sciendo

Global norms and regional innovation: *GDPR*, evolution of data protection in ASEAN and the legal trajectory of AI in Vietnam

Cong Tran Quoc Le
Viet Dung Tran
Dao Phuong Thuy Nguyen

Ho Chi Minh City University of Law
2 Nguyen Tat Thanh, Ward 13, District 4
Ho Chi Minh City, Vietnam
ltqcong@hcmulaw.edu.vn
tvdung@hcmulaw.edu.vn
ndpthuy@hcmulaw.edu.vn

Abstract: Personal data protection has emerged as a defining challenge of the digital age, particularly with the rise of artificial intelligence (AI) and the increasing reliance on cross-border data flows. The European Union's *General Data Protection Regulation* (*GDPR*) has set a global benchmark in this field, with its extraterritorial scope—the so-called Brussels Effect—provoking extensive debate worldwide. In ASEAN, with its accelerating digital transformation and economic integration, data protection laws are being reshaped under both global influences and local priorities. This study aims to identify the factors that have enabled *GDPR* standards to influence evolving legal frameworks of ASEAN and to examine how its member states are responding to global pressures, while simultaneously addressing the distinct challenges of data governance and regional data integration. Using a doctrinal and comparative approach, the study analyzes the personal data protection frameworks of ASEAN-6, with Vietnam highlighted as a distinctive case. Vietnam stands out for explicitly integrating AI-related provisions into its *Personal Data Protection Law*, reflecting both the influence of the *GDPR* and a localized adaptation aligned with strategies for national digital transformation. By examining ASEAN's varied legal responses and Vietnam's unique trajectory,

https://doi.org/10.2478/bjes-2025-0039 *TalTech Journal of European Studies*, 15(3(43))
Tallinn University of Technology (ISSN 2674-4619)

the findings underscore the dynamic interplay between global standards and regional innovation. The article contributes insights for policymakers, businesses and scholars navigating data governance in the digital future of Southeast Asia.

Keywords: *AI, ASEAN,* GDPR*, personal data protection, Vietnam*

1. Introduction

The *ASEAN Digital Masterplan 2025*[1] positions the region as an emerging digital ecosystem, emphasizing the importance of seamless cross-border data exchange while embedding privacy safeguards rooted in regional values. As ASEAN economies are becoming rapidly digitalized, personal data has become both a vital economic resource and a sensitive societal concern. The region faces the dual challenge of safeguarding privacy while sustaining economic growth in a data-driven economy.

Within this digital transformation, artificial intelligence (AI), understood here as systems exhibiting intelligent behavior through environmental analysis and autonomous goal-directed action (OECD, 2019, p. 7), has emerged as both a catalyst and a challenge. This study focuses specifically on AI systems processing personal data, thereby implicating both data protection and frameworks of AI governance. The intersection creates three regulatory challenges: (1) AI's capacity for large-scale inference, revealing sensitive attributes beyond collection purposes and challenges to traditional data minimization principles; (2) automated decision-making which raises transparency and autonomy concerns that are inadequately addressed by existing frameworks and (3) the cross-border nature of AI development, where training data, algorithms and deployment may occur in different jurisdictions, thus complicating regional approaches to regulation.

Over the past decade, ASEAN has gradually advanced from fragmented, sectoral rules toward more comprehensive legal frameworks for personal data protection, reflecting both domestic imperatives and global regulatory pressures. The rise of AI intensifies concerns over algorithmic accountability, discrimination and data inference, amplifying the need for stronger safeguards. At the same time, exponentially growing cross-border data flows

[1] The *ASEAN Digital Masterplan 2025* (2021) was officially adopted on 22 January 2021 at the first ASEAN Digital Ministers' Meeting (ADGMIN1).

demand greater regulatory convergence to balance economic competitiveness with individual rights. Within this dynamic environment, the European Union's *General Data Protection Regulation*, or *GDPR* ('Regulation (EU) 2016/679', 2016), has crystallized as a global benchmark. Its extraterritorial reach, the so-called Brussels Effect, has compelled governments worldwide, including those in Southeast Asia, to reconsider and reform their domestic legal frameworks to avoid exclusion from global digital markets.

