



Data Protection Regulations in ASEAN: Current Landscape and Prospects for Regional Collaboration

Ma Hanyu^{1*}, Zuryati Bt Mohamed Yusoff², Fariza Romli³

¹ UUM College of Law, Government and International Studies, Kedah, Malaysia

² UUM College of Law, Government and International Studies, Kedah, Malaysia

³ UUM College of Law, Government and International Studies, Kedah, Malaysia
mahanyu1995@gmail.com

Abstract. Following the vigorous development of the global digital economy, data has become a crucial strategic resource driving economic growth, and data protection has consequently emerged as a core issue attracting global attention. As emerging forces in the digital economy, ASEAN countries' data protection status not only plays a vital role in regional economic cooperation and enterprise development but also concerns the security and protection of personal information. This paper conducts an in-depth review of the data protection regulations of the major ASEAN member states and precisely focuses on the prominent problems within the region. These issues include the uneven progress of data protection legislation across countries, significant disparities in data protection regimes, and the weak binding force of regional framework agreements. Undoubtedly, the existence of these problems has brought numerous obstacles to the integration process of the digital economy in the ASEAN region. Drawing on comparative insights, this paper actively calls for taking the "ASEAN Digital Economy Framework Agreement" (DEFA) as an important opportunity to promote the establishment of unified data protection standards within the region. At the same time, it advocates the construction of a mutual trust mechanism and a cross-border regulatory cooperation system to provide a solid institutional guarantee for regional digital economic integration. By strengthening regional cooperation, countries can jointly address the various challenges brought about by the development of the digital economy, so as to achieve the sustainable and healthy development of the digital economy in the ASEAN region.

Keywords: ASEAN, Data Protection, Digital Economy, Cross-Border Data Flow.

1 Introduction

In the digital era, data has emerged as both a novel factor of production and a strategic resource, serving as a pivotal driver for nations to advance their digital economies. Consequently, the governance and protection of data have become central concerns in digital legislation worldwide. ASEAN, ranking as the world's fifth-largest economy [1], is increasingly positioned as a critical growth region for the global digital economy, leveraging its distinctive political advantages and strategic geographical positioning. According to the e-Conomy SEA 2024 Report jointly released by Google, Temasek, and Bain & Company, ASEAN's digital economy demonstrated significant progress in 2024, with its Gross Merchandise Value (GMV) projected to reach US\$263 billion—a 15% year-on-year increase [2].

In September 2023, ASEAN formally commenced negotiations on the Digital Economy Framework Agreement (DEFA), marking the world's first regional digital economy pact. Spanning nine core domains—including digital trade, cross-border

e-commerce, cybersecurity, digital identity, digital payments, and cross-border data flows—DEFA is projected to conclude negotiations in 2025. If successfully implemented, the agreement is forecasted to generate US\$2 trillion in revenue for ASEAN's digital economy, accounting for nearly one-third of the region's aggregate economic output [2]. Consequently, DEFA's implementation holds strategic significance for advancing ASEAN's digital economic development. However, substantial disparities persist in digital readiness and regulatory maturity across ASEAN Member States (AMS). Singapore, Malaysia, and the Philippines have established relatively sophisticated and dynamically updated legal frameworks through early enactment of comprehensive data protection legislation. Thailand, Indonesia, and Vietnam have recently promulgated specialized data protection statutes, while Cambodia and Brunei, Myanmar currently lack dedicated data protection laws. Divergences extend to critical dimensions such as: data subject rights, governance mechanisms, cross-border data flows (CBDFs) and Data Protection Officer (DPO) requirements even among jurisdictions with existing legislation. Although regulatory sovereignty must be respected, failure to reconcile data protection with free flow—and to bridge these regulatory gaps—will impede ASEAN's digital economic integration [3].

This study takes the DEFA negotiations as a point of departure, focusing on one of its core issues—data protection and CBDFs. It analyzes in depth the current state of data protection legislation across AMS and their institutional differences, and further assesses the potential impact of these differences on the process of regional digital integration. The study aims to provide reference and insights for understanding the maturity and sustainability of ASEAN's digital

2 Research Method

This study employs a descriptive legal analysis to systematically document and systematize the data protection regulations of AMS and relevant ASEAN-level agreements, thereby delineating the current landscape of national data protection regimes and ASEAN's framework for CBDFs. Concurrently, it utilizes normative legal analysis to conduct an in-depth examination of jurisprudential principles, institutional motivations, and prevailing challenges. In analyzing national data protection regulations, comparative legal methodology is integrated to conduct a contrastive study of regulatory convergences and divergences among AMS. The research materials comprise primary and secondary sources: primary sources encompass binding legal instruments, including ASEAN treaties and domestic legislation of member states; secondary sources incorporate scholarly journals, monographs, research papers, and statistical reports.

