, transfers are allowed if the data user has taken reasonable steps and exercised due diligence to ensure compliance with the PDPA.[20] Non-compliance with the PDPA results in criminal liability, with penalties including fines and imprisonment. Senior officials such as directors, CEOs, and managers may also face joint and several liabilities unless they can demonstrate a due diligence defense.[21]

3.1.6 Myanmar

The Telecommunications Law (2013) focuses primarily on the telecommunications sector, with limited provisions addressing cybersecurity. Its main objectives include protecting against cybercrimes involving telecommunications services and preventing unauthorized disclosure of information stored in secured or

[19] Section 129 (1) and (2) of Malaysia's Personal Data Protection Act 2010.
[20] Section 129 (3) of Malaysia's Personal Data Protection Act 2010.
[21] Sections 131-133 of the Malaysia's Personal Data Protection Act 2010.

encrypted systems to third parties. The Electronic Transactions Law (2004, amended in 2014 and 2021) facilitates electronic transactions and incorporates data protection and cybersecurity measures. It legally recognizes electronic records and signatures and enforces penalties for cybercrimes, including hacking and unauthorized data access.

The Law for Protection of Personal Privacy and Personal Security of Citizens aims to safeguard individual privacy and personal security. It grants several rights, such as the right to personal privacy free from unauthorized surveillance, and requires consent before collecting or processing personal data. The law prohibits the unauthorized collection, use, or dissemination of personal data, with violations subject to penalties. However, since 2021, provisions related to unauthorized surveillance, consent for data collection and processing, and the prohibition of unauthorized data use have been suspended. In the financial sector, the Financial Institutions Law requires banks to maintain confidentiality of user information, including accounts, records, and transactions, ensuring robust data protection within the industry.

3.1.7 Philippines

The Data Privacy Act of 2012 (Republic Act No. 10173) established the National Privacy Commission to oversee security breaches and provide guidelines on security policies. Cross-border transfer of personal information is permitted, but the personal information controller remains accountable for any incidents involving the data under its control, subject to cross-border arrangements and cooperation.[22] However, transferring sensitive personal information to third parties, whether domestically or internationally, is prohibited.[23]

The Act enforces compliance through criminal and monetary penalties. Under Section 21, the principle of accountability holds data controllers responsible for ensuring that personal data transferred to third parties for processing, whether within or outside the country, complies with the Act. Data controllers must use contracts or other reasonable measures to ensure a comparable level of protection during processing and designate a responsible individual to ensure organizational compliance with the law.

In essence, data controllers bear the primary responsibility for safeguarding personal data, even when transferred across borders. They must ensure that such data is processed in line with the provisions of the Data Privacy Act. Any outsourcing, subcontracting, or data-sharing agreements facilitating cross-border data transfers must adhere to the Act's requirements. Additionally, Section 7 empowers the National Privacy Commission to negotiate and establish agreements with data privacy authorities from other countries to ensure the cross-border application and enforcement of privacy laws.

3.1.8 Singapore

The Personal Data Protection Act 2012 (No. 26 of 2012), under Article 26, prohibits transferring data outside Singapore unless the receiving organization ensures compliance with Singaporean privacy standards. The law outlines mechanisms for achieving this, requiring the receiving organization to be bound by legal obligations (such as contracts, data transfer agreements, or binding corporate rules) that provide comparable protection to Singaporean law. Data owners in Singapore can also consent to overseas data transfers. Cross-border data transfers are allowed when necessary for

[22] Chapter II of the Philippines' Data Privacy Act of 2012 (Republic Act No. 10173); Section 21 of the Philippines' Data Privacy Act of 2012 (Republic Act No. 10173).