This study addresses three interconnected research questions that illuminate the dynamics of regulatory diffusion in the digital age. First, through what mechanism does the *GDPR* exert normative influence on ASEAN data protection frameworks, despite the absence of binding legal obligations? Drawing on Bradford's (2020) Brussels Effect, the study examines how market power, regulatory capacity and the inelasticity of digital markets create structural incentives for alignment with the *GDPR*, transmitted through economic (trade dependencies), normative (best practice discourses), and legal (FTA provisions) channels. Second, how do ASEAN-6 member states selectively adopt and adapt the *GDPR* principles, and what patterns of convergence or divergence emerge across the region? This question employs a comparative legal analysis to identify which *GDPR* elements have been widely transplanted (consent mechanisms, data subject rights) versus which remain contested (data localization, institutional models). The analysis reveals that legal transplantation in ASEAN operates through a process of selective translation rather than comprehensive adoption, reflecting diverse constitutional traditions, development priorities and governance capacities. Third, and most importantly, the study examines Vietnam's distinctive approach to integrate AI governance provisions directly into its *Personal Data Protection Law 2025 (Vietnam)* (hereafter, *V-PDPL*). Whereas the EU has adopted parallel instruments (the *GDPR* and the *AI Act*), and most other ASEAN states have yet to address AI governance comprehensively, Vietnam's integrated model represents a novel regulatory experiment. This raises a fundamental question about the optimal relationship between data protection and AI governance frameworks—specifically, whether integration achieves regulatory coherence or creates implementation challenges.

Methodologically, the paper employs a doctrinal and comparative approach, tracing the diffusion of European data protection norms across ASEAN member states, particularly the ASEAN-6 (Singapore, Malaysia, the Philippines, Thailand, Indonesia and Vietnam). Special attention is devoted to Vietnam, which illustrates a distinctive path by explicitly incorporating AI provisions into its emerging personal data protection framework. Vietnam's

regulatory trajectory demonstrates both the gravitational pull of the *GDPR* principles and the process of legal "localization" to fit domestic priorities in digital transformation and national security.

This study advances the scholarly debate in digital governance. It extends the regulatory diffusion theory by showing how global norms spread through market mechanisms without formal harmonization, enriches comparative data protection scholarship by mapping ASEAN-6 responses to the global influence of the *GDPR* and offers the first in-depth assessment of Vietnam's integrated AI data governance framework. The findings have direct policy relevance: they inform ASEAN's efforts toward regional harmonization, highlight Vietnam's dual pursuit of global alignment and institutional reform and provide the global AI governance community with an alternative model to the prevailing separation paradigm.

This article unfolds in three parts. It begins by contextualizing the *GDPR* as a global standard, examining its extraterritorial enforcement, its interface with the EU *AI Act*, and the mechanisms through which it influences non-EU jurisdictions. Section 2 maps the evolution of personal data protection laws across ASEAN, with a particular emphasis on the ASEAN-6, illustrating both convergence toward and divergence from European standards. The final section turns to Vietnam, tracing the legislative development of its personal data protection regime and its unique integration of AI governance provisions. By structuring the analysis in this way, the article contributes to a deeper understanding of how sovereignty, economic integration and technological transformation intersect in shaping the digital future in Southeast Asia.

2. The EU personal data protection regime as a global benchmark and its influence on ASEAN frameworks

The European Union's governance of personal data and AI system processing personal data has evolved into a dual regulatory framework consisting of the *GDPR* and the *Artificial Intelligence Act* (the *AI Act*). While the *GDPR* governs the processing of personal data irrespective of technology, the *AI Act* regulates AI systems regardless of whether they involve personal data. Together, the regulatory features of these two instruments exert considerable influence on the development of personal data governance frameworks across jurisdictions, particularly among EU trading partners.

2.1 *GDPR*'s extraterritorial architecture

The *General Data Protection Regulation*, which entered into force on 25 May 2018, replacing the Data Protection Directive 1995 ('Directive 95/46/EC', 1995), harmonizes data protection laws across all EU Member States and establishes a uniform standard of protection for personal data within the EU (Islam and Karim, 2020, p. 534). The *GDPR* establishes rules for data processing, in addition to reinforced consent requirements and transparency obligations on data controllers. It plays a pivotal role in strengthening the rights of individuals by providing them with enhanced control over their personal information (Kesa and Kerikmäe, 2020, p. 81). From a systemic perspective, the *GDPR* seeks to balance the fundamental right to data protection, enshrined in Article 8 of the *Charter of Fundamental Rights of the EU*, with the legitimate needs of businesses and public authorities to process personal data (Kamara and De Hert, 2018, p. 15). The systematic nature and internal coherence of the *GDPR* have quickly elevated it to an international benchmark for data governance. Countries around the world, upon developing personal data protection law, would draw significant inspiration from, or make direct reference to, the *GDPR*.

