

Custodia: Journal of Legal, Political, and Humanistic Inquiry
Vol 2 No 2 December 2026, Hal 17-32
ISSN: 3123-2116 (Print) ISSN: 3123-2108(Electronic)
Open Access: https://scriptaintelektual.com/custodia

Strengthening Personal Data Protection in the Digital Era: A Comparative Analysis of Regulatory Frameworks and Human Rights Safeguards in Southeast Asia

Nur Vita Ristiana[1*], Azka Syifaul Maula[2], Assmaa Guerra[3], Deo Renaldi Saputra[4], Elinda Novita Dewi[5], Sahal Hanafi[6]
[1-2] UIN Sunan Kalijaga Yogyakarta, Indonesia
[3] Al-Azhar University, Cairo, Mesir
[4-6] Universitas Negeri Semarang, Indonesia
Email: 25203011011@student.uin-suka.ac.id[1]

Article Info :
Received:
15-10-2026
Revised:
08-11-2026
Accepted:
20-11-2026

Abstract

This study examines the strengthening of personal data protection and human rights safeguards in Southeast Asia amid accelerating digitalisation, cross-border data flows, and emerging data-driven technologies. Employing a non-empirical legal research design, the study applies normative, doctrinal, and comparative legal approaches to ASEAN instruments and national regulatory frameworks in Indonesia, Singapore, Malaysia, Thailand, the Philippines, Vietnam, Brunei Darussalam, Cambodia, Laos, and Myanmar. The analysis focuses on legal bases for processing, data-subject rights, institutional accountability, sensitive data protection, breach notification, cross-border transfers, sanctions, remedies, anonymisation, and safeguards against automated decision-making. The findings demonstrate substantial regional convergence concerning privacy, consent, purpose limitation, security, accountability, and individual control, while significant divergence persists in statutory scope, supervisory authority, enforcement mechanisms, remedial structures, and cross-border transfer requirements. These differences indicate that formal regulatory similarity does not necessarily produce substantive equivalence in human rights protection. The study further identifies regulatory fragmentation as a significant challenge to consistent protection of data subjects within increasingly integrated regional digital ecosystems. The study argues that ASEAN data protection governance requires harmonisation based on substantive equivalence, institutional interoperability, and enforceable minimum safeguards rather than uniform legislative formulations. The study contributes a comparative legal framework for evaluating personal data protection as an integrated mechanism of privacy, dignity, autonomy, and responsible digital governance.

Keywords: *ASEAN, Data Governance, Human Rights, Legal Harmonisation, Personal Data Protection.*



©2026 Authors.. This work is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.
(https://creativecommons.org/licenses/by-nc/4.0/)

INTRODUCTION

The rapid expansion of digital platforms, artificial intelligence, cloud computing, cross-border data flows, and data-driven public services has transformed personal data from a conventional privacy concern into a strategic resource with profound implications for economic governance, institutional accountability, and human rights protection. At the global level, the European Union's General Data Protection Regulation (GDPR) has increasingly operated as a regulatory and normative reference beyond Europe, influencing the development and reform of data protection laws in other jurisdictions through processes of legal diffusion and regulatory emulation (Bentotahewa et al., 2022). This diffusion has also affected Southeast Asia, where national governments have increasingly adopted or strengthened personal data protection regimes while simultaneously pursuing digital economic integration and technological innovation (Corning, 2024). ASEAN has responded to these developments through regional instruments that establish common principles concerning human rights, personal data protection, digital data governance, and data anonymisation (ASEAN, 2012; ASEAN, 2016; ASEAN, 2018; ASEAN, 2025). Yet the existence of regional principles does not automatically generate uniform legal protection because their implementation remains embedded within diverse domestic legal, political, and institutional structures. The central challenge is therefore no longer limited to whether personal data protection has become a recognised regulatory priority, but concerns whether

rapidly expanding digital governance can provide consistent and effective safeguards for individuals across jurisdictions with substantially different approaches to privacy, state authority, economic development, and regulatory enforcement.

Previous research demonstrates that Southeast Asian countries have developed increasingly sophisticated legal responses to personal data protection, although the pace, scope, and institutional configuration of these reforms remain uneven. Indonesia established a comprehensive statutory foundation through Law No. 27 of 2022 on Personal Data Protection, representing an important shift from fragmented sectoral regulation toward a more consolidated legal framework (Republik Indonesia, 2022). Singapore had already established a dedicated statutory regime through the Personal Data Protection Act 2012, while Malaysia subsequently strengthened its framework through the Personal Data Protection (Amendment) Act 2024 (Singapore Statutes Online, 2012; Personal Data Protection Commissioner, 2024). Thailand and the Philippines similarly developed dedicated legislation through the Personal Data Protection Act B.E. 2562 (2019) and Republic Act No. 10173, respectively, indicating a broader regional movement toward formalising individual rights and organisational responsibilities in data processing (Kingdom of Thailand, 2019; Republic of the Philippines, 2012). Vietnam introduced Decree No. 13/2023/ND-CP, while Brunei Darussalam adopted the Personal Data Protection Order 2025, that regulatory development continues to expand across jurisdictions with different institutional and legal traditions (Government of Vietnam, 2023; Brunei Darussalam, 2025). Comparative scholarship nevertheless shows that these national developments should not be interpreted as evidence of complete regulatory convergence because differences remain in regulatory scope, institutional authority, accountability requirements, enforcement mechanisms, and approaches to cross-border data governance (Sudarwanto & Kharisma, 2022). The regional landscape therefore reflects simultaneous regulatory maturation and continuing fragmentation, creating an important basis for examining whether legislative proliferation has actually produced comparable levels of protection for individuals.

The existing literature also reveals that personal data protection cannot be adequately understood through statutory comparison alone because its effectiveness is closely connected to broader questions of consumer rights, sectoral regulation, digital governance, and individual autonomy. Comparative research on Indonesia, Vietnam, and Ghana indicates that consumer protection frameworks increasingly intersect with personal data governance as digital transactions transform informational control into an issue of market fairness and individual vulnerability (Kadir et al., 2024). Sector-specific research further demonstrates that sensitive information such as patient data requires interaction between general personal data legislation, healthcare regulation, institutional responsibilities, and cross-border processing safeguards (Kharisma & Diakanza, 2024). Research on Asian data governance similarly suggests that regulatory frameworks increasingly reflect competing priorities involving digital sovereignty, economic development, technological innovation, and protection from transnational data risks (Grover et al., 2024). However, much of the comparative literature continues to emphasise legislative structures and regulatory similarity without sufficiently distinguishing formal legal convergence from substantive fulfilment of privacy and human rights. The conceptual problem becomes particularly visible in debates over the legal character of personal data, where competing ownership theories demonstrate tensions between viewing data as an economic resource and recognising its connection to personality, autonomy, and individual rights (Maharani et al., 2025). These unresolved perspectives indicate that a comprehensive comparison requires attention not only to what national laws regulate but also to the underlying conception of the individual that those laws seek to protect.