3 Current Status Of Data Protection Legislation In AMS

In the digital age, data is recognized as the fuel that drives the ongoing process of digital technology, not only supporting the operation of information technology, but also providing diverse value-added services to society[4]. For this reason, the significance of data makes data protection a core element in maintaining the security and stability of cyberspace. A mature regulatory framework for data protection not

only helps to effectively reduce the risks of data breaches and misuse, but also ensures the orderly functioning of cyberspace, thereby fostering the development of the digital economy [5]. This section examines the current status of data protection legislation among ASEAN member states. Broadly, these jurisdictions may be divided into three categories: the first group, represented by Malaysia, Singapore, and the Philippines, which adopted data protection laws relatively early and have developed comparatively mature legal frameworks; and the second group, including Thailand, Indonesia, and Vietnam, which have more recently embarked on data protection lawmaking and thus warrant focused discussion as emerging legislative regimes; The third category of countries includes Laos, Brunei, Cambodia, and Myanmar, where data protection legislation remains at an early stage of development, and some have not yet enacted dedicated laws. Therefore, they are not treated as primary subjects of analysis in this study.

3.1 Singapore

As the economic frontrunner among AMS, Singapore is also one of the most competitive economies globally. According to the Global Digitalization Index (GDI) 2024, which assessed the digitalization progress of 77 countries, Singapore ranked second worldwide, just behind the United States [6]. The rapid development of the digital economy has not only reinforced Singapore's leading position in the region but has also driven the country to attach great importance to data protection. As one of the first AMSto adopt comprehensive data protection legislation, Singapore enacted the Personal Data Protection Act (PDPA) in 2012, establishing the foundational legal framework for data protection. The PDPA has since undergone several amendments, the most recent of which was passed on November 2, 2020, and implemented in phases starting from February 2021. The PDPA aims to regulate the collection, use and disclosure of personal data by organisations, balancing the protection of individual rights with the legitimate need for organisations to process personal data [7]. The PDPA applies to any individual, company, association or organisation processing personal data within Singapore, including both incorporated and unincorporated entities, whether or not constituted or recognised under Singapore law, or resident in Singapore, or maintaining an office or place of business in Singapore [7]. This means that even foreign companies conducting business in Singapore and engaging in the collection, use, or disclosure of personal data are subject to the Act. However, the PDPA also provides certain exemptions, including: individuals acting in a personal or domestic capacity; employees processing personal data in the course of their employment with an organization; and activities carried out by public agencies [7].

To further ensure the effective application and practical enforcement of PDPA, the Personal Data Protection Commission (PDPC) has issued a series of supporting regulations, including the Personal Data Protection (Enforcement) Regulations 2021, Personal Data Protection Regulations, Personal Data Protection (Appeal) Regulations 2021, and Personal Data Protection (Notification of Data Breaches) Regulations 2021. In addition, the PDPC has published various sector-specific guidelines, practical guides, and advisory guidelines, providing clear references for organizations across different industries to ensure compliance in data protection practices.

3.2 Malaysia

Malaysia stands as a pivotal nation among Southeast Asian countries in advancing personal data protection and privacy legislation. Enacted in 2010 and effective from November 2013, The Personal Data Protection Act 2010 (Act 709) represents Malaysia's first comprehensive personal data protection legislation. The Act comprises 11 parts, covering its scope of application, seven fundamental principles governing data processing by Data Users, regulatory mechanisms, Data Subject rights, and penalty provisions. The principal objective of this legislation is to regulate the processing of personal data in commercial transactions by Data Users and to safeguard the interests of Data Subjects [8]. The law was passed after major revisions in 2024: Personal Data Protection (Amendment) Act 2024 (Act A1727). It will be implemented in three batches from January 1, 2025. Key points of the amendment include:

(1) Harmonization of terminology and definitions: The term “Data User” is replaced with “Data Controller” to align with the terminology of the General Data Protection Regulation (GDPR). The scope of sensitive personal data is expanded to include biometric data, and a new definition of Personal Data Breach is introduced.

(2) Stricter penalties: The maximum fine for non-compliance with security principles by data processors is increased from RM 300,000 to RM 1,000,000, while the maximum imprisonment term is extended from 2 years to 3 years.

(3) Enhanced attention to data breach incidents: Mandatory data breach notification is introduced. In the event of a personal data breach, data controllers must immediately notify the Commissioner, and in cases of serious harm, promptly inform the affected data subjects as well.

(4) Introduction of the right to data portability: Data subjects may, through a written electronic request, require the data controller to transfer their personal data to another controller, provided it is technically feasible and the data format is compatible.

