



Personal Data Governance in ASEAN Digital Public Services: A Comparative Analysis

**Fitrahtul Saahira Khairunnisa^{1*}, Mufidah binti Mastor², Khodijah Asshofiah³, Maryam⁴,
Desilva D. R. U.⁵**

^{1, 3, 4} Universitas Islam Negeri Raden Mas Said Surakarta, Indonesia

² Al Azhar University, Egypt

⁵ Nāgānanda International Institute for Buddhist Studies, Sri Lanka

Email: saahirafitrahul@gmail.com¹

Article Info :

Received:

18-09-2026

Revised:

14-10-2026

Accepted:

20-10-2026

Abstract

Cross-border and interoperable digital public services increasingly depend on personal-data exchange across agencies, vendors, and jurisdictions. This study compared the legal and operational governance architecture relevant to digital public services in seven ASEAN jurisdictions with overarching personal-data instruments in force by August 2026: Brunei Darussalam, Indonesia, Malaysia, the Philippines, Singapore, Thailand, and Vietnam. A comparative doctrinal method examined national legislation alongside ASEAN frameworks on personal data protection, data management, contractual clauses, anonymisation, and digital integration. The analysis found convergence around notice, security, accountability, individual rights, and cross-border safeguards, but material differences remained in statutory scope, public-sector application, supervisory arrangements, breach processes, and transfer mechanisms. Regional instruments supplied useful interoperability tools without replacing national law. The study developed a non-ranking governance workflow linking lawful basis, role allocation, data mapping, risk assessment, security, transfer controls, rights handling, incident response, and audit. The findings indicated that digital public-service interoperability depends less on identical statutes than on demonstrable operational equivalence and traceable accountability across the full data lifecycle.

Keywords: ASEAN, data governance, digital public services, personal data protection, cross-border data.



©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

Digital public services increasingly operate through shared identity systems, cloud infrastructure, interoperable registries, outsourced platforms, and cross-agency data exchange. These arrangements can reduce administrative duplication and improve service continuity, but they also increase the number of actors able to collect, infer, transfer, or retain personal data. The governance problem is therefore wider than cybersecurity: public institutions must establish lawful authority, purpose boundaries, role allocation, data minimization, security, individual-rights procedures, and accountability throughout the lifecycle of information. The World Bank (2021) frames data as a development asset whose value depends on trust and safeguards, while NIST (2020) emphasizes privacy-risk management as an organizational process rather than a one-time compliance exercise. ISO/IEC 27701 (2019) provides a complementary management-system approach by extending information-security controls to privacy information management. These perspectives are especially relevant to ASEAN, where service interoperability can involve multiple legal regimes within one transactional chain.

ASEAN has developed a layered regional architecture rather than a single supranational data-protection statute. The ASEAN Framework on Personal Data Protection established common principles for consent, purpose, security, access and correction, transfers, retention, and accountability (ASEAN, 2016). The Framework on Digital Data Governance later connected trusted data flows with economic and digital integration (ASEAN, 2018). In 2021, the ASEAN Data Management Framework translated governance into organizational practices, while the ASEAN Model Contractual Clauses offered a voluntary tool for cross-border transfers (ASEAN, 2021a; ASEAN, 2021b). These instruments are significant because they create common vocabulary and operational templates across different national systems. They do not, however, displace domestic statutory requirements, a point that becomes

important when a public-service workflow uses a regional vendor or transfers information to another member state.

Regional guidance has continued to evolve. The Joint Guide to ASEAN Model Contractual Clauses and European Union Standard Contractual Clauses describes practical commonalities between the two contractual systems and illustrates how organizations may operationalize safeguards across regions (ASEAN Secretariat & European Commission, 2024). The ASEAN Guide on Data Anonymisation provides technical guidance for reducing identifiability in structured datasets and explicitly positions anonymisation as part of wider governance controls (ASEAN, 2025a). ASEAN also published a joint guide linking its contractual clauses with those of the Ibero-American Data Protection Network, extending the interoperability discussion beyond Southeast Asia (ASEAN, 2025b). The ASEAN Digital Masterplan 2030 places trusted cross-border data flows, privacy-enhancing technologies, digital identity interoperability, and regional cooperation within the next phase of digital integration (ASEAN, 2026). The trajectory shows a shift from principles toward implementation tools, which is particularly relevant for operational public services.