A significant gap consequently emerges in the limited integration of regulatory harmonisation with human rights assessment across the Southeast Asian context. Recent scholarship identifies continuing challenges concerning the effectiveness, scope, institutional implementation, and coherence of personal data protection governance across the Asia-Pacific region, suggesting that formal legislative adoption does not necessarily guarantee effective protection in practice (Palupy et al., 2026). Comparative research between Indonesia and South Korea further that the existence of extensive statutory rights must be examined in relation to their actual capacity to fulfil privacy rights and provide meaningful protection to individuals (Shahrullah et al., 2025). The problem becomes increasingly complex in cross-border data environments, where differences between national regulatory standards can affect the protection available to individuals when personal information moves between jurisdictions. ASEAN's regional frameworks provide important normative foundations, but their non-

uniform implementation leaves substantial space for domestic interpretation and institutional discretion. The recent development of data anonymisation guidance demonstrates continued regional efforts to operationalise responsible data governance while responding to the increasing need to use data without unnecessarily exposing identifiable individuals (ASEAN, 2025). At the same time, the regulatory trajectories of Cambodia, Laos, and Myanmar demonstrate that Southeast Asian data governance encompasses jurisdictions operating under markedly different legislative foundations and stages of regulatory development (Kingdom of Cambodia, 2019; Lao People's Democratic Republic, 2017; Republic of the Union of Myanmar, 2017). This fragmentation creates an unresolved empirical question concerning whether regional regulatory development is moving toward meaningful harmonisation or merely producing parallel national systems that share terminology but differ substantially in rights protection and enforcement capacity.

The urgency of this problem has increased as digital transformation intensifies the volume, velocity, and cross-border movement of personal information while emerging technologies create new forms of data processing that challenge conventional regulatory assumptions. Cross-border health data flows, for example, demonstrate how technological integration can simultaneously generate opportunities for improved services and create significant governance and human rights challenges when data move across different legal jurisdictions (Xia et al., 2024). The diffusion of GDPR principles into Asian legal systems further demonstrates that external regulatory norms can influence domestic reform while remaining subject to selective adaptation according to national legal and institutional contexts (Bentotahewa et al., 2022). The development of artificial intelligence regulation in Indonesia also how data protection is increasingly connected with broader questions concerning automated decision-making, technological accountability, and responsible innovation (Revolusi & Febriandy, 2025). Recent comparative research on ASEAN similarly identifies legal harmonisation as a continuing challenge because national frameworks differ in their regulatory maturity, institutional arrangements, and approaches to digital privacy (bin Kirin & Ismail, 2025). The resulting situation creates practical uncertainty for individuals, businesses, regulators, and cross-border digital service providers because the rights and obligations applicable to personal information may change according to the jurisdiction in which data are collected, transferred, processed, or stored. A rigorous comparative examination is therefore necessary to determine whether existing regulatory arrangements are capable of reconciling regional digital integration with consistent protection of privacy, dignity, autonomy, and other fundamental rights.

This study positions itself within this unresolved intersection of comparative law, digital governance, regulatory harmonisation, and human rights by treating personal data protection as both a legal institution and a mechanism for safeguarding individuals in increasingly interconnected digital environments. It aims to comparatively analyse the regulatory frameworks governing personal data protection in Southeast Asia by examining their principal legal safeguards, individual rights, institutional mechanisms, enforcement structures, and approaches to cross-border data governance. The analysis is directed toward identifying substantive areas of convergence and divergence rather than merely cataloguing the existence of national legislation. It also seeks to assess whether ASEAN-level regulatory principles provide an adequate normative foundation for strengthening regional consistency while allowing domestic legal systems to retain their distinctive institutional and constitutional characteristics. The research further addresses the conceptual distinction between formal regulatory convergence and effective human rights protection by examining whether statutory rights are supported by mechanisms capable of translating legal principles into meaningful safeguards for individuals. Theoretically, the study contributes to the comparative data protection literature by connecting regulatory diffusion and regional harmonisation with a human rights-based understanding of privacy, autonomy, dignity, and accountability. Methodologically, it contributes a structured comparative framework for evaluating national regulatory systems through both their formal legal architecture and their capacity to provide coherent and effective safeguards in the digital era.

RESEARCH METHOD

This study adopts a non-empirical legal research design employing normative, doctrinal, and comparative legal approaches to examine the strengthening of personal data protection and human rights safeguards in Southeast Asia. The normative approach is used to analyse the legal principles governing privacy, personal data protection, individual rights, institutional responsibilities, and state

obligations within the digital environment. The doctrinal approach focuses on the interpretation and systematic examination of primary legal materials, particularly statutory provisions, regulatory instruments, institutional mandates, individual rights, consent requirements, data-processing obligations, cross-border data transfer rules, sanctions, and available remedies. The primary legal materials comprise ASEAN instruments and national legislation from selected Southeast Asian jurisdictions, including Indonesia, Singapore, Malaysia, Thailand, the Philippines, Vietnam, Brunei Darussalam, Cambodia, Laos, and Myanmar, together with relevant regional regulatory frameworks. ASEAN instruments are treated as important regional normative references because they establish principles concerning human rights, personal data protection, digital data governance, and responsible data utilisation (ASEAN, 2012; ASEAN, 2016; ASEAN, 2018). The study also incorporates secondary legal materials consisting of peer-reviewed journal articles and comparative legal scholarship addressing regulatory harmonisation, privacy rights, data governance, and the development of personal data protection regimes in Southeast Asia. The comparative approach is applied by systematically placing the substantive provisions of the selected jurisdictions alongside one another to identify similarities, differences, regulatory gaps, and variations in the legal protection afforded to data subjects.

The analysis proceeds through a structured legal interpretation that connects textual provisions with the underlying principles of privacy, autonomy, dignity, accountability, proportionality, and effective human rights protection. Each relevant legal provision is examined according to its normative function, including provisions governing the definition and scope of personal data, lawful processing, consent, data-subject rights, obligations of controllers and processors, institutional oversight, breach notification, cross-border transfers, enforcement, and remedies. The comparative assessment distinguishes between formal regulatory convergence, which concerns similarities in statutory formulation, and substantive convergence, which concerns the extent to which legal frameworks provide comparable and effective safeguards for individuals. Particular attention is given to the relationship between general personal data protection statutes and sector-specific rules because the protection of sensitive information may depend upon overlapping regulatory regimes and institutional responsibilities (Kharisma & Diakanza, 2024). The interpretation also considers the influence of international regulatory diffusion and the adaptation of external legal norms within domestic Southeast Asian frameworks, rather than assuming that legislative similarity necessarily reflects identical regulatory objectives (Corning, 2024). The validity and consistency of the legal analysis are strengthened through triangulation of primary legislation, ASEAN instruments, and authoritative comparative scholarship, allowing individual provisions to be interpreted within their broader regulatory and human rights context. The resulting analytical framework is used to formulate a comparative assessment of the strengths, limitations, inconsistencies, and harmonisation opportunities within Southeast Asian personal data protection regimes, with particular emphasis on whether existing legal safeguards are capable of responding to contemporary digital risks while preserving fundamental human rights.