(5) Mandatory appointment of Data Protection Officer (DPO): Each data controller is required to appoint one or more DPOs.

In addition, Malaysia has introduced a set of supplementary regulations and guidelines to facilitate the effective implementation of data protection provisions. These include: Personal Data Protection Regulations 2013, Personal Data Protection Standard 2015, Personal Data Protection Guidelines on Cross-Border Transfer of Personal Data (CBPDT), Personal Data Protection Guidelines on the Appointment of Data Protection Officer.

3.3 Philippines

The Philippines is also one of the early adopters of digital protection legislation among AMS, with the enactment of the Data Privacy Act in 2012 aimed at upholding human rights and ensuring free flow of information to promote innovation and

growth[9]. On September 9, 2016, the final implementing rules and regulations took effect, providing greater clarity and detail to the Data Privacy Act[10].

The act establishes a broad scope of application, covering natural and legal persons engaged in the processing of personal information, and reflects a clear extraterritorial effect. It applies to entities operating within the Philippines, to processing activities carried out through equipment located in the country, and to the processing of personal information of Philippine citizens regardless of their place of residence. However, it excludes from its scope personal information processed in the Philippines that has been lawfully collected from residents of foreign jurisdictions [11].

3.4 Thailand, Indonesia and Vietnam

Following the enactment of the GDPR, data protection legislation in the ASEAN region has entered a new phase since 2020. Singapore and Malaysia were among the first to recognize the necessity of aligning their national data protection laws with contemporary developments, undertaking revisions to establish more robust and higher-standard regulatory frameworks. In parallel, countries such as Thailand, Indonesia, and Vietnam have likewise initiated or accelerated their legislative efforts on data protection, reflecting a broader regional trend toward strengthening data governance.

On June 1, 2022, Thailand's Personal Data Protection Act came into full effect after two postponements, establishing the country's first comprehensive data protection framework. The Act was initially promulgated on May 28, 2019, with a one-year grace period provided for the establishment of the Personal Data Protection Committee and the development of supporting regulations. However, on 21 May 2020, the Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020) (Royal Decree) was published in the Royal Gazette, which effectively extended the implementation of the key provisions of the PDPA until 31 May 2021. On 8 May 2021, an amendment to the Royal Decree was published in the Royal Gazette (Royal Decree No. 2), which postpone the full enforcement of the PDPA for another year [12]. In substantive terms, Thailand's Personal Data Protection Act draws upon the framework of GDPR while incorporating differentiated arrangements tailored to the specific context of personal data protection in Thailand.

The earliest regulation on data protection in Indonesia dates back to Article 28G of the 1945 Constitution of the Republic of Indonesia [13]. Since then, provisions on privacy and personal data protection have been dispersed in a number of laws, including the Banking Act, the Telecommunications Act, the Consumer Protection Act, the Population Act, the Human Rights Act, the Electronic Information and Transactions Act, the Public Information Disclosure Act and so on. However, the legal system has long been fragmented due to the lack of unified personal data protection legislation. It was not until 20 September 2022 that Indonesia's House of Representatives passed the NO.27 regarding Personal Data Protection Law, marking the first time that the country had a dedicated data protection law in place [14].

Since 2023, Vietnam's legislative process in the field of data has accelerated significantly. In April 2023, the Vietnamese government promulgated Decree No. 13/2023/ND-CP on personal data protection (2023 Decree), the country's first dedicated regulation on data protection. The 2023 Decree had an immediate impact on both domestic and foreign enterprises directly engaged in or involving the processing of Vietnamese personal data. However, as a government decree, its legal status and deterrent effect are relatively limited. Subsequently, on November 30, 2024, the National Assembly of Vietnam passed the Law on Data, which is scheduled to take effect on July 1, 2025. This law distinguishes between digital data, important data, and core data at the terminological level, establishes national data centers and a national integrated database, and strengthens international cooperation in the field of data, marking a critical step forward in Vietnam's digital data governance. In June 2025, the National Assembly passed the Personal Data Protection Law, which will take effect on January 1, 2026. With a higher legal status than the 2023 Decree, it represents the country's first comprehensive law specifically addressing personal data protection. Vietnam is thereby advancing a concentrated legislative approach to gradually improve its data governance system and laying the foundation for the unified implementation of subsequent regulations.