National law has also changed materially since the first regional framework. Indonesia enacted Law No. 27 of 2022 on Personal Data Protection, establishing rights, controller and processor obligations, transfer requirements, and an institutional mandate for supervision (Republic of Indonesia, 2022). Malaysia's Personal Data Protection Act 2010 remains the foundation for commercial-sector processing and was amended through the Personal Data Protection (Amendment) Act 2024, followed by implementation guidance including cross-border transfer rules (Malaysia, 2010; Malaysia, 2024). The Philippines has operated under Republic Act No. 10173 since 2012, Singapore under its Personal Data Protection Act 2012, and Thailand under the Personal Data Protection Act B.E. 2562 (2019) (Republic of the Philippines, 2012; Singapore, 2012; Thailand, 2019). These instruments share recognizable data-protection concepts but differ in statutory scope and public-sector treatment.

Two developments make a 2026 comparison necessary. Brunei Darussalam adopted the Personal Data Protection Order 2025 and brought it into force on 1 January 2026, adding another omnibus framework to the regional landscape (Brunei Darussalam, 2025). Vietnam enacted Law No. 91/2025/QH15 on Personal Data Protection, effective from 1 January 2026, replacing a governance environment that had previously relied heavily on Decree No. 13/2023 and sectoral rules (Vietnam National Assembly, 2025). Scholarship written before these changes can therefore understate the present level of statutory convergence. Recent comparative research has nevertheless identified continuing variation in rights, enforcement design, and transfer rules among ASEAN jurisdictions (Sholehuddin et al., 2024; Sukerta & Sutrisno, 2024). Safitri and Mahfud (2023) specifically examine the interaction between Indonesia's legislation and ASEAN cross-border instruments, while Aurelia and Lewiandy (2025) describe continuing harmonization challenges around transfer regulation.

The legal-policy literature also shows why formal similarity should not be confused with operational interoperability. Greenleaf (2021) critiques ambiguities in the ASEAN Model Contractual Clauses and questions the extent to which voluntary clauses alone can resolve differences in national protection. Cai (2026) identifies comparable tensions in ASEAN consumer data protection for e-commerce, where national law remains central to cross-border compliance. Gellert (2018) demonstrates that risk-based data-protection concepts require concrete methods for translating legal standards into organizational decisions, while Bradford (2020) explains how regulatory standards can influence practices beyond their territory through market and compliance effects. The GDPR remains an important external reference for transfer and accountability architecture, but comparative analysis should not assume that ASEAN systems are intended to reproduce the European model (European Union, 2016; Kuner et al., 2020). The research need is an applied description of how diverse legal rules can be assembled into a common governance workflow for digital public services without ranking national systems.

This study therefore compared the legal architecture relevant to digital public-service data governance in seven ASEAN jurisdictions with overarching personal-data instruments in force by 31 August 2026. It asked three questions: which governance components show clear regional convergence; where do legally meaningful differences remain; and which operational controls can support interoperable services despite those differences. The analysis was deliberately non-ranking. It did not assign country scores or identify a preferred national model because statutory design reflects different constitutional, administrative, and institutional arrangements. Instead, the study developed a descriptive

comparison and a minimum operational workflow that can help public agencies and service providers trace lawful authority, accountability, transfers, rights, and incidents across jurisdictional boundaries. OECD (2026) similarly treats cross-border data governance in ASEAN as an interoperability problem in which legal certainty and trusted flows must be considered together.