The *GDPR* introduced a more stringent and cohesive legal framework while significantly expanding its territorial scope through Article 3, with the express objective of safeguarding the personal data of EU residents regardless of where the processing takes place. Article 3 delineates the *GDPR*'s territorial scope through two primary criteria. Under Article 3(1), the Regulation applies to processing of personal data in the context of activities of an establishment within the EU, irrespective of where the processing itself takes place (Pramesti and Afriansyah, 2020, p. 85). This entails that all data processing operations carried out by EU establishments must comply with the *GDPR*, regardless of the nationality or residence of the data subject (EDPB, 2018b, para. 19).

Article 3(2) of the *GDPR* broadens this reach to include controllers or processors not located in the EU when their processing activities relate to offering goods or services to, or monitoring the behavior of, data subjects in the EU. This provision establishes a universalist territorial approach whereby the nationality of the data subject becomes immaterial, provided they are physically present within the European Union, and epitomizes a comprehensive protective framework designed to extend maximal safeguards to data subjects, irrespective of the processing entity's origin or the geographical location of data processing mechanisms (Islam and

Karim, 2020, pp. 542–543). The idea of protecting EU citizens' personal data irrespective of its processing location was pursued long before the enactment of the *GDPR*, as evidenced by rulings of the Court of Justice of the European Union (CJEU). In 'Google Spain v. AEPD and Mario Costeja González' (2014), the CJEU affirmed that the "right to be forgotten" should be recognized and that individuals are entitled to request search engine providers to remove results containing personal information (Kesa and Kerikmäe, 2020, p. 82). This approach was followed in 'Google LLC v. CNIL' (2019, para. 62) after the *GDPR* came into effect, as the CJEU examined the practical applicability of Article 3 of the *GDPR* under the circumstances of CNIL's request for global search result suppression.

Chapter v. of the *GDPR* complements Article 3 by establishing a graduated framework for international data transfers premised on ensuring continuous protection regardless of geographic location. The architecture operates through three tiers, each creating distinct incentives for third-country regulatory alignment.

1. Article 45 of the *GDPR* permits unrestricted transfers to countries recognized by the European Commission as providing "adequate" protection, which is essentially equivalent to EU standards. Adequacy decisions eliminate compliance burdens associated with additional safeguards, facilitating seamless data flows. However, adequacy recognition requires a comprehensive assessment of the third country's legal framework, enforcement mechanisms and international commitments, including consideration of the rule of law, respect for human rights and effective independent supervision ('Directive 95/46/EC', 1995, Article 45(2)). This creates the strongest incentive for alignment, as countries seeking adequacy must substantially transplant the core rules and principles of the *GDPR* in their domestic framework.
2. Article 46 of the *GDPR* permits transfers through "appropriate safeguards" where adequacy is lacking—in principle, standard contractual clauses (SCCs) approved by the European Commission (Commission Implementing 'Decision (EU) 2021/914'), binding corporate rules (BCRs), authorized by competent supervisory authorities for intra-group transfers ('Directive 95/46/EC', 1995, Article 47) and approved certification mechanisms coupled with binding commitments from data recipients (EDPB, 2023, paras. 15–28). These institutional safeguards create ongoing, systematic protection independent of individual consent (EDPB, 2020, para. 5). The European

Data Protection Board has emphasized that these instruments must ensure "essentially equivalent" protection to that provided within the EU, requiring controllers to assess whether the third country's legal framework, particularly regarding government access to data, undermines the safeguards (EDPB, 2020, para. 8).

Yet, these mechanisms impose transaction costs and legal uncertainties. The Schrems II decision ('Data Protection Commissioner v. Facebook', 2020) demonstrated their fragility: the CJEU invalidated the EU–US Privacy Shield adequacy decision because US surveillance laws, particularly Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333, permitted government access to transferred data in ways incompatible with Articles 7, 8 and 47 of the Charter of Fundamental Rights ('Data Protection Commissioner v. Facebook', 2020, paras. 168–201). Critically, the Court held that the existence of oversight mechanisms proved insufficient where the substantive legal framework permitted disproportionate interference with fundamental rights ('Data Protection Commissioner v. Facebook', 2020, paras. 176–177). For transfers under SCCs, the Court emphasized that their contractual nature could not prevent third-country public authorities from accessing data in ways incompatible with EU law ('Data Protection Commissioner v. Facebook', 2020, para. 125), requiring data exporters to conduct transfer impact assessments and implement supplementary measures where necessary ('Data Protection Commissioner v. Facebook', 2020, para. 134; EDPB, 2020).