3.5 Other ASEAN countries

In addition to the six countries discussed above, the legislative process on data protection in Laos, Brunei, Cambodia, and Myanmar remains relatively underdeveloped, although all show signs of gradual progress. Laos enacted the Law on Electronic Data Protection in 2017, followed by the Instructions on the Implementation of the Law on Electronic Data Protection in 2018, but its scope is limited to electronic data and does not cover other forms of data [15]. Moreover, Laos has not established an independent data protection authority, and its legal framework remains at an early stage of development. Brunei, by contrast, promulgated the Personal Data Protection Order in January 2025, which applies to the handling of personal data by private sector entities and non-governmental organizations, with the aim of aligning domestic rules with international data protection standards [16]. Cambodia and Myanmar, however, have not yet adopted dedicated data protection legislation; instead, relevant provisions remain scattered across other laws, leaving their overall institutional frameworks either blank or at an initial stage.

Given that the data protection regulations in these countries have not yet developed into stable and comprehensive legal systems, that their legislative texts continue to show gaps or remain in transition with respect to key issues such as definitions, enforcement procedures, and data transfers, and that accessible scholarly and policy materials are limited, this study does not examine them in depth but provides only a brief overview.

4 Comparative Analysis Of Data Protection Regulations In AMS

A comparison limited to legal frameworks and legislative processes is insufficient to uncover the deeper implications of data protection regimes for national security, economic development, and the safeguarding of individual rights. The crux lies in the specific institutional design differences among member states, such as the definition of personal data, the establishment of data subject rights, the regulation of cross-border data flows, and the compliance requirements imposed on enterprises. These differences not only directly affect the security and circulation of data within the region but also largely determine whether states can strike a balance between safeguarding sovereignty and advancing digital economic development. Accordingly, this chapter will undertake an in-depth analysis of the variations in the substantive content and implementation pathways of national laws, thereby laying the groundwork for examining the challenges they pose to regional data protection integration.

4.1 Differences in Key Terminologies

Alignment of basic terminology is essential for compliance with data-related regulations. If there are terminological differences between different AMS, it will be difficult for multinational enterprises to adjust their data processing to the different definitions [3].

The definition of ‘personal data’ constitutes the foundation of data protection law. In this regard, AMS generally align with international standards by adopting “identifiability” as the core criterion—namely, any information relating to an identified or identifiable natural person [17]. Nevertheless, differences remain with respect to the scope of data covered. The definitions in Laos and Vietnam are relatively narrow: Laos confines personal data to electronic data, while Vietnam explicitly limits it to data generated within electronic environments. By contrast, the Philippine legislation encompasses information recorded in any form, and Indonesia’s Personal Data Protection Law goes even further by covering any information capable of directly or indirectly identifying an individual, regardless of whether it is processed through electronic systems.

With respect to ‘sensitive personal data’, most AMS establish a distinct category within the broader framework of personal data, although the criteria for classification vary; Singapore remains an exception, as its legislation does not expressly differentiate sensitive personal data. Health information, religious beliefs, criminal records, racial or ethnic information, and biometric data are commonly recognized as sensitive categories across the region. At the same time, Vietnam explicitly includes geolocation data obtained through location-based services as sensitive personal data, whereas Indonesia specifically designates children’s data as sensitive. In regulating sensitive personal data, member states generally impose stricter requirements, such as obtaining the explicit consent of the data subject or implementing additional security safeguards during processing, thereby enhancing the level of protection afforded to this category of data.

4.2 Differences in Data Subject Rights

In the protection of data subject rights, legislative differences among AMS have a direct impact on the compliance costs of CBDFs. When discrepancies exist between the destination and origin countries in terms of the scope or strength of rights protection, multinational enterprises are often required to adopt supplementary contractual arrangements or internal compliance measures to bridge the gap and safeguard the lawful rights of data subjects [3]. However, such additional mechanisms not only increase institutional complexity but also substantially raise the compliance costs of CBDFs.

Despite these divergences, AMS generally recognizes four fundamental rights—namely, the right to be informed, the right to rectification, the right of access, and the right to consent—which collectively constitute the common foundation of data subject rights frameworks. Building upon this foundation, however, states have adopted distinct institutional approaches to the allocation and expansion of rights. First, Indonesia and Vietnam have strengthened data subject protection through comprehensive and detailed enumerations of rights. Second, Thailand and the Philippines have expanded beyond the four core rights to include the right to erasure, the right to anonymity, and the right to restriction of processing; moreover, the Philippines has introduced transferable rights and the right to data portability, reflecting a distinctive innovation in rights design. Third, Malaysia and Singapore, having adopted data protection laws relatively early, initially concentrated on the four core rights but have in recent years incorporated additional rights, such as data portability and the right to civil action, through legislative amendments to respond to emerging needs in the digital economy.

Accordingly, while AMS demonstrate convergence in their recognition of fundamental rights, they also exhibit considerable divergence in the detailed design and extension of data subject rights. These divergences not only shape compliance practices within the region but also pose potential challenges to the advancement of data protection integration in ASEAN.