RESEARCH METHODS

The research used comparative doctrinal and institutional analysis. The jurisdictional sample consisted of Brunei Darussalam, Indonesia, Malaysia, the Philippines, Singapore, Thailand, and Vietnam because each had an overarching personal-data instrument in force by 31 August 2026. The primary legal corpus comprised Brunei's Personal Data Protection Order 2025, Indonesia's Law No. 27 of 2022, Malaysia's Personal Data Protection Act 2010 as amended in 2024, the Philippines' Data Privacy Act of 2012, Singapore's Personal Data Protection Act 2012, Thailand's Personal Data Protection Act 2019, and Vietnam's Law No. 91/2025/QH15 (Brunei Darussalam, 2025; Republic of Indonesia, 2022; Malaysia, 2010; Malaysia, 2024; Republic of the Philippines, 2012; Singapore, 2012; Thailand, 2019; Vietnam National Assembly, 2025). The comparison focused on rules materially relevant to public digital-service data flows rather than attempting an article-by-article restatement of each statute.

A structured coding frame captured statutory scope, controller or responsible-organization concepts, lawful or permitted processing bases, individual rights, security obligations, incident or breach processes, supervisory arrangements, and cross-border transfer mechanisms. Where public bodies were regulated through separate regimes or exclusions, the analysis recorded that institutional fact rather than converting it into a positive or negative score. Regional instruments were coded separately as soft-law or interoperability tools: the ASEAN personal-data framework, digital-data-governance framework, data-management framework, model contractual clauses, anonymisation guide, joint contractual-clause guides, and the Digital Masterplan 2030 (ASEAN, 2016; ASEAN, 2018; ASEAN, 2021a; ASEAN, 2021b; ASEAN Secretariat & European Commission, 2024; ASEAN, 2025a; ASEAN, 2025b; ASEAN, 2026). The European Union's GDPR was used only as an external reference point for concepts such as accountability and transfer safeguards, not as a benchmark for ranking ASEAN law (European Union, 2016).

The applied phase translated the doctrinal comparison into a lifecycle workflow for digital public services. Controls were grouped into nine stages: legal authority and purpose definition; data inventory and role allocation; necessity and minimization; risk assessment; security and access control; vendor and transfer safeguards; individual-rights handling; incident response; and documentation, audit, and deletion. The workflow was informed by NIST's Privacy Framework, ISO/IEC 27701, and the ASEAN Data Management Framework because these instruments provide operational vocabulary that can connect legal duties with system design (NIST, 2020; ISO/IEC 27701, 2019; ASEAN, 2021a). The analysis also drew on comparative scholarship to identify areas where formal clauses may require additional institutional interpretation (Greenleaf, 2021; Gellert, 2018; Kuner et al., 2020).

The study was limited to publicly available legal and policy materials and did not measure enforcement intensity, case outcomes, agency staffing, or actual compliance rates. National implementing rules can change more quickly than primary statutes, and the new Brunei and Vietnam frameworks have limited post-commencement case experience. Findings are therefore descriptive of formal governance architecture and operational implications as of the stated cutoff date. The method is appropriate for applied comparative legal research because it preserves jurisdictional differences while identifying process steps that can be implemented across institutional settings. It also avoids converting contested policy choices into a country league table, which would obscure the legal context needed to understand why similar concepts operate differently.

RESULTS AND DISCUSSION

Convergence and divergence in national and regional governance architecture

The comparative analysis shows broad convergence around the idea that personal-data processing requires defined purposes, organizational responsibility, reasonable security, and mechanisms through which individuals can exercise recognized rights. Table 1 summarizes the principal statutory architecture without assigning scores. Singapore, Malaysia, the Philippines, Thailand, Indonesia, Vietnam, and Brunei all use an overarching instrument, but the relationship between that instrument and

public-sector processing differs. Malaysia's base statute is expressly centered on personal data in commercial transactions, while other jurisdictions organize public and private obligations differently through statutory scope, exclusions, or associated public-law rules (Malaysia, 2010). These distinctions matter for digital public services because a single technical platform can involve a ministry, state-owned entity, private cloud provider, identity vendor, and cross-border processor, each potentially governed by a different legal pathway.