For ASEAN states with expansive national security or cybersecurity laws enabling government data access, Schrems II created obstacles to both adequacy recognition and reliance on Article 46 mechanisms. The decision signals that legal frameworks permitting broad surveillance powers even when supplemented with procedural safeguards may be deemed incompatible with *GDPR*'s protection standards (Kohl, 2022).

3. Article 49 of the *GDPR* provides narrow derogations for specific situations, explicit informed consent after being informed of possible risks, contract performance, vital interests, important reasons of public interest, establishment or defense of legal claims, but only for occasional, non-repetitive transfers (Article 49(1)). The EDPB has consistently emphasized that Article 49 derogations must be interpreted restrictively and cannot provide basis for repetitive or structural transfers (*EDPB Guidelines* 2/2018). Consent under Article 49(1(a)) requires heightened transparency regarding risks and cannot substitute for institutional protections in regular business operations (EDPB, 2018a, paras. 10,

14). As Recital 111 clarifies, such transfers should be "occasional and necessary", not routine practice ('Directive 95/46/EC', 1995, Recital 111; EDPB, 2018a, paras. 23–24).

Taken together, the architecture of Chapter v. incentivizes comprehensive *GDPR* alignment. Article 49 provides only limited relief unsuitable for regular data flows. Article 46 mechanisms enable ongoing transfers but impose costs and create legal uncertainties, particularly post-Schrems II. Adequacy recognition eliminates these frictions but requires substantial legal harmonization, creating a regulatory quid pro quo driving third-country legal development toward *GDPR* standards (Bradford, 2020, pp. 149–150).

2.2 The EU *AI Act* as a complementary framework

The *AI Act* ('Regulation (EU) 2024/1689', 2024), adopted in 2024, complements the *GDPR* by extending data protection principles into the broader governance of artificial intelligence. While the *GDPR* focuses on safeguarding individuals in the processing of personal data, the *AI Act* regulates the design, development and deployment of AI systems that process such data. Together, their extraterritorial reach amplifies the EU's regulatory influence beyond its borders, subjecting external partners, such as ASEAN member states, whose economies are increasingly driven by e-commerce and AI-based data processing involving the EU.

The *AI Act* employs risk-based differentiation that supersedes earlier four-tier conceptualizations. Prohibited AI practices ('Regulation (EU) 2024/1689', 2024, Article 5) categorically ban systems posing unacceptable risks to fundamental rights—including subliminal manipulation causing psychological or physical harm, exploitation of vulnerabilities of specific groups, social scoring systems by public authorities leading to detrimental treatment, real-time remote biometric identification in publicly accessible spaces for law enforcement purposes (subject to narrow exceptions), biometric categorization systems inferring sensitive attributes, emotion recognition in workplace and education contexts (with limited exceptions) and scraping of facial images from internet or CCTV footage for facial recognition databases ('Regulation (EU) 2024/1689', 2024, Article 5(1(a–h)).

High-risk AI systems ('Regulation (EU) 2024/1689', 2024, Article 6, read together with Annex III) are permitted but subject to comprehensive ex-ante conformity assessment and ongoing obligations. High-risk classification depends on whether the AI system is a safety component of products

covered by EU harmonization legislation or falls within specified high-risk areas including biometric identification and categorization, critical infrastructure management, education and vocational training, employment and worker management, access to essential private and public services, law enforcement, migration and border control management and administration of justice and democratic processes. High-risk obligations include risk management systems throughout the AI lifecycle (Article 9), data governance ensuring quality, relevance and representativeness (Article 10), technical documentation and record-keeping (Articles 11–12), transparency and provision of information to users (Article 13), human oversight to prevent or minimize risks (Article 14) and accuracy, robustness and cybersecurity requirements (Article 15).

The interface with the *GDPR* creates both complementarity and overlap with direct implications for ASEAN AI developers. Both regulate AI processing personal data cumulatively. Article 10(5) of the *AI Act* applies "without prejudice" to *GDPR* obligations. Automated decision-making provisions interact: Article 22 of the *GDPR* protects individual autonomy against purely automated decisions with legal or similarly significant effects, while Article 14 of the *AI Act* mandates human oversight for high-risk systems. Data quality requirements overlap the *GDPR*'s data minimization and accuracy principles ('Directive 95/46/EC', 1995, Article 5(1(c–d)) intersect with the *AI Act*'s mandate that training data be "relevant, representative, free of errors and complete" considering intended purpose and reasonably foreseeable misuse ('Regulation (EU) 2024/1689', 2024, Article 10(3)), creating a *lex specialis* relationship elaborating *GDPR* principles for AI contexts.