4.3 Differences in the DPO Regime

DPO is a dedicated position appointed within an organization by the data controller or processor, with the core responsibility of overseeing and promoting the organization's data compliance management, ensuring that personal data processing activities adhere to applicable laws and regulations. Whether the appointment of a DPO is mandatory not only directly affects the implementation and effectiveness of internal data compliance mechanisms but also influences the balance between compliance costs and governance efficiency.

As regional data governance frameworks gradually develop, AMS have shown an expanding trend in the establishment and implementation of the DPO regime. An increasing number of countries recognize that establishing a dedicated position is crucial for reinforcing data protection accountability, enhancing compliance transparency, and strengthening public trust. Differences among countries exist in terms of DPO appointment requirements, reflecting both the varying stages of legal

development and the dynamic characteristics of regional convergence. Specific appointment requirements are summarized in the table below:

Table 1. DPO Appointment Form.

Countries	Mandatory DPO Appointment	Appointment Criteria
Malaysia	Yes	Data controllers and data processors are required to appoint one or more DPO if their processing of personal data involves: 1) personal data exceeding 20,000 data subjects, 2) sensitive personal data including financial information data exceeding 10,000 data subjects, and 3) involves activities that require regular and systematic monitoring of personal data.
Philippines	No	\
Thailand	Yes	Data controller and processor shall designate a DPO in the following circumstances: 1) the data controller or the data processor is a public authority as prescribed and announced by the committee, 2) the activities of the data controller or the data processor in the collection, use, or disclosure of the Personal Data require a regular monitoring of the Personal data or the system, by the reason of having a large number of personal data as prescribed and announced by the committee and 3) the core activity of the data controller or the data processor is the collection, use, or disclosure of the personal data.
Indonesia	Yes	The data controller or processor must appoint a DPO in any of the following circumstances: 1) Where the processing of personal data is for the performance of a public service, 2) Where the core activities involve the large-scale, regular and systematic monitoring of personal data, and 3) Where the core activities include the large-scale processing of specific (sensitive) personal data or personal data relating to criminal offences.

Vietnam	Yes	All organisations processing personal data shall appoint a DPO, with small/start-up enterprises granted a five-year grace period.
Singapore	Yes	Organisations processing personal data in Singapore, regardless of size or whether they are foreign companies, must appoint at least one DPO.

The comparative overview in the table1 demonstrates that following Malaysia's enactment of amendments to its Personal Data Protection Act in 2024, which introduced mandatory requirements for appointing DPO, the Philippines currently stands as the sole ASEAN nation without compulsory provisions for DPO appointments. Concurrently, significant variations exist in appointment criteria across nations: Vietnam and Singapore adopt stricter models, mandating all organisations processing personal data to designate a DPO for comprehensive coverage; whereas Thailand, Indonesia, and Malaysia employ differentiated standards, setting specific thresholds based on the scale, nature, purpose of data processing, or the industry sector of the enterprise.

4.4 Differences in CBDFs Rules

CBDFs are central to both the development of the digital economy and national security, making them a core issue within the data protection regimes of AMS. Given varying levels of economic development and security considerations, these nations strike different balances between economic growth and national security, resulting in inconsistent stringency in CBDF policies. Overall, apart from Vietnam imposing local storage requirements for specific data categories, other nations have not implemented mandatory data localisation mandates. The prevailing trend remains oriented towards facilitating cross-border data flows. While countries generally emphasise that recipient nations must possess ‘adequate’ or ‘equivalent’ data protection standards, significant variations exist in institutional design and implementation pathways.

Singapore requires that, for CBDFs, the receiving country or region must offer protection standards equivalent to its own. Where this is not the case, either the individual's consent must be obtained or the transferring organisation must implement reasonable measures to ensure the recipient does not use the transferred personal data for any other purpose [7]. Indonesia, while sharing similarities with Singapore, differs in its implementation sequence. It adopts a ‘three-tiered’ model: prioritising an assessment of the recipient country's protection level; requiring binding safeguards where protection is inadequate; and only then considering the consent of the data subject.

Malaysia and Thailand both provide relatively detailed compliance pathways for CBDFs. In 2025, Malaysia issued the Guidelines on Cross-Border Transfer of Personal Data, aimed at clarifying the requirements of Section 129 of the amended

Personal Data Protection Act 2010 The Guidelines outline eight specific compliance scenarios, including substantially similar legal frameworks or adequate protection levels, contractual necessity, data subject consent, legal procedures, and legitimate interests, among others. Compliance with any one of these eight scenarios is sufficient, and there is no prescribed order of application [18]. Thailand explicitly enumerates four legal bases for CBDFs: adequacy decisions, binding corporate rules, appropriate safeguards, and statutory exemptions, which must be applied sequentially. Binding corporate rules refer to situations where the data controller or processor has established a personal data protection policy for cross-border transfers, and the foreign recipient is part of the same corporate group or affiliated enterprise, with the purpose of jointly operating the business of such entities. Statutory exemptions can only be invoked if the preceding three conditions are not met, and include six specific provisions such as compliance with legal requirements, informed consent of the data subject, and legitimate interests [19].