[23] Chapter VIII of the Philippines' Data Privacy Act of 2012 (Republic Act No. 10173).

contract performance between the organization and the individual, provided certain conditions are met.[24]

The Personal Data Protection Commission of Singapore has issued guidance for organizations on cross-border transfers, including model clauses for data transfer agreements and a guide to data sharing, covering both intra-group and third-party sharing. For enforcement, the PDPC released the Advisory Guidelines on Enforcement of Data Protection Provisions in April 2016. These guidelines detail how the Commission handles complaints, reviews, and investigations of data protection breaches, as well as enforcement measures and sanctions. The guidelines also specify enforcement objectives and factors influencing decisions, such as prompt incident response, cooperation during investigations, and timely breach notification. Decisions or reconsiderations by the Commission can be appealed to a Data Protection Appeal Committee.

3.1.9 Thailand

Thailand's Personal Data Protection Act 2019, under Section 28, permits cross-border transfers of personal data to a third country only if the country has an adequate standard of personal data protection, as determined by the Personal Data Protection Commission. The adequacy of these standards is assessed by the Commission, and its decision may be reviewed if new evidence shows improvements in the destination country or international organization meeting the required standards. However, even without adequate approval, cross-border transfers are allowed in specific cases, such as when the data subject provides consent, the transfer is necessary for contract performance, or it is required for tasks carried out in the public interest. Thai law also enables cooperation with other jurisdictions. Section 44(9) grants the Commission the authority to establish agreements and collaborate with domestic or international organizations or agencies concerning the Office's tasks, subject to the Commission's approval.[25]

3.1.10 Vietnam

Vietnam does not have a single comprehensive data privacy regulation. However, individuals and organizations may transfer personal information abroad if they have obtained prior consent from the data owner. Sensitive data, such as banking information, must be encrypted before transfer and requires the data owner's consent.[26] For cross-border banking data transfers, a written agreement must outline the responsibilities of the parties involved, including terms and conditions, breach consequences, and compensation for any resulting loss or damage. The Ministry of Information and Communications oversees data privacy issues in the telecommunications, internet, and IT sectors, including complaint resolution and enforcement of violations. In the e-commerce sector, the Vietnam e-Commerce and Information Technology Authority under the Ministry of Industry and Trade handles data privacy violations, including issuing guidelines, licensing, monitoring, and regulating e-commerce activities. There is no general requirement to ensure that data

[24] Singapore's Personal Data Protection Act 2012.

[25] Thailand's Personal Data Protection Act 2019.

[26] Art 38 (2) of the Vietnam's Civil Code (No. 91/2015/QH13); Article 21 (1) of Vietnam's Law on Information Technology (No. 67/2006/QH11); Article 17 (1) of Vietnam's Law on Network Information Security (No. 86/2015/QH13).

exports meet comparable privacy standards or are governed by binding contracts, except in the case of banking data transfers, as specified.[27]

3.2 The challenges of implementing the ASEAN MCCs amidst the lack of harmonization in cross-border data transfer regulations among ASEAN member states

The rapid growth of ASEAN's digital economy has highlighted the need for a cohesive regulatory framework for cross-border data transfers.[28] However, the absence of harmonized data privacy laws among member states creates legal fragmentation, making compliance difficult for businesses, particularly SMEs. While some ASEAN countries enforce strict data localization laws, others adopt more flexible approaches, leading to inconsistencies that increase operational costs and regulatory uncertainty. Unlike the European Union's GDPR, ASEAN relies on voluntary frameworks like the ASEAN MCCs and the ASEAN Framework on Personal Data Protection, which lack binding enforcement.[29] This weak regulatory structure results in inconsistent implementation, discouraging investment and slowing digital economic growth. Moreover, the ASEAN MCCs adopt a limited scope, covering only controller-to-controller and controller-to-processor transfers, while excluding processor-initiated transfers, creating compliance gaps.[30]

Despite aiming to facilitate data transfers, the MCCs impose obligations that may exceed local legal requirements, leading to "over-compliance" issues. Additionally, weak data protection standards compared to global frameworks, such as the GDPR, raise concerns about cybersecurity risks and the adequacy of ASEAN's data governance. Without stronger institutional oversight, legal mandates, and enforcement mechanisms, ASEAN risks falling behind in the global digital economy. These challenges highlight the fundamental weaknesses in ASEAN's approach to cross-border data transfers. The lack of a unified regulatory framework results in inconsistencies that create legal uncertainty, compliance burdens, and barriers to digital trade. Three key issues hinder the effective implementation of the ASEAN MCCs:

3.2.1 Lack of uniform data privacy law across ASEAN

The ASEAN region, composed of ten diverse nations, faces significant challenges in establishing a unified data privacy framework. Each country has its own priorities, with some still emphasizing traditional security concerns over digital governance. This divergence has resulted in fragmented regulations on personal data protection, making cross-border data governance a complex issue. While a few countries have enacted comprehensive data protection laws, others continue to rely on sectoral regulations, creating inconsistencies in how data privacy is managed across the region.[31]

---

[27] Waewpen Piemwichai, "Jurisdictional Report: Socialist Republic of Vietnam", in *Regulation of Cross-border Transfers of Personal Data in Asia, A compendium of 14 reports by the Asian Business Law Institute*, ed. Asian Business Law Institute (2018).

[28] United Nations Development Programme (UNDP), Enabling Cross-Border Data Flow: ASEAN and Beyond, UNDP Global Centre (2021): 6-7.

[29] Jingting Liu, "Facilitating Data Flows Across ASEAN: Challenges and Policy Directions", Asia Competitiveness Institute Research Paper Series (2023): 9.

[30] ASEAN Model Contractual Clauses for Cross Border Data Flows (2021): 6.

[31] Merlita Yuli Safitri and Mahfud, "The ASEAN Cross-Border Personal Data Transfer Instrument: Has Indonesian's Personal Data Protection Law Followed it?", *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)* Volume 12 Number 3 (2023): 557.

Economic disparities further complicate the region's digital landscape. Singapore, as Southeast Asia's leading technology hub, relies heavily on IT across nearly all sectors, making it particularly vulnerable to cyberattacks that could disrupt essential infrastructure. In contrast, countries like Indonesia have lower levels of IT integration, reducing their exposure to cyber threats but also limiting their digital resilience. This uneven technological landscape further exacerbates the challenges of establishing a standardized approach to data privacy across ASEAN.[32]

Unlike the European Union, which has successfully implemented the GDPR to create a unified legal framework for data protection across its member states, ASEAN lacks a harmonized regulatory system. The GDPR ensures that all EU countries adhere to the same data privacy standards, fostering trust, facilitating cross-border data flows, and strengthening cybersecurity across the region. In contrast, ASEAN's fragmented approach makes it difficult to establish common safeguards, creating uncertainty for businesses and individuals operating across multiple jurisdictions. Without a cohesive framework, ASEAN countries risk falling behind in the global digital economy, as data protection and cybersecurity become increasingly critical for international trade, investment, and technological innovation.

The absence of a harmonized data protection framework not only hinders digital cooperation but also raises concerns about security, economic stability, and regional trust. As ASEAN moves towards deeper digital integration, addressing these regulatory gaps will be crucial in ensuring a secure, efficient, and cooperative digital ecosystem for the region. Learning from the EU's GDPR model could serve as a valuable reference point for ASEAN policymakers in their efforts to develop a more synchronized and effective data protection strategy.

3.2.2 No legal mandate or enforcement mechanism

Unlike the EU's Standard Contractual Clauses (SCCs), which are legally binding under the GDPR, ASEAN's MCCs lack a clear legal foundation, either in domestic legislation or through a regional treaty. No ASEAN member state has enacted laws explicitly stating that the use of MCCs ensures compliance with national data protection regulations. Instead, the MCCs are merely a voluntary standard, allowing modifications as long as they do not contradict the original framework. However, there are no defined consequences for deviations, making enforcement highly uncertain.[33]

Furthermore, the MCCs acknowledge that parties may adopt alternative data transfer mechanisms recognized within ASEAN, should such options exist. However, the only available mechanisms are those outlined in the national laws of individual ASEAN member states, further reinforcing the fragmented and inconsistent regulatory landscape. Without a legal mandate or enforcement mechanism, the effectiveness of ASEAN's MCCs remains uncertain, limiting their ability to facilitate secure and standardized cross-border data transfers within the region.[34]

3.2.3 Weak data protection standards compared to global frameworks

---

[32] J. Lee and M. Perone, "The Influx of Cybercrime Across Southeast Asia and the Cyber Security and Data Protection Measures That Are Being Placed to Bolster Security Within the Region" (2019).