RESULT AND DISCUSSION

Comparative Regulatory Architecture of Personal Data Protection in Southeast Asia

The regulatory architecture of personal data protection in Southeast Asia has developed through interaction between regional normative instruments and increasingly comprehensive domestic legislation, producing common regulatory principles alongside substantial differences in legal construction. The ASEAN Human Rights Declaration establishes privacy within a broader human rights framework, while the ASEAN Framework on Personal Data Protection formulates principles concerning consent, notification, purpose limitation, data integrity, security, access, and accountability (ASEAN, 2012; ASEAN, 2016). The ASEAN Framework on Digital Data Governance extends these principles toward responsible data management and governance within an increasingly integrated digital economy (ASEAN, 2018). These instruments primarily function as regional normative references rather than directly enforceable supranational legislation, leaving domestic statutes responsible for determining the concrete scope of individual rights and institutional obligations. The resulting legal landscape must therefore be assessed through the substance of national rules rather than merely through the existence of dedicated data protection legislation. Comparative scholarship indicates that Southeast Asian jurisdictions have strengthened privacy regulation while retaining different

approaches shaped by domestic legal traditions, institutional capacities, and digital governance priorities (Polii et al., 2025).

Indonesia provides one of the region's most comprehensive statutory frameworks through Law No. 27 of 2022 on Personal Data Protection (UU PDP), which establishes a dedicated legal architecture governing personal data subjects, controllers, processors, processing activities, rights, obligations, and sanctions. Article 1 defines Personal Data, Personal Data Subject, Personal Data Controller, and Personal Data Processor, while Article 4 distinguishes general personal data from specific personal data, including health, biometric, genetic, criminal-record, child, and personal financial information (Republik Indonesia, 2022). Articles 20–22 establish lawful bases for processing and impose specific requirements where consent constitutes the legal basis, while Articles 5–15 formulate rights concerning information, access, correction, deletion, withdrawal of consent, objection, restriction, compensation, and portability (Republik Indonesia, 2022). The Indonesian model consequently moves beyond a purely consent-based approach by recognising several alternative legal bases for processing, including contractual necessity, legal obligations, vital interests, public interest, public-service functions, and legitimate interests. Singapore adopts a comparatively accountability-oriented structure through the Personal Data Protection Act 2012, with Sections 13–18 regulating consent and purpose limitation and Sections 21–26 addressing access, correction, protection, retention, and overseas transfers (Singapore Statutes Online, 2012). Malaysia's Personal Data Protection Act 2010 (Act 709) initially relied upon seven principles concerning general processing, notice and choice, disclosure, security, retention, data integrity, and access, while the 2024 amendment introduced further adjustments toward a controller-centred regulatory structure (Personal Data Protection Commissioner, 2010; Personal Data Protection Commissioner, 2024). These differences demonstrate that comparable regulatory objectives may be pursued through materially different statutory architectures.

Table 1. Comparative Regulatory Frameworks and Core Personal Data Protection Norms in Selected Southeast Asian Jurisdictions

Normative Element	Indonesia – UU No. 27/2022	Singapore – PDPA 2012	Malaysia – PDPA 2010 as amended 2024
Legal Basis	Article 20	Sections 13–17	Section 6
Consent	Articles 20–22	Sections 13–16	Section 6
Purpose Limitation	Article 20 and processing principles	Section 18	Section 7
Access and Correction	Articles 5–7	Sections 21–22	Section 12
Security	Controller obligations	Section 24	Section 9
Retention	Controller obligations	Section 25	Section 10
Breach Notification	Article 46	Sections 26A–26E	Amended framework
Cross-Border Transfer	Article 56	Section 26	Amended transfer requirements
Accountability	Controller and processor obligations	PDPC and organisational accountability	Commissioner and controller obligations

Table 1 demonstrates that regulatory convergence is relatively strong concerning consent, purpose limitation, security, access, and accountability, while divergence becomes more visible in lawful bases, institutional arrangements, enforcement, and cross-border governance. Indonesia's Article 20 adopts a pluralistic lawful-basis model, whereas Singapore's Sections 13–17 develop a more detailed consent and exception structure, creating different relationships between autonomy and legally authorised processing. Malaysia's principles-based structure places greater emphasis on organisational compliance with processing conditions, while its 2024 amendments indicate gradual movement toward contemporary controller-based terminology and responsibilities (Personal Data Protection Commissioner, 2024). The comparison indicates that statutory similarity cannot automatically be treated as substantive harmonisation because equivalent concepts may operate under different legal conditions and institutional mechanisms. ASEAN provides a common normative vocabulary for data protection, but domestic legislation remains decisive in determining the enforceability and practical

scope of individual rights (ASEAN, 2016). Regional harmonisation therefore requires compatibility between substantive obligations, supervisory structures, remedies, and enforcement standards rather than merely uniform legislative terminology.

The regulatory landscape becomes more differentiated when Thailand, the Philippines, Vietnam, and Brunei Darussalam are incorporated into the comparison. Thailand's Personal Data Protection Act B.E. 2562 (2019) establishes comprehensive rules concerning collection, use, disclosure, data-subject rights, controller and processor obligations, and regulatory supervision (Kingdom of Thailand, 2019). The Philippines' Republic Act No. 10173 of 2012 establishes transparency, legitimate purpose, proportionality, data-subject rights, and institutional responsibilities through the National Privacy Commission (Republic of the Philippines, 2012). Vietnam's Decree No. 13/2023/ND-CP establishes detailed classifications and processing requirements while integrating personal data governance into a broader state-centred digital regulatory structure (Government of Vietnam, 2023). Brunei Darussalam's Personal Data Protection Order 2025 represents a recent expansion of dedicated statutory protection within ASEAN and the continuing institutionalisation of personal data regulation (Brunei Darussalam, 2025). The different legislative trajectories demonstrate that ASEAN regulation does not follow a single statutory template, but reflects domestic adaptation of principles concerning lawful processing, individual rights, security, and accountability. This pattern is consistent with research identifying the interaction between global regulatory norms, particularly GDPR principles, and domestic legal innovation within ASEAN and Vietnam (Le et al., 2025). The resulting framework is therefore better characterised as regulatory diffusion accompanied by national adaptation rather than complete regional legal uniformity.

Cambodia, Laos, and Myanmar further demonstrate the uneven development of personal data governance within Southeast Asia. Cambodia's Law on E-Commerce 2019 provides rules concerning electronic transactions and information governance but does not reproduce the comprehensive architecture of newer standalone personal data protection statutes (Kingdom of Cambodia, 2019). Laos regulates electronic information through Law No. 25/NA of 2017 on Electronic Data Protection, establishing an earlier statutory foundation for electronic data protection (Lao People's Democratic Republic, 2017). Myanmar's Law Protecting the Privacy and Security of Citizens 2017 adopts a broader privacy and security orientation rather than the detailed controller-processor model increasingly found in dedicated data protection legislation (Republic of the Union of Myanmar, 2017). These differences affect the precision of lawful-processing requirements, data-subject rights, supervisory authority, enforcement, and available remedies. Comparative scholarship accordingly identifies fragmentation and differences in regulatory effectiveness as continuing challenges in Asia-Pacific personal data governance (Palupy et al., 2026). The regional architecture consequently encompasses a spectrum from comprehensive personal data protection statutes to broader electronic-data and privacy legislation, making uniform protection difficult to achieve through regional principles alone.