Vietnam's CBDF regulations are more strongly oriented toward national security. Certain categories of data are subject to localization requirements, and transfers are subject to ex-post review. Under the Cybersecurity Law, domestic and foreign enterprises providing telecommunications networks, internet services, or value-added network services in Vietnam must store personal information data within the country [20]. Furthermore, for cross-border transfers, enterprises must submit an impact assessment report within 60 days of the first transfer and are subject to periodic or ad hoc inspections by the competent authorities, who may even order an immediate halt to transfers on national security grounds.

In comparison, the Philippines adopts a relatively flexible approach. Data controllers may rely on contracts or other reasonable measures to ensure an adequate level of protection when personal data are processed by third parties, providing considerable flexibility in implementation.

5 Current Status And Prospect Of Regional Data Protection Cooperation In Asean

The rapid rise of ASEAN's digital economy has spurred proactive efforts to refine its data protection framework, seeking to balance global standards with regional requirements. However, the delicate balance between the free flow of data and the preservation of national sovereignty and security has rendered regional cooperation on data protection both complex and sensitive. Having previously examined the developmental status and institutional variations of national data protection regulations, this chapter further analyses the current state of regional cooperation within ASEAN, identifies key challenges encountered during data protection development, and proposes recommendations for future advancement.

5.1 Analysis of Existing Cooperation Frameworks

In recent years, ASEAN has introduced several framework agreements related to the development of the digital economy. These include the 2016 Personal Data Protection Framework (PDPF), the 2021 Model Contractual Clauses for Cross-border Data Flow (MCCs), and the Data Management Framework (DMF). These frameworks primarily serve as guidance tools rather than legally binding instruments. DEFA currently under negotiation, is expected to complete its discussions by the end of 2025.

As a response to the rapid growth of data flows in the region, ASEAN Telecommunications and Information Technology Ministers initiated a framework to strengthen the region's data ecosystem. This framework refers to the 2016 PDPF, which primarily establishes a set of fundamental principles for safeguarding data privacy, encourages member states to improve their data governance frameworks, and promotes innovation in the digital economy[21]. However, it is important to note that the 2016 PDPF is not legally binding at the national or international level, and reflects only the commitment of member states to protect personal data from misuse, without substantive legal consequences[3].

In 2021, ASEAN introduced the MCCs to serve as a model for cross-border personal data transfers within the region, facilitating business transactions among member states. The MCCs are voluntary in nature and provide guidance on basic considerations for personal data transfers. Parties may adopt or modify the MCCs through written agreements or choose other data transfer mechanisms recognized by AMS, as long as they do not conflict with the principles of the ASEAN PDPF or the legal requirements of any AMS. The DMF, also adopted in 2021, provides guidance on data governance for businesses, particularly small and medium-sized enterprises (SMEs). Similar to the MCCs, it remains voluntary and does not carry legal force.

On August 19, 2023, a study on DEFA was officially approved at the ASEAN Economic Ministers' Meeting. DEFA aims to harmonize digital trade rules across ASEAN, leveraging regional complementarities to promote economic growth and facilitate the transition to more advanced economies[22]. According to a Boston Consulting Group projection, the gradual implementation of DEFA's rules could unlock USD 2 trillion for the ASEAN digital economy by 2030 [2]. Given its potential economic impact, DEFA is of significant value to ASEAN's development, though negotiations are still ongoing, with completion expected by the end of 2025.

5.2 Key Challenges Encountered in Regional Cooperation

ASEAN has been making continuous efforts to promote regional cooperation on data protection; however, it still faces certain challenges in this process. Based on the analysis above, there are three key challenges to ASEAN's regional cooperation on data protection: the uneven pace of legislative development, differences in institutional design, and the limited binding force of regional framework agreements. The interplay of these three issues has hindered the progress of regional cooperation.

Uneven Legislative Development: Insufficient Institutional Foundations for Regional Integration. Personal data protection forms the bedrock of data governance

and constitutes a fundamental prerequisite for the robust development of the digital economy. In the ASEAN region, Singapore, Malaysia, and the Philippines place a high priority on personal data protection legislation. These three countries enacted their laws relatively early, and after more than a decade of development and amendments, they have established relatively mature legal frameworks as well as enforcement and implementation capacities, resulting in a comprehensive and systematic institutional structure. In contrast, Indonesia, Thailand, and Vietnam have enacted dedicated personal data protection laws only in recent years. Due to their shorter legislative history, these countries have limited regulatory experience, and their institutional maturity and enforcement capacity remain at an early stage, posing certain challenges for cross-border data compliance. Cambodia, Laos, Brunei, and Myanmar have yet to establish dedicated data protection laws and rely solely on scattered regulations and industry guidelines, with unclear legal foundations and lagging legislative progress.