Most significantly for ASEAN, the extraterritorial scope of the *AI Act* mirrors that of the *GDPR*, applying to providers who place AI systems on the EU markets or putting them into service within the EU, regardless of location; to deployers of AI systems established in the EU; and to providers or deployers outside the EU whose AI system output are used within the EU ('Regulation (EU) 2024/1689', 2024, Article 2(1(a–c)). This jurisdictional reach operates independently of the *GDPR*: even an AI system that processes only non-personal data but producing outputs used in the EU falls withing the scope of the *AI Act*. Consequently, ASEAN technology exporters face an expanded sphere of regulatory exposure under the EU's AI governance framework.

The dual framework compounds *GDPR* compliance burdens but also creates alignment incentives, such as market access considerations parallel to *GDPR* adequacy, Article 63 contemplates international cooperation agreements,

potentially including mutual recognition of conformity assessments ('Regulation (EU) 2024/1689', 2024, Articles 63(1) and 63(2)). However, comprehensive adoption of the *AI Act* may not suit ASEAN contexts. The regulation reflects EU's priorities—fundamental rights protection, precautionary approach, emphasis on ex-ante conformity assessment—potentially in tension with ASEAN development imperatives favoring innovation enablement and lighter-touch regulation. Vietnam's integrated approach, embedding AI governance within data protection law rather than creating parallel instruments, represents an alternative pathway attempting to adopt AI governance principles while avoiding the coordination complexity and dual compliance costs inherent in the EU's separation model.

2.3 Mechanisms of normative diffusion: the Brussels Effect

The global influence of the *GDPR* and *AI Act* exemplifies what Bradford (2020) describes as the "Brussels Effect"—the EU's unique capacity to externalize its regulatory standards globally through the sheer force of its market power, rather than through formal legal harmonization or diplomatic negotiation. This extraterritorial diffusion of EU norms is underpinned by four underlying structural conditions, each of which holds particular significance for the governance of the digital economy.

1. The EU market of 450 million affluent consumers creates gravitational pull (Eurostat, no date); exclusion from EU digital markets entails substantial revenue loss for ASEAN firms.
2. The EU possesses regulatory capacity for effective standard-setting and enforcement, the European Data Protection Board ensures uniform *GDPR* interpretation while Member State data protection authorities wield substantial sanctioning authority, with over 5.88 billion euros in cumulative fines issued through the end of 2024 (McKean *et al.*, 2025) and the *AI Act* establishes the European AI Board coordinating implementation across Member States ('Regulation (EU) 2024/1689', 2024, Articles 64–67).
3. Both the *GDPR* and the *AI Act* standards exceed most jurisdictions' requirements, establishing high regulatory ceilings through comprehensive scope, robust individual rights and strict accountability obligations.
4. Digital markets exhibit technical inelasticity, cloud infrastructure and AI systems typically cannot easily segregate EU data from non-EU data

or functionality (Bradford, 2020, pp. 57–58), making dual compliance models costly relative to universal adoption.

These conditions transmit through three channels observable in ASEAN.

2.3.1 The channels observable in ASEAN

The economic channel operates through trade dependencies and foreign investment. ASEAN firms serving EU clients must implement *GDPR–AI Act* compliance or face exclusion, while EU multinationals impose these standards on local subsidiaries and vendors through corporate governance (Bradford, 2020, pp. 184, 185; Rustad and Koenig, 2019, pp. 413, 418). Evidence from business practice suggests that firms with EU partnerships often implement *GDPR*-aligned measures even where not legally required domestically, driven by commercial imperatives rather than legal mandates (Rustad and Koenig, 2019, pp. 438, 439). For AI specifically, ASEAN technology companies exporting services to Europe confront dual compliance obligations under both the *GDPR* (governing personal data processing) and the *AI Act* (regulating AI systems). This overlapping regulatory burden generates potential "comply-or-exit" dynamics, echoing patterns observed in other technology-intensive sectors (Bradford, 2020).

The normative channel functions through epistemic communities and best practice discourses. International frameworks including the *OECD Privacy Guidelines* (OECD, 2013) and *APEC Cross-Border Privacy Rules* (APEC, 2019) share core principles with the *GDPR*, demonstrating normative convergence in global privacy governance. Technical standard-setting organizations embed the *GDPR* principles into global standards—ISO/IEC 27701:2019, designed for *GDPR* compatibility and available for adoption globally, provides internationally recognized framework (ISO/IEC 27701:2019). For AI governance, the OECD *AI Principles* (2019), endorsed by ASEAN member states, reflect concerns about transparency, accountability and human oversight that are central to the *AI Act*, demonstrating normative convergence (OECD, 2019, p. 7).