The comparative evidence establishes a pattern of functional convergence without complete normative uniformity, in which Southeast Asian jurisdictions increasingly recognise the need for lawful processing, security, accountability, individual control, and regulatory supervision while retaining different legal mechanisms for achieving those objectives. Indonesia's comprehensive rights-and-obligations model, Singapore's accountability-oriented framework, and Malaysia's principles-based system how different statutory structures can pursue partially equivalent regulatory functions (Sudarwanto & Kharisma, 2022). Thailand, the Philippines, Vietnam, and Brunei demonstrate more recent forms of statutory consolidation, whereas Cambodia, Laos, and Myanmar retain regulatory architectures with comparatively different degrees of comprehensiveness. The differences become particularly significant in relation to sensitive data, supervisory independence, breach notification, cross-border transfers, sanctions, and judicial or administrative remedies. These variations indicate that ASEAN harmonisation should prioritise substantive minimum safeguards rather than impose identical statutory formulations across jurisdictions. Such an approach is also consistent with scholarship emphasising that regional data protection requires legal harmonisation capable of accommodating national regulatory differences while strengthening individual privacy protection (bin Kirin & Ismail, 2025). A human-rights-oriented regional framework would therefore be better constructed around minimum enforceable standards of protection, accountability, and remedy while preserving the legislative autonomy of individual Southeast Asian states.

Personal Data Protection as a Human Rights Safeguard

Personal data protection has acquired a distinct human rights dimension because the processing of information concerning an identifiable person may affect privacy, autonomy, dignity, reputation, and the individual's capacity to control personal information. Article 21 of the ASEAN Human Rights Declaration recognises protection against arbitrary interference with privacy and personal information, establishing a regional normative connection between data protection and fundamental rights (ASEAN, 2012). The ASEAN Framework on Personal Data Protection further operationalises this orientation through principles concerning consent, notice, purpose limitation, data integrity, security, access, and accountability (ASEAN, 2016). These instruments indicate that the legality of personal data processing cannot be separated from protection against arbitrary or disproportionate informational interference. The central legal question is whether domestic legislation transforms regional principles into enforceable individual rights supported by institutional duties and effective remedies. The human rights character of data protection therefore depends not merely on recognising privacy as a legal value, but on establishing mechanisms through which individuals can exercise meaningful control over information concerning them.

The Indonesian framework provides an explicit statutory articulation of data-subject rights through Articles 5–15 of Law No. 27 of 2022 on Personal Data Protection (UU PDP), covering information, correction, access, termination of processing, deletion, withdrawal of consent, objection, restriction, compensation, and portability. Article 5 establishes the right to obtain information concerning the identity of the controller, legal basis, purpose, and accountability, while Articles 6 and 7 recognise correction and access rights (Republik Indonesia, 2022). Article 8 regulates termination of processing and deletion or destruction, Article 9 recognises withdrawal of consent, and Article 10 establishes an objection mechanism concerning decisions based solely on automated processing, including profiling, where legal or significant effects arise (Republik Indonesia, 2022). These provisions indicate a shift from passive privacy protection toward informational self-determination because the data subject is positioned as a legal actor capable of controlling subsequent uses of personal information. The statutory architecture also recognises that automated processing may affect autonomy and procedural fairness when significant decisions are generated without meaningful human intervention. The Indonesian model consequently provides a substantive benchmark for assessing whether comparable safeguards in other Southeast Asian jurisdictions provide equivalent protection in terms of rights, limitations, institutional duties, and remedies.

The Philippine Data Privacy Act of 2012 establishes a similarly developed rights architecture through Section 16, which recognises rights to be informed, access, correction, objection, suspension or withdrawal of processing, blocking or removal, and indemnification for damages arising from unlawful or inaccurate processing (Republic of the Philippines, 2012). Section 18 additionally recognises data portability, connecting informational autonomy with the individual's capacity to obtain and reuse electronically processed personal information (Republic of the Philippines, 2012). The Philippine framework is significant because privacy is constructed not merely as secrecy but as a collection of procedural entitlements enabling individuals to monitor, challenge, and correct processing activities. Section 21 further incorporates accountability into the governance of transfers, demonstrating that individual rights operate alongside organisational responsibilities rather than independently from them (Republic of the Philippines, 2012). Thailand adopts a comparable rights-based structure through Chapter III of the Personal Data Protection Act B.E. 2562 (2019), including access under Section 30 and related rights concerning correction, deletion, restriction, objection, and portability (Kingdom of Thailand, 2019). The comparative significance of these frameworks lies in the fact that formal recognition of similar rights does not necessarily establish equivalent protection because statutory exceptions, procedural requirements, enforcement authority, and available remedies may differ substantially.

Table 2. Comparative Human Rights Safeguards in Personal Data Protection Frameworks

Human Rights Safeguard	Indonesia – UU No. 27/2022	Philippines – RA No. 10173	Thailand – PDPA 2019	Human Rights Function
Right to information	Article 5	Section 16(a)–(b)	Sections 23 and related provisions	Transparency and informed autonomy
Right to correction	Article 6	Section 16(c)	Section 35	Accuracy and informational integrity
Right to access	Article 7	Section 16(d)	Section 30	Individual control and accountability
Right to deletion	Article 8	Section 16(e)	Section 33	Protection against unnecessary or unlawful retention
Withdrawal of consent	Article 9	Section 16(d)–(e)	Section 19	Autonomy over lawful processing
Objection	Article 10	Section 16(d)	Section 32	Protection against objectionable processing
Automated decision safeguards	Article 10	Section 16 and related rules	Related statutory safeguards	Procedural fairness
Compensation/remedy	Article 12	Section 16(f)	Civil and administrative remedies	Effective redress
Data portability	Article 13	Section 18	Section 31	Control and data mobility

Table 2 demonstrates that convergence exists in the recognition of access, correction, deletion, objection, and other mechanisms of individual control, while substantive differences remain in the conditions governing their exercise. Indonesia expressly incorporates safeguards against significant automated decision-making through Article 10, whereas the Philippine framework provides a broader collection of informational, objection, and remedial rights under Section 16 (Republic of the Philippines, 2012). Thailand similarly establishes individual rights subject to statutory conditions and exceptions, equivalent terminology does not necessarily produce equivalent legal protection (Kingdom of Thailand, 2019). The comparison supports a distinction between recognition of rights, conditions for exercising rights, and remedial enforceability as separate dimensions of human rights protection. Research comparing Indonesia and South Korea likewise demonstrates that the fulfilment of privacy rights should be evaluated through the effectiveness of legal mechanisms rather than through statutory recognition alone (Shahrullah et al., 2025). A rights-based assessment must therefore examine whether individuals possess realistic legal capacity to challenge unlawful processing and obtain meaningful redress when privacy interests are violated.

The human rights implications become more complex when personal data are differentiated according to sensitivity and potential consequences for the individual. Article 4 of the Indonesian UU PDP classifies health, biometric, genetic, criminal-record, child, and personal financial information as specific personal data requiring heightened protection (Republik Indonesia, 2022). Such differentiation reflects a proportionality-based rationale because the potential consequences of misuse may vary according to the nature and sensitivity of the information. Healthcare data this concern because unlawful disclosure or inaccurate processing may affect privacy, bodily integrity, employment, insurance, and access to healthcare simultaneously. Comparative research concerning Indonesia, Singapore, and the European Union demonstrates that patient data protection requires interaction between general data protection rules and sector-specific healthcare regulation (Kharisma & Diakanza, 2024). The doctrinal position becomes more complex when personal data are treated simultaneously as an element of individual personality and as an economic resource subject to commercial processing, because ownership-based approaches may inadequately capture the continuing relationship between information

and individual identity (Maharani et al., 2025). Consumer protection considerations further reinforce this issue because unequal bargaining positions may transform formal consent into a weak indicator of genuine autonomy where individuals have limited alternatives to providing personal information (Kadir et al., 2024). Human rights protection therefore requires a regulatory structure in which consent, necessity, proportionality, transparency, and accountability operate together rather than treating consent as the sole measure of lawful informational control.