These disparities in legislative development reflect significant differences among countries in terms of economic development and digital technology adoption. Even under regional framework agreements, member states continue to exhibit inconsistencies in regulatory enforcement and compliance practices, and may lack sufficient capacity to respond to data security risks. The unevenness of legislative progress not only results in varying levels of data protection across the region but also hinders ASEAN from establishing a unified institutional starting point, leaving regional integration efforts without a common legal foundation or operational premise.

Divergent Institutional Designs: Fragmentation of Regulatory Models and Compliance Requirements. Even among countries that have established dedicated data protection legislation, significant differences remain in the emphasis placed on economic development versus individual rights, directly resulting in inconsistencies in the design of data protection standards. Specifically, variations in the definitions of personal and sensitive personal data complicate the processes of data collection and screening; divergent provisions on data subject rights, differing requirements for the appointment of DPO, and significant differences in cross-border data compliance procedures collectively increase the compliance costs and operational complexity for multinational enterprises within ASEAN. Consequently, these factors not only hinder smooth market entry for businesses but also weaken the coordination and predictability of data protection regimes across the region.

Limited Binding Force of Regional Frameworks: Absence of Standardized Data Protection Measures. To promote regional digital economic development and strengthen cross-border data governance, ASEAN has introduced several framework agreements. However, most of these agreements lack legal enforceability and exist primarily as voluntary guidance documents, resulting in limited enthusiasm and consistency among member states in adoption and implementation. Consequently, multinational enterprises must primarily rely on domestic laws in their operations rather than regional frameworks as a unified compliance reference. This not only renders the agreements at risk of being largely symbolic in practice but also prevents

the establishment of uniform data protection and governance standards across the region, thereby weakening the effectiveness of ASEAN regional cooperation.

5.3 Recommendations for Advancing Regional Cooperation

In addressing the above challenges, ASEAN can adopt a phased and prioritized strategy. In the short term, priority should be given to establishing regionally binding minimum compliance standards and mutually recognized templates to provide enterprises with clear pathways for cross-border compliance. At the same time, pilot cooperation and mutual recognition mechanisms among multiple countries can be initiated to reduce compliance costs for multinational enterprises and accumulate practical experience. Additionally, leveraging the DEFA framework, particular attention should be paid to provisions on CBDFs and data protection, promoting the development of unified data protection standards across the region.

In the long term, ASEAN should focus on strengthening regional capacity and institutional foundations. This includes establishing digital technology and legal assistance mechanisms to help member states with relatively underdeveloped legislation to enhance their lawmaking and institutional design capabilities. Furthermore, a regional platform for capacity building and enforcement cooperation can be created. By sharing training resources, conducting joint investigations, and facilitating cross-border evidence collection, disparities in enforcement capabilities among member states can be partially mitigated, thereby supporting a more cohesive and predictable regional data governance environment.

6 Conclusion

In conclusion, ASEAN has made notable progress in promoting regional data protection cooperation and digital economic development, yet it continues to face challenges such as uneven legislative development, divergent institutional designs, and the limited binding force of regional frameworks. These issues create disparities in regulatory enforcement and cross-border compliance practices, increasing operational costs for enterprises and constraining the legal and institutional foundation for regional integration. To address these challenges, ASEAN can adopt a combined short-term and long-term strategy: in the short term, establish minimum compliance standards and mutual recognition mechanisms, and leverage DEFA to promote unified data protection standards; in the long term, strengthen capacity building, legal assistance, and enforcement cooperation platforms to enhance institutional maturity and effectiveness. Overall, a progressively improved regional cooperation mechanism is expected to safeguard data security while supporting the sustainable development of ASEAN's digital economy.