The legal channel operates through trade agreements and adequacy mechanisms. The *EU–Vietnam Free Trade Agreement* (*EVFTA*, effective since 2020) requires both parties to "adopt or maintain" laws providing "high level of protection" of personal data and "endeavor to ensure that their respective rules are interoperable" (*EVFTA*, 2020, Article 8(62)). The *EU–Singapore Digital Partnership Agreement* (*ESDPA*, signed in 2023) similarly requires both parties to maintain "comprehensive legal frameworks for

the protection of personal data" and facilitate cross-border flows "on the basis of a high level of data protection" (*ESDPA*, 2023, Article 7). Adequacy mechanisms themselves constitute powerful diffusion channels—countries seeking adequacy must essentially transplant the *GDPR*'s core elements, as empirically demonstrated through legislative amendments in jurisdictions pursuing adequacy recognition.

2.3.2 The limits of the Brussels Effect in Southeast Asia: structural constraints on regulatory convergence

Competing regulatory models offer alternatives. The United States' sectoral approach, fragmented regulation across domains, emphasizes flexibility over comprehensive coverage, advocated by American technology firms dominant in ASEAN markets. China's *Personal Information Protection Law* (2021) presents a third model combining *GDPR*-style individual rights with extensive state surveillance authorities and data localization mandates (Lee, 2021). These competing models create regulatory cross-currents, the ASEAN frameworks exhibit *GDPR* influence in substantive provisions while retaining sectoral localization requirements aligned with alternative regulatory philosophies.

ASEAN's institutional culture emphasizes consensus, non-interference and flexibility over binding harmonization. The *ASEAN Framework on Digital Data Governance* (2018) establishes principles but lacks enforcement mechanisms (ASEAN, 2016). The *Digital Economy Framework Agreement* (ASEAN, 2023b) similarly provides aspirational goals without binding commitments (ASEAN, 2023a). This preference impedes deep *GDPR–AI Act* alignment—even where individual states adopt compatible laws, regional harmonization remains elusive.

Development diversity creates divergent regulatory capacities and priorities. Advanced economies possess institutional capacity for sophisticated data protection and AI governance regimes, while less developed members struggle with basic frameworks, rendering EU-style comprehensive regulation premature for some jurisdictions (Habibulloh, 2025, pp. 2–3).

Data localization mandates represent direct resistance to *GDPR*'s facilitation of free data flows, reflecting competing priorities such as national security, domestic tech development and digital sovereignty. While Chapter v. of the *GDPR* presumes cross-border flows subject to protective conditions, absolute localization requirements negate this model (Wong, 2019, pp. 172–173). Evolving state practices regarding localization reflect ongoing calibration

between sovereignty imperatives and the practical requirements of AI development and adequacy goals. The result is selective translation rather than comprehensive transplantation. The Brussels Effect exerts the greatest influence where legal tradition align, market access incentives exist and sovereignty concerns are limited; it weakens where national security or developmental constraints prevail. This framework illuminates the varied ASEAN-6 responses examined in the following chapter, which shows how *GDPR*-inspired norms diffuse through the Brussels Effect mechanisms, yet are adapted to each country's constitutional traditions, development strategies and governance philosophies.

3. ASEAN-6 personal data protection laws: the selective transplantation of the *GDPR*'s legal principles

3.1 Pre-*GDPR* frameworks and post-2018 adaptations

Within the ASEAN-6, Singapore, Malaysia and the Philippines stand out for having developed independent and comprehensive legal frameworks on personal data protection at an early stage, well before the *GDPR* entered into force in 2018. The emergence and evolution of these frameworks were primarily driven by domestic imperatives to modernize data governance amid rapidly expanding digital economies, while simultaneously fostering trust among international investors and consumers in electronic commerce. A notable common feature across these jurisdictions is that their legislative designs were shaped to a considerable extent by the common law legal tradition (Amiludin *et al*., 2024, p. 175) and by international instruments and recommendations, particularly those issued by the OECD and APEC, rather than being directly modeled on the *GDPR* which had not yet crystallized as a global benchmark.