The human rights dimension becomes particularly significant when personal data are used for profiling, automated decision-making, and artificial intelligence systems capable of producing substantial effects on individuals. Article 10 of the UU PDP establishes a right to object to decisions based solely on automated processing, including profiling, where such decisions have legal consequences or significant impacts on the data subject (Republik Indonesia, 2022). The development of artificial intelligence regulation reinforces the need to integrate data protection with algorithmic accountability, transparency, and responsible technological governance (Revolusi & Febriandy, 2025). Comparative research on the diffusion of GDPR principles demonstrates that European data protection norms have influenced Asian regulatory development while undergoing adaptation to domestic legal and institutional conditions (Bentotahewa et al., 2022). ASEAN's Guide on Data Anonymisation further demonstrates the regional need to reconcile legitimate data utilisation with protection against re-identification and associated privacy risks (ASEAN, 2025). The resulting legal framework should therefore protect not only against unlawful collection or disclosure but also against discriminatory, opaque, or disproportionate consequences generated from lawfully processed information. Human rights safeguards become substantively meaningful when privacy, autonomy, dignity, procedural fairness, and effective remedies operate as integrated legal criteria for evaluating the legitimacy of digital data governance.

Cross-Border Data Governance, Regulatory Fragmentation, and Emerging Digital Risks

The increasing cross-border circulation of personal data has transformed data protection from a predominantly domestic regulatory issue into a problem of transnational legal coordination, particularly as digital platforms, cloud services, financial technologies, healthcare systems, and artificial intelligence applications routinely process information across multiple jurisdictions. The ASEAN Framework on Digital Data Governance establishes principles concerning data lifecycle management, accountability, interoperability, and responsible data utilisation that are relevant to the governance of cross-border digital activities (ASEAN, 2018). The ASEAN Framework on Personal Data Protection similarly provides regional principles concerning data transfers, accountability, security, and individual protection, but leaves considerable discretion to member states in determining the legal conditions for international transfers (ASEAN, 2016). This institutional design creates a structural tension between the economic objective of facilitating regional data flows and the legal objective of ensuring that personal information remains subject to adequate safeguards after leaving the jurisdiction in which it was initially collected. Comparative research identifies the diffusion of privacy regulation across Southeast Asia as partly influenced by the extraterritorial reach and normative influence of the European Union's GDPR, although domestic jurisdictions have selectively adapted those principles according to their own regulatory priorities (Corning, 2024). The legal significance of cross-border transfer therefore lies not merely in whether data may leave national territory, but in whether the originating state's protection continues through contractual, organisational, regulatory, or jurisdictional mechanisms after the transfer occurs.

Indonesia addresses cross-border transfers through Article 56 of Law No. 27 of 2022 on Personal Data Protection, which establishes conditions concerning the adequacy of protection in the receiving country, appropriate safeguards, and, under specified circumstances, the consent or other legal basis necessary for transferring personal data outside Indonesia (Republik Indonesia, 2022). The provision reflects a conditional transfer model in which international data circulation is not prohibited as such, but is subjected to requirements designed to prevent the transfer from weakening the protection enjoyed by the data subject. Singapore adopts a comparable risk-based orientation through Section 26 of the Personal Data Protection Act 2012, which requires organisations transferring personal data outside Singapore to ensure a standard of protection comparable to that required under the domestic regime (Singapore Statutes Online, 2012). Malaysia also regulates international transfers through its statutory framework, while the 2024 amendments strengthen the contemporary governance structure

surrounding controllers and international processing activities (Personal Data Protection Commissioner, 2024). Thailand's Personal Data Protection Act similarly establishes requirements for transferring personal data to foreign jurisdictions and recognises conditions under which cross-border processing may be permitted (Kingdom of Thailand, 2019). These approaches demonstrate functional convergence around the principle that international transfer should not operate as a mechanism for circumventing domestic protection standards, although the specific tests, exemptions, and institutional mechanisms remain legally differentiated.

Table 3. Comparative Cross-Border Data Transfer and Digital Governance Safeguards in Selected ASEAN Jurisdictions

Regulatory Element	Indonesia	Singapore	Malaysia	Thailand
Principal Legal Basis	Article 56 UU PDP	Section 26 PDPA 2012	Cross-border transfer provisions under amended PDPA	PDPA 2019 transfer provisions
Transfer Principle	Adequacy, safeguards, or recognised legal basis	Comparable protection	Protection subject to statutory conditions	Adequacy and statutory safeguards
Accountability	Controller and processor obligations	Organisational accountability	Data controller obligations	Controller and processor obligations
Individual Protection	Rights under Articles 5–15	Access, correction, withdrawal and related rights	Seven principles and amended safeguards	Chapter III data-subject rights
Digital Governance Orientation	Personal data governance	Accountability-based governance	Principles-based governance	Comprehensive data governance
Principal Legal Concern	Protection after international transfer	Comparable overseas protection	Harmonisation following amendments	Conditions and exceptions for foreign transfer

Table 3 indicates that the jurisdictions share a fundamental concern that cross-border processing should remain subject to legally recognisable safeguards, but they differ in the mechanisms used to establish adequate protection. The Indonesian model places the assessment of the receiving jurisdiction and appropriate safeguards within a statutory transfer framework, whereas Singapore emphasises a comparable level of protection as an organisational obligation (Republik Indonesia, 2022). Malaysia's evolving framework how amendments can be used to adjust an established domestic regime to the demands of increasingly internationalised data processing (Personal Data Protection Commissioner, 2024). Thailand similarly integrates cross-border transfer into a comprehensive data protection statute rather than treating international movement as an isolated trade or telecommunications issue (Kingdom of Thailand, 2019). The absence of a single ASEAN-wide transfer mechanism, however, means that organisations operating regionally may face different compliance thresholds depending on the jurisdiction from which data originate and the destination to which they are transferred. Such fragmentation increases transaction costs and may simultaneously create regulatory uncertainty for controllers and uneven protection for data subjects. Regional harmonisation therefore requires more than recognition of cross-border transfers as a legitimate activity; it requires interoperable legal criteria concerning adequacy, safeguards, accountability, and remedies.

The regulatory challenge becomes more complex when cross-border data governance intersects with emerging technologies, particularly artificial intelligence, because the processing chain may involve multiple controllers, processors, jurisdictions, and computational infrastructures that are difficult to identify through conventional territorial regulation. Vietnam's Decree No. 13/2023/ND-CP on Personal Data Protection a regulatory response that places detailed obligations on entities involved

in personal data processing while linking data protection with broader state oversight of digital information (Government of Vietnam, 2023). Recent comparative research on GDPR development, ASEAN regulation, and AI governance in Vietnam demonstrates that emerging regulatory models increasingly combine global data protection principles with domestic approaches to technological governance (Le et al., 2025). Indonesia's developing AI regulatory agenda likewise indicates the need to coordinate personal data protection with principles concerning transparency, accountability, risk management, and responsible algorithmic deployment (Revolusi & Febriandy, 2025). The legal problem is intensified when AI systems rely on datasets obtained from several jurisdictions because the legality of collection, transfer, training, profiling, and subsequent inference may be governed by different regulatory standards. Comparative analysis of data governance frameworks in Asia further demonstrates that regulatory systems cannot be understood solely through the lens of protectionism because data governance also involves competing interests concerning innovation, economic integration, national sovereignty, and public-sector utilisation (Grover et al., 2024). Cross-border AI governance consequently requires an integrated legal approach capable of connecting personal data protection with accountability across the entire data-processing lifecycle.