[33] ASEAN Model Contractual Clauses for Cross Border Data Flows (2021): 4.

[34] Graham Greenleaf, "ASEAN Model Contractual Clauses: Low and Ambiguous Data Privacy Standards", *University of New South Wales Law Research Series* (2021): 1.

ASEAN's MCCs are based on outdated OECD (1980) and APEC (2004) principles, offering weaker data protection than global frameworks like the GDPR. While some ASEAN member states, such as Thailand, Indonesia, and Vietnam, have adopted stricter GDPR-inspired laws, the MCCs fail to reflect these advancements, creating inconsistencies between national and regional standards. Despite being designed for intra-ASEAN data flows, the MCCs allow transfers to non-ASEAN states with similarly weak privacy laws. The ASEAN Framework on Personal Data Protection adds minimal updates to older standards, requiring only that organizations obtain consent or take "reasonable steps" to protect transferred data. However, it does not mandate equivalent protection to the exporting country's law, weakening safeguards.[35]

Ironically, most ASEAN countries with data privacy laws follow GDPR principles rather than OECD guidelines, yet the MCCs still adhere to outdated models. While they introduce obligations like compliance with "applicable AMS law" and a Data Breach Notification requirement, these provisions lack clarity and enforceability. The MCCs also fail to regulate onward transfers, merely encouraging importers to conduct due diligence. This weak framework makes ASEAN's MCCs unlikely to align with GDPR standards, limiting their effectiveness in global data governance. For ASEAN to ensure a secure digital environment, stronger, enforceable regulations are essential.[36]

4. CONCLUSION

The analysis of cross-border data transfer regulations among ASEAN member states reveals a complex landscape characterized by varying levels of legislative development and enforcement. While some countries have enacted comprehensive data protection laws, others continue to operate under fragmented or sector-specific regulations, creating significant challenges for regional data governance. The implementation of ASEAN MCCs, while representing a step toward regional harmonization, faces substantial obstacles due to its voluntary nature and the absence of binding enforcement mechanisms.

The research identifies three critical challenges that must be addressed to strengthen ASEAN's data protection framework. First, the lack of uniform data privacy laws across member states creates regulatory inconsistencies that impede efficient cross-border data transfers. Second, the absence of legal mandate and enforcement mechanisms undermines the effectiveness of the ASEAN MCCs, reducing them to voluntary guidelines rather than enforceable standards. Third, the relatively weak data protection standards compared to global frameworks like the GDPR limit ASEAN's ability to participate fully in the global digital economy.

To address these challenges, ASEAN must prioritize the development of a more cohesive and comprehensive regional data protection framework. This could involve establishing minimum standards for data protection across member states, creating binding enforcement mechanisms, and updating the MCCs to align with contemporary global standards. Additionally, stronger institutional oversight and coordination among member states will be essential to ensure consistent implementation and enforcement of data protection regulations. Without these improvements, ASEAN risks falling behind

[35] Merlita Yuli Safitri and Mahfud, "The ASEAN Cross-Border Personal Data Transfer Instrument: Has Indonesian's Personal Data Protection Law Followed it?", *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)* Volume 12 Number 3 (2023): 557.

[36] Graham Greenleaf, "ASEAN Model Contractual Clauses: Low and Ambiguous Data Privacy Standards", *University of New South Wales Law Research Series* (2021): 2-3.

in the increasingly competitive digital economy and may struggle to protect the privacy rights of its citizens effectively.

REFERENCE

ASEAN Framework on Personal Data Protection (2022).

ASEAN Model Contractual Clauses for Cross Border Data Flows (2021).

Drew Network Asia, "DNA ASEAN Guide to: Data Protection and Cybersecurity Regulation in Southeast Asia" (2024).

Efendi, Jonaedi dan Ibrahim, Johny. *Metode Penelitian Hukum: Normatif dan Empiris* (Depok, Prenada Media Group, 2018).