Singapore enacted its *Personal Data Protection Act* in 2012 (*S-PDPA*), establishing one of the region's pioneering regimes for the regulation of personal data. Section 26 authorizes cross-border data transfers where an "equivalent level of protection" is ensured, but simultaneously acknowledges the APEC *Cross-Border Privacy Rules* (*CBPR*) and the APEC *Privacy Recognition for Processors* (*PRP*) as legitimate alternative safeguards (PDPC Singapore, 2021). This dual recognition reflects a hybrid regulatory approach that embeds global standards within a broader Asia-Pacific normative framework, thereby signaling Singapore's intent to reconcile international

best practices with regional mechanisms tailored to the dynamics of cross-border digital trade (Chik, 2013, p. 557). The provision stipulating protection of personal data of individuals in Singapore "regardless of nationality" indicates that Singapore adopted an expansive approach to the scope of protection, mirroring GDPR's extraterritorial spirit while carefully adapted to align with the country's open economic orientation.

Malaysia had already taken similar steps with the enactment of the *Personal Data Protection Act (Malaysia)* in 2010 (*M-PDPA*), which became effective in 2013 and focused in particular on key sectors such as finance, telecommunications and online services. Unlike Singapore, Malaysia adopts a more stringent conditional approach to cross-border data transfers. In addition to requiring that the recipient country provide an "equivalent level of data protection", Malaysia imposes a distinctive obligation on data controllers to conduct their own assessment of the adequacy of protection through a transfer impact assessment (TIA), to be reviewed at least once every three years, rather than relying on a centralized adequacy determination as in the EU (Tan *et al*., 2021, pp. 167, 169). Malaysia refrains from imposing data localization requirements under its *M-PDPA*, though Federal and State Government operations are exempted from the Act's application (*Personal Data Protection Act (Malaysia)*, 2021, Section 3(1)(a); Alibeigi and Munir, 2020, p. 366).

The Philippines followed with the *Data Privacy Act (Philippines) 2012* (*P-DPA*), accompanied by the establishment of a specialized enforcement authority, the National Privacy Commission, tasked with regulatory oversight and implementation. Anchored in the dual objectives of safeguarding the fundamental right to privacy and ensuring the free flow of information as a driver of innovation and economic growth (Ching *et al*., 2018, p. 121), the Philippines' *P-DPA* provides a robust legal framework governing the processing of personal information across private and public sectors (Pitogo, 2019, pp. 280, 251–252). The *P-DPA* codifies key data protection principles—transparency, legitimate purpose and proportionality—and affords individuals an extensive catalog of rights, including the rights to be informed, to access, to rectification, to erasure or blocking, to seek damages and to lodge complaints.

Following the *GDPR*'s entry into force in May 2018, all three states undertook legislative updates to bring their frameworks more closely in line with emerging international standards, demonstrating the influence of the Brussels Effect operating through normative channels. Singapore introduced

major amendments in 2020–2021, which included new legal bases for data processing beyond consent, an expanded definition of deemed consent, the introduction of mandatory data breach notification, an increase in maximum financial penalties to 1 million Singapore dollars (approximately 665,000 euros) or 10% of annual turnover—representing a tenfold increase from the original framework, and the addition of a data portability right (Alfred, 2020). These post-*GDPR* reforms reflected a recognition that the original data protection frameworks risked placing jurisdictions at a competitive disadvantage in global digital markets, where the *GDPR* had established elevated baseline standards. In response, Singapore enacted major amendments between 2020 and 2021, introducing provisions consistent with international best practices, including mandatory data breach notification and data portability mechanisms broadly aligned with the *GDPR* requirements. Malaysia enacted the *Personal Data Protection (Amendment) Act 2024*, introducing a transfer impact assessment mechanism, removing the whitelist approach to cross-border transfers in favor of adequacy assessments and expanding data subject rights including data portability (Baker McKenzie, 2024a; 2024c; Shivhare, 2025). The Philippines has also expressed its intention to undertake legislative reform efforts in relation to the DPA, with the National Privacy Commission proposing amendments to strengthen its enforcement powers and introduce additional revisions to the legislation. However, these proposed legal amendments remain under study and impact assessment at the current stage (Desiderio, 2021; *Digital Policy Alert*, 2024).

3.2 Post-*GDPR* frameworks with explicit EU influence

Thailand and Indonesia enacted their data protection laws after the *GDPR* had entered into force and explicitly acknowledged the influence of the European legal framework in legislative materials and design choices. These states developed comprehensive frameworks after the *GDPR*'s demonstration effect became apparent, incorporating *GDPR*-style rights catalogs from inception alongside robust enforcement frameworks authorizing substantial fines and detailed cross-border transfer provisions.