Table 1. Descriptive Personal-Data Architecture in Seven ASEAN Jurisdictions

Jurisdiction	Principal overarching instrument in force by Aug. 2026	Scope note relevant to public services
Brunei Darussalam	Personal Data Protection Order 2025	Organization-focused framework; public-service applicability requires instrument-specific analysis
Indonesia	Law No. 27 of 2022	General personal-data law with controller/processor duties and institutional provisions
Malaysia	PDPA 2010, amended 2024	Centered on processing in commercial transactions; public-sector arrangements require separate legal mapping
Philippines	Data Privacy Act 2012	General privacy framework administered by the National Privacy Commission
Singapore	Personal Data Protection Act 2012	Private-sector PDPA operates alongside separate public-sector governance
Thailand	Personal Data Protection Act 2019	General framework with statutory exceptions and sector-specific interactions
Vietnam	Law No. 91/2025/QH15	Personal-data protection law effective 1 January 2026

Source: National legislation and official legal publications.

Individual-rights architecture is one area of visible convergence, although the wording and conditions vary. Access and correction rights are common features, while newer frameworks also articulate deletion, objection, consent withdrawal, portability, or related controls in different forms. Indonesia's Law No. 27 of 2022 sets out data-subject rights and establishes corresponding controller responsibilities (Republic of Indonesia, 2022). Vietnam's Law No. 91/2025/QH15, in force from January 2026, expressly regulates personal-data protection and enumerates core rights including knowledge, consent, access, correction, and deletion (Vietnam National Assembly, 2025). Comparative scholarship confirms that rights categories increasingly resemble one another across selected ASEAN states even though procedures, exceptions, and institutional remedies remain nationally specific (Sholehuddin et al., 2024; Sukerta & Sutrisno, 2024).

Accountability and organizational-role concepts also show convergence. Contemporary regimes increasingly distinguish the entity that determines processing purposes from service providers that process data on its behalf, even when domestic terminology is not identical. This distinction is

operationally important for public procurement because contracts must allocate instructions, security responsibilities, subprocesses, deletion obligations, and assistance with rights or incidents. The ASEAN Data Management Framework encourages organizations to define governance roles and manage data through its lifecycle, providing a regional operational layer that can sit beneath diverse statutes (ASEAN, 2021a). ISO/IEC 27701 (2019) offers a similar management-system logic, linking privacy roles to policies, risk treatment, and documented controls. The result is a strong basis for role mapping across service chains even when legal labels differ.

Cross-border transfer rules remain a principal area of legal variation. Some jurisdictions use adequacy-like concepts, contractual safeguards, consent exceptions, certification or comparable mechanisms, while the exact statutory triggers and permitted derogations differ. The ASEAN Model Contractual Clauses were designed as a voluntary transfer tool that organizations can incorporate into commercial contracts, and the 2024 ASEAN–EU joint guide identifies commonalities and practical use patterns across the ASEAN MCCs and EU SCCs (ASEAN, 2021b; ASEAN Secretariat & European Commission, 2024). Greenleaf (2021) argues that the voluntary and uneven legal basis of the ASEAN clauses creates limits that must be understood rather than assumed away. Safitri and Mahfud (2023) likewise show that domestic transfer rules remain decisive when the ASEAN clauses are used. Digital public services therefore need a transfer inventory that identifies both the regional tool and the national legal basis for each outbound flow.

Malaysia illustrates how a national framework can evolve while retaining its original statutory foundation. The Personal Data Protection (Amendment) Act 2024 modified the 2010 regime, and subsequent regulator guidance addressed cross-border transfers, data breach notification, data-protection officers, and other implementation issues (Malaysia, 2024). The change is relevant to regional interoperability because organizations cannot rely on an old description of the Malaysian regime when designing 2026 service contracts. OECD (2026) notes that Malaysia’s current cross-border approach allows safeguards such as contractual clauses and explicitly recognizes international models as possible compliance tools. This example supports a broader methodological finding: comparative maps must be date-specific, especially where amendment acts and guidance materially change operational obligations without replacing the title of the original statute.