Georgios Yannopoulos, et. al., "Personal Data as the Currency of the Digital Age Having as an Example Art. 3 Par. 1 (and Preamble No. 24) of Directive 2019/770)", *Postgraduate Thesis National and Kapodistrian University of Athens* (2022).

Graham Greenleaf, "ASEAN Model Contractual Clauses: Low and Ambiguous Data Privacy Standards", *University of New South Wales Law Research Series* (2021).

GSMA, "Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation" (2018).

Indonesia's Minister of Communications & Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System (MOCI Regulation).

J. Lee and M. Perone, "The Influx of Cybercrime Across Southeast Asia and the Cyber Security and Data Protection Measures That Are Being Placed to Bolster Security Within the Region" (2019).

Jingting Liu, "Facilitating Data Flows Across ASEAN: Challenges and Policy Directions", *Asia Competitiveness Institute Research Paper Series* (2023).

Lingjie Kong, "Data Protection and Transborder Data Flow in the European and Global Context", *European Journal of International Law* 21, Issue 2 (2010).

Malaysia's Personal Data Protection Act 2010. Marc Van Lieshout, "The Value of Personal Data", *Conference Paper in IFIP Advances in Information and Communication Technology* (2015).

Merlita Yuli Safitri and Mahfud, "The ASEAN Cross-Border Personal Data Transfer Instrument: Has Indonesian's Personal Data Protection Law Followed it?", *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)* 12, No. 3 (2023).

Michael G. Plummer, et. al. *Connecting Asia: Infrastructure for Integrating South and Southeast Asia*, (Northampton: Edward Elgar Publishing, 2016).

Oluwatosin Reis, et. al., "Privacy Law Challenges in the Digital Age: A Global Review of Legislation and Enforcement", *International Journal of Applied Research in Social Sciences* 6, Issue 1 (2024).

Philippines' Data Privacy Act of 2012 (Republic Act No. 10173).

Prapanpong Khumon, "Cross-Border Data Privacy Regulation in ASEAN: Overcoming Institutional Challenge", *Research Paper of University of the Thai Chamber of Commerce* (2020).

Rahmi Ayunda, "Personal Data Protection to E-Commerce Consumer: What are the Legal Challenges and Certainties?", *Law Reform* 18, Issue 2 (2022).

Gabriel Rodrigues, et. al. "Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review", *Data 2023* 9, Issue 2 (2023).

Salsabila Siliwangi Surtiwa and Christian Jeremia Gultom, "ASEAN for Data Protection: Remarks on 2016 ASEAN Framework on Personal Data Protection and the Impact Towards Regional Peer to Peer Lending", *Atlantis Press: Advances in Social Sciences, Education and Humanities Research*, Volume 558 (2021).

Sigit Sapto Nugroho, et. al. *Metodologi Riset Hukum* (Surakarta: Oase Pustaka, 2020).

Singapore's Personal Data Protection Act 2012.

Syafri Haariansah, et. al., "Personal Data Protection in ASEAN: Indonesia's Role in Developing ASEAN's Personal Data Protection Legal Framework", *Novateur Publication India, Proceedings of International Seminar on Indonesian Lecturer is Born to Report Regularly* (2023).

Thailand's Personal Data Protection Act 2019.

United Nations Capital Development Fund, "The Role of Cross-Border Data Flows in the Digital Economy", *Policy Accelerator* (2022).

United Nations Development Programme (UNDP), Enabling Cross-Border Data Flow: ASEAN and Beyond, *UNDP Global Centre* (2021).

Vietnam's Civil Code (No. 91/2015/QH13).

Vietnam's Law on Information Technology (No. 67/2006/QH11).

Vietnam's Law on Network Information Security (No. 86/2015/QH13).

Waewpen Piemwichai, "Jurisdictional Report: Socialist Republic of Vietnam", *in Regulation of Cross-border Transfers of Personal Data in Asia, A compendium of 14 reports by the Asian Business Law Institute, ed. Asian Business Law Institute* (2018).