An additional regulatory issue concerns anonymisation and the legal distinction between identifiable personal data and information that has been sufficiently transformed so that identification is no longer reasonably possible. The ASEAN Guide on Data Anonymisation provides regional guidance for managing anonymisation processes, reflecting the need to facilitate legitimate data utilisation while reducing risks associated with identification and re-identification (ASEAN, 2025). Anonymisation has particular significance for cross-border research, healthcare, artificial intelligence, and digital innovation because it may enable data use without exposing individuals to the same level of privacy risk associated with directly identifiable information. The legal difficulty arises because anonymisation cannot be assessed exclusively through the removal of obvious identifiers, as technological capabilities may permit information to be combined with external datasets to reconstruct individual identities. Cross-border processing intensifies this problem because the legal standard for determining whether information remains personal data may vary between jurisdictions, creating uncertainty concerning which safeguards continue to apply. Research on cross-border health data governance similarly identifies the tension between facilitating data flows and protecting human rights, particularly privacy, autonomy, and control over sensitive information (Xia et al., 2024). The legal treatment of anonymised information therefore requires a risk-sensitive approach that considers the possibility of re-identification, the context of processing, available technical safeguards, and the consequences for affected individuals.

The comparative assessment reveals that ASEAN's principal regulatory challenge is not the absence of data protection principles, but the fragmentation of legal mechanisms through which those principles operate across borders, sectors, and emerging technological environments. Regional instruments provide a foundation for interoperability, while national legislation determines the enforceable requirements applicable to controllers, processors, and data subjects within each jurisdiction (ASEAN, 2018). The resulting divergence may produce situations in which a data transfer is legally permissible in one jurisdiction but subject to substantially different conditions in another, complicating compliance and potentially creating uneven levels of human rights protection. Comparative research on Southeast Asian regulatory harmonisation similarly identifies legal fragmentation as a continuing obstacle to coherent regional personal data protection (bin Kirin & Ismail, 2025). The appropriate legal response is not necessarily the adoption of identical national legislation, but the development of compatible minimum standards concerning cross-border transfer, accountability, anonymisation, security, automated processing, and effective remedies. A regional framework based on substantive equivalence could preserve national regulatory autonomy while reducing conflicts between domestic data protection regimes and facilitating legitimate digital economic activity. Such an approach would also strengthen the human rights dimension of regional data governance by ensuring that the movement of information across borders does not result in the dilution of privacy, autonomy, dignity, and effective legal protection.

Regulatory Gaps, Enforcement, and the Prospect of ASEAN Legal Harmonisation

The comparative examination of Southeast Asian personal data protection regimes reveals that the principal weakness of the regional framework lies not in the absence of regulatory principles, but in

differences concerning institutional authority, enforcement capacity, sanctions, remedies, and the substantive consistency of statutory safeguards. ASEAN instruments provide a common normative foundation for privacy, personal data protection, and responsible digital governance, yet their framework-oriented character leaves domestic jurisdictions with substantial discretion in translating regional principles into binding obligations (ASEAN, 2016; ASEAN, 2018). This institutional arrangement permits regulatory innovation but also produces divergent legal thresholds concerning lawful processing, data-subject rights, breach notification, cross-border transfers, and accountability. Comparative scholarship identifies continuing fragmentation in Southeast Asian privacy regulation and indicates that efforts toward legal harmonisation remain constrained by differences in national legislative structures and regulatory priorities (bin Kirin & Ismail, 2025). The resulting legal problem is particularly significant for regional digital markets because data controllers operating across multiple jurisdictions must navigate potentially inconsistent obligations while individuals may receive different levels of protection depending on the location of processing. The question of harmonisation must therefore be assessed through substantive legal compatibility rather than through formal similarity between statutory provisions.

Indonesia's Law No. 27 of 2022 on Personal Data Protection establishes a relatively comprehensive enforcement architecture through provisions concerning administrative sanctions, criminal liability, compensation, and institutional responsibilities. Articles 57–58 regulate administrative sanctions and supervisory authority, while Articles 67–73 establish criminal provisions for unlawful acquisition, disclosure, use, falsification, and destruction of personal data (Republik Indonesia, 2022). Article 46 further requires notification following a personal data protection failure, establishing a procedural obligation intended to limit the consequences of data breaches and facilitate accountability. The availability of administrative and criminal sanctions demonstrates that Indonesian law does not treat personal data protection merely as a contractual relationship between controllers and data subjects, but as a matter involving public regulatory interests and legal accountability. The Philippine Data Privacy Act of 2012 similarly combines individual remedies with institutional enforcement through the National Privacy Commission and sanctions for unlawful processing, while Thailand's Personal Data Protection Act B.E. 2562 (2019) establishes civil, administrative, and criminal consequences for specified violations (Republic of the Philippines, 2012; Kingdom of Thailand, 2019). These models demonstrate a regional movement toward multidimensional enforcement, although differences in sanctioning powers and institutional arrangements continue to complicate the development of common regional standards.

Institutional accountability constitutes a separate dimension of harmonisation because substantive rights may have limited practical value where supervisory bodies lack sufficient authority, independence, resources, or jurisdictional reach. Singapore's PDPA establishes the Personal Data Protection Commission as a specialised regulatory institution responsible for administering and enforcing the statutory framework, while organisational accountability remains a central regulatory principle (Singapore Statutes Online, 2012). Malaysia's amended framework similarly strengthens the role of data controllers and regulatory oversight through the Personal Data Protection Commissioner, reflecting an institutional shift toward clearer allocation of responsibility within data-processing relationships (Personal Data Protection Commissioner, 2024). The Indonesian framework requires institutional arrangements capable of supervising controllers and processors, although the effectiveness of the regulatory architecture depends upon the operationalisation of the supervisory authority and its enforcement capacity under the statutory framework (Republik Indonesia, 2022). Comparative research indicates that differences in institutional design contribute materially to variations in the effectiveness of data protection regimes across the Asia-Pacific region (Palupy et al., 2026). A regional harmonisation strategy therefore requires attention not only to substantive statutory rights but also to minimum standards for supervisory independence, investigative powers, sanctioning authority, complaint procedures, and inter-agency cooperation.