Brunei and Vietnam change the regional baseline in another way. Brunei’s Personal Data Protection Order 2025 was commenced from 1 January 2026, bringing a new omnibus instrument into operation after years in which regional comparisons often described Brunei as lacking such a law (Brunei Darussalam, 2025). Vietnam’s Law No. 91/2025/QH15 also became effective on 1 January 2026 and now provides the central statutory basis for personal-data protection (Vietnam National Assembly, 2025). Older ASEAN comparison tables can therefore be factually outdated even when their analysis was accurate at publication. Cai (2026) demonstrates this moving target in the consumer-data field, where regional e-commerce integration interacts with national reforms. For public-service designers, version control of legal inventories should be treated as a governance control rather than as a research housekeeping task.

The regional instruments provide increasing operational detail but retain a different legal character from national legislation. The 2016 framework sets common principles; the 2018 digital-data framework connects trust with data flows; the 2021 management framework and contractual clauses provide organizational tools; the 2025 anonymisation guide adds a technical privacy measure; and the 2030 masterplan places trusted data flows and privacy-enhancing technologies within ASEAN’s digital integration agenda (ASEAN, 2016; ASEAN, 2018; ASEAN, 2025a; ASEAN, 2026). Figure 1 shows this progression as a timeline rather than a hierarchy. The sequence suggests that ASEAN interoperability is being built through layered guidance and coordination. It should not be read as legal unification because national statutes continue to determine enforceable duties within each jurisdiction.

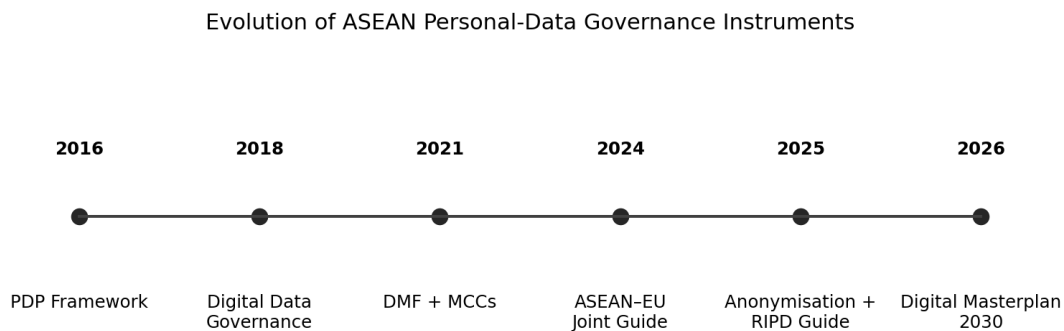


Figure 1. Evolution of ASEAN Personal-Data Governance Instruments

The comparison also demonstrates why public-sector scope deserves explicit treatment in procurement and system architecture. A private contractor may be directly subject to an omnibus data-protection statute even where the commissioning public body operates under separate administrative, secrecy, archival, or sector-specific rules. The legal relationship between the two actors can therefore be asymmetrical. A contract that merely states that all parties will 'comply with applicable law' may fail to specify which actor handles access requests, who notifies incidents, where data may be hosted, or how subcontractors are approved. Bradford (2020) shows how regulatory requirements can propagate through cross-border commercial relationships, but operational clarity still depends on contractual translation. The descriptive national matrix is most useful when paired with a transaction-level role map for each service.

The principal finding from the doctrinal comparison is not that ASEAN systems are becoming identical. It is that a recognizable common governance vocabulary now exists across national law and regional guidance, while important institutional differences persist around scope, supervision, transfers, and public-sector application. Aurelia and Lewiandy (2025) similarly identify harmonization challenges in cross-border transfer regulation, and Sholehuddin et al. (2024) document variation across selected national laws. These differences do not prevent interoperability, but they require explicit legal mapping. A digital public service that assumes equivalence without documenting it creates avoidable compliance risk; a service that identifies the applicable regime, processing role, transfer basis, and rights procedure can operate across different legal architectures with clearer accountability.