References

1. ASEAN-China Centre. Digital Economy Landscape in ASEAN: Regulatory Developments. Ministry of Commerce of China. 2024. Retrieved August 14, 2025 from

- http://asean.mofcom.gov.cn/dmj/j/dnygjlm/art/2024/art_a90081a6cefa470c9f96ee91d7418926.html
2. Hoppe, F.; Chang, W.; Baijal, A.; Chadha, S.; and Fock, W. (2024). *e-Conomy SEA 2024: Profits on the Rise, Harnessing SEA's Advantage*. Bain & Company (in collaboration with Google and Temasek). November 5, 2024. <https://www.bain.com/insights/e-conomy-sea-2024/>
 3. Keita Oikawa. ASEAN Data Governance: Implications for the Digital Economy Framework Agreement
 4. Irina Lock and Peter Seele. 2017. Theorizing stakeholders of sustainability in the digital age. *Sustain Sci* 12, 2 (March 2017), 235–245. <https://doi.org/10.1007/s11625-016-0404-2>
 5. A. Malatras, I. Sanchez, L. Beslay, I. Coisel, I. Vakalis, G. D'Acquisto, M. G. Sanchez, M. Grall, M. Hansen, and V. Zorkadis. 2017. Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities. *Computer Law & Security Review* 33, 4 (2017), 458–469. Elsevier
 6. Huawei Technologies and International Data Corporation. 2024. Global Digitalization Index 2024. Huawei.
 7. Singapore. 2012. Personal Data Protection Act 2012 (No. 26 of 2012). <https://sso.agc.gov.sg/Act/PDPA2012>
 8. Malaysia. 2010. Persona Data Protection Act 2010 (Act709). <https://www.pdp.gov.my/ppdpv1/en/akta/pdp-act-2010-en/>
 9. Amiludin Amiludin, Siti Nurhalisa, Undang Prasetya Umara, and Hidayatullah. 2024. Comparison of protection laws private data in Indonesia and the Philippines. *Jurisprudence* 14, 2 (December 2024), 171–191. <https://doi.org/10.23917/jurisprudence.v14i2.4266>
 10. IAPP. 2017. A summary: Philippines Data Protection Act and implementing regulations. International Association of Privacy Professionals. Retrieved September 2, 2025 from <https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations/>
 11. A. Lonzetta and T. Hayajneh. 2018. Challenges of complying with data protection and privacy regulations. *ICST Transactions on Scalable Information Systems* 5, 18 (July 2018), 166352. <https://doi.org/10.4108/eai.26-5-2020.166352>
 12. DLA Piper. 2025. Data protection laws of the world: Thailand. DLA Piper. Retrieved September 2, 2025 from <https://www.dlapiperdataprotection.com/index.html?t=law&c=TH>
 13. R. Anggriawan, A. A. Salim, Y. Gunawan, and M. H. Arumbinang. 2022. Passenger name record data protection under European Union and United States agreement: security over privacy? *Hasanuddin Law Review* 8, 2 (2022), 95–110.
 14. Rina Shahriyani Shahrullah, Jihyun Park, and Irwansyah Irwansyah. 2024. Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment. *Hasanuddin Law Rev.* 10, 1 (January 2024), 1. <https://doi.org/10.20956/halrev.v10i1.5016>
 15. DLA Piper. 2025. Data Protection Laws of the World: Laos. Retrieved September 6, 2025 from <https://www.dlapiperdataprotection.com/index.html?t=law&c=LA>
 16. The Scoop. 2025. Brunei enacts new law giving citizens control over personal data. Retrieved September 6, 2025 from <https://thescoop.co/2025/03/08/brunei-enacts-new-law-giving-citizens-control-over-personal-data/>
 17. European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the

- Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), Art. 4: Definitions. Official Journal of the European Union, L119, 1–88. Retrieved September 12, 2025 from <https://gdpr-info.eu/art-4-gdpr/>
18. Personal Data Protection Commissioner. (2025). Personal Data Protection Guidelines on Cross-Border Transfer of Personal Data (CBPDT). Retrieved from <https://www.pdp.gov.my/ppdpv1/en/akta/personal-data-protection-guidelines-on-cross-border-transfer-of-personal-data-cbpdt/>
 19. Office of the Personal Data Protection Committee. (n.d.). Personal Data Protection Act, B.E. 2562 (2019). Retrieved from https://pdpathailand.com/pdpa/index_eng.html
 20. Vietnam National Assembly. (2018). Article 26 of the Law on Cybersecurity. Retrieved September 8, 2025 from <https://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=132957>
 21. Salsabila Siliwangi Surtiwa and Christian Jeremia Gultom. 2021. ASEAN for Data Protection: Remarks On 2016 ASEAN Framework on Personal Data Protection and The Impact Towards Regional Peer to Peer Lending. 2021. Jakarta, Indonesia. <https://doi.org/10.2991/assehr.k.210531.090>
 22. ASEAN Secretariat. (2023, August 19). Digital Economy Framework Agreement (DEFA): ASEAN to leap forward its digital economy and unlock US\$2 Tn by 2030. ASEAN. Retrieved September 10, 2025 from <https://asean.org/asean-defa-study-projects-digital-economy-leap-to-us2tn-by-2030/>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