Table 4. Comparative Regulatory Gaps and Harmonisation Priorities in Selected Southeast Asian Data Protection Regimes

Legal Dimension	Existing Regulatory Pattern	Principal Gap	Harmonisation Priority
Supervisory Authority	National regulators with different mandates	Unequal institutional powers	Minimum standards for independence and authority
Data-Subject Remedies	Access, correction, deletion, objection, compensation	Different procedures and enforcement routes	Regional minimum remedial standards
Breach Notification	Recognised in several comprehensive regimes	Different thresholds and procedures	Compatible notification requirements
Cross-Border Transfer	Adequacy and safeguard-based models	Divergent transfer conditions	Substantive equivalence mechanism
Sanctions	Administrative, civil, and criminal models	Different thresholds and severity	Proportionate minimum enforcement standards
Sensitive Data	Heightened protection in several jurisdictions	Different classifications	Common minimum sensitive-data safeguards
Automated Processing	Emerging statutory protection	Uneven AI-specific requirements	Algorithmic accountability principles
Anonymisation	Regional guidance and domestic practices	Divergent legal treatment	Common risk-based standards

Table 4 demonstrates that the most significant harmonisation challenges concern institutional and remedial compatibility rather than the complete absence of legal protection. The divergence in supervisory powers may create unequal enforcement outcomes even where national statutes recognise similar substantive rights. Differences in breach notification, cross-border transfer, sanctioning thresholds, and treatment of sensitive or anonymised information may also permit regulatory arbitrage in which processing activities are structured around jurisdictions presenting comparatively lower compliance burdens. The comparative literature on Indonesia, Malaysia, and Hong Kong demonstrates that differences in statutory construction can affect the practical operation of data protection even where the underlying objective of privacy protection is shared (Sudarwanto & Kharisma, 2022). Similar concerns emerge from comparative analysis of Indonesia and other ASEAN jurisdictions, which identifies legal fragmentation as a continuing obstacle to coherent regional privacy protection (Polii et al., 2025). Harmonisation should therefore focus on establishing a common substantive floor while allowing individual states to retain stricter domestic safeguards where those measures are compatible with regional digital integration.

The enforcement problem also has a significant human rights dimension because inadequate remedies may convert formally recognised privacy rights into rights that are difficult to exercise in practice. The ASEAN Human Rights Declaration establishes privacy protection as part of the regional human rights framework, meaning that data protection should be interpreted in connection with dignity, personal security, and protection against arbitrary interference rather than solely through commercial compliance (ASEAN, 2012). Effective remedies require accessible complaint mechanisms, meaningful investigative powers, proportionate sanctions, compensation for demonstrable harm, and procedures capable of addressing unlawful processing across organisational and jurisdictional boundaries. Comparative analysis of privacy rights in Indonesia and South Korea demonstrates the importance of examining whether legal systems provide mechanisms capable of translating statutory recognition into effective rights fulfilment (Shahrullah et al., 2025). Consumer protection scholarship similarly indicates that regulatory protection must address structural information asymmetries between individuals and organisations possessing superior technological and informational resources (Kadir et al., 2024). The legal significance of remedies consequently extends beyond compensation because effective redress performs preventive, corrective, and deterrent functions within the broader regulatory system. A harmonised ASEAN framework should therefore establish minimum standards for complaint handling,

administrative enforcement, compensation, and judicial review while preserving national procedural autonomy.

Emerging artificial intelligence systems create an additional harmonisation challenge because conventional data protection rules may not adequately address automated inference, profiling, secondary use, and algorithmic decision-making. Indonesia's Article 10 UU PDP establishes a specific right to object to decisions based solely on automated processing where legal or significant effects arise, providing a statutory entry point for algorithmic accountability (Republik Indonesia, 2022). Comparative policy research concerning AI regulation in Indonesia identifies the need for regulatory coordination between data protection, algorithmic governance, transparency, accountability, and risk management (Revolusi & Febriandy, 2025). Research on the normative influence of GDPR further indicates that external regulatory models can shape domestic legal development beyond their territorial boundaries, although national adaptation remains significant (Bentotahewa et al., 2022). The ASEAN Framework on Digital Data Governance provides a broader regional basis for responsible data utilisation, but its principles require further legal operationalisation if they are to address the specific risks associated with high-impact automated processing (ASEAN, 2018). The absence of fully harmonised regional standards concerning AI-generated profiling, automated decisions, and data-intensive technologies creates a potential gap between traditional privacy regulation and emerging forms of technological power. Regional harmonisation should therefore incorporate algorithmic accountability into the broader architecture of personal data protection rather than treating AI regulation as an entirely separate legal field.

The development of anonymisation standards provides another opportunity to reconcile data utilisation with individual protection within a harmonised regional framework. The ASEAN Guide on Data Anonymisation recognises the importance of technical and organisational measures for reducing identification risks while enabling legitimate data use in research, innovation, governance, and other activities (ASEAN, 2025). The legal challenge is that anonymisation may not permanently eliminate privacy risks where datasets can be combined with other information or subjected to increasingly sophisticated re-identification techniques. Cross-border health-data governance demonstrates the importance of maintaining human rights safeguards when sensitive datasets are transferred between jurisdictions for legitimate research or healthcare purposes (Xia et al., 2024). Regional standards should therefore adopt a risk-based interpretation of anonymisation that considers identifiability, technological capability, contextual risk, and the consequences of re-identification rather than relying exclusively on the removal of direct identifiers. Such an approach would complement existing principles of purpose limitation, security, proportionality, and accountability while facilitating responsible secondary use of information. The resulting framework could also provide a common reference point for controllers and processors operating across ASEAN jurisdictions where national definitions and treatment of anonymised information may otherwise differ.

The comparative legal analysis indicates that ASEAN harmonisation should be constructed around substantive equivalence, institutional interoperability, and enforceable human rights safeguards, rather than uniformity of legislative wording. Substantive equivalence would require member states to recognise minimum standards concerning lawful processing, data-subject rights, sensitive data, security, breach notification, cross-border transfers, automated decision-making, and remedies. Institutional interoperability would require mechanisms enabling supervisory authorities to exchange information, coordinate investigations, and cooperate in cross-border enforcement while respecting domestic jurisdictional boundaries. The importance of such compatibility is reinforced by comparative research demonstrating that ASEAN data protection systems are moving toward greater legal convergence but continue to exhibit significant differences in regulatory scope and institutional design (bin Kirin & Ismail, 2025). Regional digital governance also requires a balance between data protection and legitimate economic or technological objectives, particularly because excessive regulatory fragmentation can impede innovation while inadequate protection can undermine trust and individual rights (Grover et al., 2024). The appropriate model is therefore a regional minimum framework that establishes enforceable protection while permitting individual jurisdictions to adopt stronger safeguards according to domestic constitutional and human rights standards. This approach would strengthen ASEAN's capacity to govern personal data as both a component of digital economic integration and an essential dimension of individual dignity, autonomy, privacy, and legal security.

CONCLUSION

The comparative legal analysis demonstrates that personal data protection in Southeast Asia has developed through an interaction between ASEAN normative instruments and increasingly comprehensive domestic regulatory frameworks. Indonesia, Singapore, Malaysia, Thailand, the Philippines, Vietnam, Brunei Darussalam, Cambodia, Laos, and Myanmar have adopted different legal mechanisms for regulating personal data, producing convergence in fundamental principles while retaining substantial differences in statutory scope, institutional arrangements, enforcement mechanisms, and remedies. The ASEAN Human Rights Declaration, ASEAN Framework on Personal Data Protection, and ASEAN Framework on Digital Data Governance provide an important regional normative foundation, but their non-supranational character leaves the effective protection of individuals largely dependent upon domestic implementation. The comparison further establishes that personal data protection cannot be reduced to a matter of regulatory compliance because privacy, autonomy, dignity, informational self-determination, and effective remedies constitute interconnected human rights interests. Cross-border data transfers, sensitive information, anonymisation, automated decision-making, and artificial intelligence create additional regulatory pressures that expose the limitations of fragmented national approaches. The principal legal gap therefore concerns the absence of sufficiently interoperable regional standards capable of ensuring comparable substantive protection without requiring identical domestic legislation. ASEAN legal harmonisation should consequently be oriented toward substantive equivalence, institutional interoperability, and enforceable minimum safeguards that preserve national regulatory autonomy while preventing significant disparities in individual protection.