An operational governance workflow for interoperable digital public services

The first stage of the proposed workflow is to document legal authority, public-service purpose, and the categories of data genuinely required to deliver the service. Purpose definition limits function creep and creates the reference point against which later reuse can be assessed. Data minimization should be applied at field level rather than only at database level: each identifier, attribute, and derived variable should have an operational justification. The ASEAN Framework on Personal Data Protection and GDPR both link processing legitimacy to purpose and accountability, although they do so through different legal systems (ASEAN, 2016; European Union, 2016). A public-service project should record these decisions before procurement or software configuration because retrofitting purpose limitations after systems are integrated is technically and institutionally harder.

The second stage is data and role mapping. Every dataset should be linked to a source, responsible agency, service provider, storage location, retention rule, recipient category, and cross-border transfer route. This map converts abstract legal obligations into system architecture and makes dependencies visible. The ASEAN Data Management Framework provides a practical foundation for such lifecycle governance, while NIST (2020) treats inventory and processing awareness as core privacy-risk management activities (ASEAN, 2021a). In multi-agency services, role mapping should also identify who answers an individual request, who can authorize data correction, who controls access logs, and who can instruct a processor. Without this mapping, responsibility tends to diffuse precisely when an incident or rights request requires a rapid decision.

The third stage is a documented privacy and security risk assessment proportionate to the sensitivity, scale, and consequences of processing. Gellert (2018) explains that risk under data-

protection law is not self-executing; organizations need methods that connect legal concepts with identifiable harms and controls. High-risk public-service functions can include biometric identity, health data, child data, large-scale behavioral profiles, automated eligibility decisions, or linkage across previously separate registers. The assessment should examine necessity, foreseeable misuse, discriminatory error, re-identification, unauthorized disclosure, and service exclusion. Risk treatment then connects legal review to technical choices such as access segmentation, encryption, logging, pseudonymisation, or reduced retention. This stage is where privacy engineering and administrative-law accountability should meet.

The fourth stage is to select technical and organizational safeguards that are traceable to the identified risks. ISO/IEC 27701 (2019) is useful because it embeds privacy controls within a management system and encourages evidence of implementation rather than policy statements alone. The ASEAN Guide on Data Anonymisation adds a specific option for datasets that can support analytics or inter-agency planning without retaining direct identifiability (ASEAN, 2025a). Anonymisation should not be treated as a label applied after removing names; the guide emphasizes a process that considers structured data, technique selection, and re-identification risk. For public services, the most defensible architecture may combine role-based access, pseudonymisation for operational workflows, and stronger anonymisation for secondary statistical use where individual identification is unnecessary.

The fifth stage addresses vendors and cross-border transfers. Contracts should specify processing instructions, confidentiality, security measures, subcontracting, assistance with individual rights, breach cooperation, return or deletion, audit evidence, and the legal mechanism for any international transfer. The ASEAN MCCs can provide standardized transfer clauses, while the joint ASEAN–EU and ASEAN–RIPD guides improve interpretive interoperability across contractual systems (ASEAN, 2021b; ASEAN Secretariat & European Commission, 2024; ASEAN, 2025b). Kuner et al. (2020) emphasize that international transfer compliance depends on the interaction between contractual mechanisms and the surrounding legal environment. Public agencies should therefore avoid treating a model clause as a complete transfer assessment; the clause is one component of documented due diligence.

The sixth stage is rights and service-redress design. Rights are effective only if people can discover the relevant process, authenticate themselves without excessive burden, receive a response within applicable requirements, and challenge inaccurate or inappropriate processing. A digital portal should therefore include an accessible channel for data access, correction, objection or other applicable rights, while preserving alternatives for people who cannot use online authentication. Sukerta and Sutrisno (2024) and Sholehuddin et al. (2024) show that rights and enforcement structures vary across national laws, which means a regional service may need jurisdiction-specific routing behind a common user interface. The legal diversity can be hidden from users only if the service operator has mapped it accurately internally.