This study contributes theoretically by positioning personal data protection as a multidimensional legal institution situated at the intersection of privacy rights, human dignity, digital governance, consumer protection, technological accountability, and transnational regulatory cooperation. The comparative findings indicate that formal legislative convergence does not necessarily produce substantive convergence because equivalent concepts may operate through different legal bases, institutional structures, procedural requirements, and remedial mechanisms. A rights-oriented interpretation requires assessment not only of whether data-subject rights are formally recognised, but also of whether those rights are supported by enforceable obligations, independent supervision, proportionate sanctions, and accessible remedies. The study also demonstrates that cross-border data governance requires regulatory compatibility extending beyond transfer permissions to include security, accountability, anonymisation, automated processing, and continuing protection after information moves between jurisdictions. From a methodological perspective, the normative, doctrinal, and comparative approaches enable the systematic examination of statutory provisions, regional instruments, legal principles, and comparative scholarship across diverse Southeast Asian legal systems. The resulting analytical framework provides a basis for evaluating regulatory convergence through substantive safeguards rather than through legislative similarity alone. Future regulatory development should strengthen regional minimum standards while permitting domestic jurisdictions to maintain or establish higher levels of protection consistent with constitutional principles, human rights obligations, and legitimate digital-economy objectives.

REFERENCES

ASEAN. (2012). *ASEAN Human Rights Declaration*. Association of Southeast Asian Nations.

ASEAN. (2016). *ASEAN Framework on Personal Data Protection*. Association of Southeast Asian Nations.

ASEAN. (2018). *ASEAN Framework on Digital Data Governance*. Association of Southeast Asian Nations.

ASEAN. (2025). *ASEAN Guide on Data Anonymisation*. Association of Southeast Asian Nations.

Bentotahewa, V., Hewage, C., & Williams, J. (2022). The normative power of the GDPR: A case study of data protection laws of South Asian countries. *SN Computer Science*, *3*(3), 183. https://doi.org/10.1007/s42979-022-01079-z

bin Kirin, A., & Ismail, Y. C. T. (2025). Digital Privacy and Personal Data Protection in Southeast Asia: Challenges and Efforts toward Legal Harmonization. *Justitia Nova: Indonesian Journal of Modern Law*, *1*(1), 32-49. https://doi.org/10.5281/zenodo.21306986

Brunei Darussalam. (2025). *Personal Data Protection Order 2025*.

Corning, G. P. (2024). The diffusion of data privacy laws in Southeast Asia: learning and the extraterritorial reach of the EU's GDPR. *Contemporary Politics*, *30*(5), 656-677. https://doi.org/10.1080/13569775.2024.2310220

Government of Vietnam. (2023). *Decree No. 13/2023/ND-CP on personal data protection*.

Grover, R., Jang, K., & Su, L. W. (2024). Beyond digital protection (ism) comparing data governance frameworks in Asia. *Journal of Information Policy*, *14*, 161-193. https://doi.org/10.5325/jinfopoli.14.2024.0005

Kadir, M. Y. A., Arifin, M., Disantara, F. P., Thuong, M. T. H., & Nutako, B. S. M. (2024). The reform of consumer protection law: Comparison of Indonesia, Vietnam, and Ghana. *Jurnal Suara Hukum*, *6*(2), 255-278. https://doi.org/10.26740/jsh.v6n2.p255-278

Kharisma, D. B., & Diakanza, A. (2024). Patient personal data protection: comparing the health-care regulations in Indonesia, Singapore and the European Union. *International Journal of Human Rights in Healthcare*, *17*(2), 157-169. https://doi.org/10.1108/IJHRH-04-2022-0035

Kingdom of Cambodia. (2019). *Law on e-commerce*.

Kingdom of Thailand. (2019). *Personal Data Protection Act B.E. 2562 (2019)*.

Lao People's Democratic Republic. (2017). *Law on electronic data protection No. 25/NA*.

Le, C. T. Q., Tran, V. D., & Nguyen, D. P. T. (2025). Global norms and regional innovation: GDPR, evolution of data protection in ASEAN and the legal trajectory of AI in Vietnam. *TalTech Journal of European Studies*, *15*(3), 250-290. https://doi.org/10.2478/bjes-2025-0039

Maharani, D. P., Kusumadara, A., Widhiyanti, H. N., & Dewantara, R. (2025). Revisiting personal data: Ownership theories and comparative legal perspectives from Europe, Indonesia and the United States. *Journal of Data Protection & Privacy*, *7*(3), 274-291. https://doi.org/10.69554/ZMLG9061

Palupy, H. E., Nawing, R., & Susantijo, S. (2026). Personal Data Protection Governance in the Asia Pacific Region: A Review of the Scope, Effectiveness, and Legal Challenges. *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi, 9*(1). https://doi.org/10.24090/volksgeist.v9i1.15362

Personal Data Protection Commissioner. (2010). *Personal Data Protection Act 2010 (Act 709)*. Ministry of Digital Malaysia.

Personal Data Protection Commissioner. (2024). *Personal Data Protection (Amendment) Act 2024*. Ministry of Digital Malaysia.

Polii, V., Julius, D., & Banaya, C. L. (2025). Legal Protection of Personal Data Privacy in the Digital Era: A Comparative Study between Indonesia and ASEAN Countries. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *3*(2), 1194-1206. https://doi.org/10.51903/yjyvvy47

Republic of the Philippines. (2012). *Republic Act No. 10173: Data Privacy Act of 2012*. National Privacy Commission.

Republic of the Union of Myanmar. (2017). *Law protecting the privacy and security of citizens (Union Parliament Law No. 5/2017)*.

Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.

Revolusi, P., & Febriandy, R. K. (2025). Developing AI regulations in Indonesia: Policy recommendations based on comparative policy analysis from the European Union, the United States, and Singapore. *Jurnal Indonesia: Manajemen Informatika Dan Komunikasi*, *6*(2), 1035-1049. https://doi.org/10.63447/jimik.v6i2.1380

Shahrullah, R. S., Park, J., & Irwansyah, I. (2025). Examining personal data protection law of Indonesia and South Korea: The privacy rights fulfilment. *Hasanuddin Law Review*, *10*(1), 1-20. https://doi.org/10.20956/halrev.v10i1.5016

Singapore Statutes Online. (2012). *Personal Data Protection Act 2012*. Attorney-General's Chambers.

Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, *29*(4), 1443-1457. https://doi.org/10.1108/JFC-09-2021-0193

Xia, L., Cao, Z., & Zhao, Y. (2024). Paradigm transformation of global health data regulation: challenges in governance and human rights protection of cross-border data flows. *Risk Management and Healthcare Policy*, 3291-3304. https://doi.org/10.2147/RMHP.S450082