The seventh stage is incident response and breach governance. The plan should identify technical containment roles, legal-notification triggers, affected-person communication procedures, evidence preservation, vendor escalation, and post-incident review. Malaysia's amended framework and associated guidance illustrate the increasing regional attention to breach-notification processes (Malaysia, 2024). Indonesia's statute assigns controllers obligations related to failures of personal-data protection and establishes an institutional enforcement architecture, while the practical supervisory environment continues to develop (Republic of Indonesia, 2022). An interoperable service should use the shortest applicable internal escalation time across participating actors because waiting to determine jurisdiction after an incident can consume the period needed for legally required notification. Figure 2 summarizes the full governance flow.

Cross-Border Digital Public-Service Governance Workflow



Figure 2. Cross-Border Digital Public-Service Governance Workflow

The eighth stage is accountability through documentation and audit. Logs should show who accessed high-risk data, which transfers occurred, whether retention limits were applied, and how complaints or rights requests were resolved. Documentation also supports continuity when vendors or officials change. The Digital Masterplan 2030 emphasizes trusted data ecosystems and cross-border cooperation, which increases the importance of demonstrable governance rather than informal institutional knowledge (ASEAN, 2026). OECD (2026) likewise links cross-border data flows with regulatory interoperability and certainty. Table 2 converts the workflow into an applied control register that can be attached to project governance, procurement, or assurance processes without presuming a single ASEAN legal model.

Table 2. Operational Control Register for Interoperable Digital Public Services

Governance stage	Minimum evidence	documented	Primary operational question
Authority and purpose	Legal basis; service mandate; purpose statement		Why is each data element processed?
Data and roles	Data controller/processor equivalent map	inventory; or	Who decides and who acts?
Risk assessment	Privacy/security impact record		What harm could arise and to whom?
Security	Access model; encryption; logs; retention		How are risks reduced and evidenced?
Transfers/vendors	Transfer basis; clauses; subprocessors; hosting map		Where does data move and under which rules?
Rights/redress	Request workflow; identity checks; escalation		How can individuals exercise applicable rights?
Incidents	Breach plan; contact tree; notification analysis		Who acts within the first hours?
Audit/deletion	Review logs; deletion evidence; contract exit plan		Can compliance be demonstrated over time?

Source: Authors' synthesis of ASEAN, national, NIST, and ISO governance materials.

This operational model has limitations and should not be mistaken for jurisdiction-specific legal advice. It does not resolve conflicts of law, sectoral secrecy duties, national-security exceptions, evidence rules, archival requirements, or specialized health and financial regulations. It also cannot substitute for regulatory guidance issued after the study cutoff. Its value lies in providing a traceable sequence that allows public agencies to identify where national differences must be resolved before data moves. The comparative evidence supports a practical proposition: ASEAN digital public-service

interoperability can be built through documented equivalence of controls even when legislation is not textually uniform. Regional frameworks supply common tools, while national law continues to determine legal authority and enforceable duties in each participating jurisdiction.

CONCLUSION

ASEAN personal-data governance has moved toward greater statutory and operational convergence, particularly through new national laws in Brunei and Vietnam and through regional instruments on data management, contractual transfers, anonymisation, and digital integration. The seven jurisdictions examined share a substantial vocabulary of purpose, security, accountability, individual rights, and transfer safeguards, yet meaningful differences remain in public-sector scope, institutional oversight, breach procedures, and legal mechanisms for cross-border processing. Regional instruments facilitate interoperability but do not replace national law.

For digital public services, the most useful response to legal diversity is a documented lifecycle that links legal authority and purpose to data mapping, risk assessment, safeguards, transfer controls, rights handling, incident response, and audit. Future research should update the comparison as the new Brunei and Vietnam regimes generate implementation practice and should examine sector-specific service chains using real procurement and data-flow documentation. Such work can test whether operational equivalence is sufficient to sustain trusted interoperability across agencies and jurisdictions.

REFERENCES

- ASEAN Secretariat, & European Commission. (2024). Joint guide to ASEAN model contractual clauses and EU standard contractual clauses. ASEAN Secretariat.
- ASEAN. (2016). ASEAN framework on personal data protection. ASEAN Secretariat.
- ASEAN. (2018). Framework on digital data governance. ASEAN Secretariat.
- ASEAN. (2021a). ASEAN data management framework. ASEAN Secretariat.
- ASEAN. (2021b). ASEAN model contractual clauses for cross border data flows. ASEAN Secretariat.
- ASEAN. (2025a). ASEAN guide on data anonymisation. ASEAN Secretariat.
- ASEAN. (2025b). Joint guide to ASEAN MCCs and Ibero-American Data Protection Network MCCs. ASEAN Secretariat.
- ASEAN. (2026). ASEAN digital masterplan 2030. ASEAN Secretariat.
- Aurelia, J., & Lewiandy. (2025). The challenge of harmonizing cross-border data transfer regulations among ASEAN member states. *Kertha Semaya: Journal Ilmu Hukum*, 13(3), 287–300. <https://doi.org/10.24843/KS.2025.v13.i03.p01>
- Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.
- Brunei Darussalam. (2025). Personal Data Protection Order, 2025.
- Cai, Q. (2026). ASEAN consumer data protection in e-commerce. *Journal of Consumer Policy*. <https://doi.org/10.1007/s10603-026-09630-8>
- European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1–88.
- Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, 34(2), 279–288. <https://doi.org/10.1016/j.clsr.2017.12.003>
- Greenleaf, G. (2021). ASEAN model contractual clauses: Low and ambiguous data privacy standards. *Privacy Laws & Business International Report*, 174, 22–24. <https://doi.org/10.2139/ssrn.4027670>
- International Organization for Standardization. (2019). ISO/IEC 27701:2019 security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management.
- Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.
- Malaysia. (2010). Personal Data Protection Act 2010 (Act 709).
- Malaysia. (2024). Personal Data Protection (Amendment) Act 2024 (Act A1727).
- National Institute of Standards and Technology. (2020). NIST privacy framework: A tool for improving privacy through enterprise risk management, Version 1.0. U.S. Department of Commerce.
- OECD. (2026). Digital trade review of the Association of Southeast Asian Nations: Maximising the benefits of cross-border data flow regulation. OECD Publishing.
- Republic of Indonesia. (2022). Law No. 27 of 2022 concerning personal data protection.

- Republic of the Philippines. (2012). Republic Act No. 10173: Data Privacy Act of 2012.
- Safitri, M. Y., & Mahfud, M. (2023). The ASEAN cross-border personal data transfer instrument: Has Indonesia's personal data protection law followed it? *Jurnal Magister Hukum Udayana*, 12(3), 553–564. <https://doi.org/10.24843/JMHU.2023.v12.i03.p06>
- Sholehuddin, N., Miskam, S., Mohd Shahwahid, F., Raja Abdul Aziz, T. N., & Mansor, N. (2024). A comparative legal analysis on personal data protection laws in selected ASEAN countries. *Journal of Muwafaqat*, 7(1), 23–38. <https://doi.org/10.53840/muwafaqat.v7i1.166>
- Singapore. (2012). Personal Data Protection Act 2012.
- Sukerta, P. A. D., & Sutrisno, A. (2024). Personal data protection in ASEAN: A critical comparison between Indonesia's and Malaysia's legal frameworks. *Constitutional Law Review*, 3(2), 133–147. <https://doi.org/10.30863/clr.v3i2.5605>
- Thailand. (2019). Personal Data Protection Act B.E. 2562 (2019).
- Vietnam National Assembly. (2025). Law No. 91/2025/QH15 on personal data protection.
- World Bank. (2021). World development report 2021: Data for better lives. World Bank. <https://doi.org/10.1596/978-1-4648-1600-0>