The *Personal Data Protection Act (Thailand)* (*T-PDPA*), adopted in 2019 and fully effective in 2022 following implementation delays, has been characterized domestically as "Thailand's *GDPR*" reflecting its close modeling on the European regulation (Sudirman *et al.*, 2023, p. 497). The framework authorizes fines up to 5 million Thai bahts (approximately 132,200 euros)

and establishes the Personal Data Protection Committee with regulatory and adjudicatory functions (LawAsia, 2025; Norton Rose Fulbright, no date). Notably, in November 2023, Thailand issued two *Notifications of the Personal Data Protection Committee on Criteria for the Protection of Personal Data Sent or Transferred to a Foreign Country* (the *Whitelist Notification* and the *BCRs and Appropriate Safeguards Notification*). These instruments expressly recognize both the ASEAN Model Contractual Clauses for Cross-Border Data Flows and the EU Standard Contractual Clauses (SCCs) as acceptable alternative safeguards (Baker McKenzie, 2024b), demonstrating explicit incorporation of EU transfer mechanisms alongside regional instruments.

The *Personal Data Protection Law (Indonesia)* (*I-PDPL*), enacted in October 2022, has incorporated almost comprehensively the principles of the *GDPR*—ranging from the definition of personal data and the rights of data subjects to mechanisms for cross-border data transfer (ASEAN Briefing, 2024; Sudirman *et al.*, 2023, p. 501). The framework authorizes administrative fines of up to 2% of annual revenue for data protection violations, while serious criminal offences may incur fines of up to 6 billion Indonesian rupiahs (approximately 312,000 euros), reflecting the influence of the *GDPR* on deterrence-oriented enforcement design (Sudirman *et al.*, 2023, p. 497). However, a key distinction lies in Indonesia's continued imposition of data localization requirements for public electronic system operators (ESO) under 'Government Regulation No. 71' (2019) on the Implementation of Electronic Systems and Transactions (which replaced 'Government Regulation No. 82' of 2012). Article 20 of 'Government Regulation No. 71' mandates that public ESOs—including government agencies and their partners—must process and store electronic systems and data within Indonesia. This framework illustrates Indonesia's strategy of aligning substantive provisions of the *I-PDPL* with *GDPR*-compatible standards to support international digital trade, while retaining localization mandates in the public sector to safeguard national data sovereignty and security—exemplifying selective translation, where convergence coexists with sovereignty-protective divergence.

Among the ASEAN-6 nations, Vietnam's legal framework for personal data governance initially evolved with greater caution, primarily driven by national security considerations. The *Cybersecurity Law (Vietnam) 2018* adopted a highly securitized stance, mandating stringent data localization and emphasizing state sovereignty over cross-border data flows. However, recent developments mark a notable policy shift toward a more balanced and innovation-oriented model, as reflected in the promulgation of the

Personal Data Protection Law (Vietnam) and the *Law on Digital Industry and Technology (Vietnam)* in 2025, which together signify Vietnam's transition from a purely security-driven approach to one increasingly linked to the imperatives of international integration, including adaptation to the standards embodied in the EU regulatory frameworks. A detailed analysis of Vietnam's case will be presented in the section below.

Overall, the post-2018 trend of *GDPR*-inspired regulatory modeling among the ASEAN-6 reflects three mutually reinforcing dynamics.

1. *The temporal advantage*: enacting comprehensive frameworks after *GDPR*'s entry into force enabled legislatures to observe its implementation, enforcement patterns, and global influence, reducing uncertainty about its viability as a regulatory model.
2. *Clean-slate flexibility*: unlike pre-*GDPR* states that required amendments to existing frameworks with established stakeholder expectations and institutional infrastructures, post-*GDPR* states could design comprehensive regimes from inception, incorporating *GDPR* elements without transitional frictions.
3. *Adequacy incentives*: Thailand's export-oriented economy—with substantial trade relations with the European Union, where the EU accounted for 7.1% of Thailand's total trade in goods in 2023—created strong motivations for *GDPR* alignment to facilitate cross-border data flows and market access (European Commission, 2024), while Indonesia's ambitions for digital economy expansion similarly reinforced this convergence trend.

3.3 Persistent divergences: limits of regulatory diffusion

While ASEAN-6 frameworks converge substantially on core data protection principles transmitted through the Brussels Effect mechanisms, persistent divergences on data localization, institutional models and cross-border transfer mechanisms reveal structural limits to regulatory diffusion imposed by path dependencies, sovereignty imperatives and developmental priorities.

3.3.1 Data localization: sovereignty imperatives versus economic integration

Data localization requirements vary significantly across ASEAN-6, revealing fundamental tensions between *GDPR*'s facilitation of cross-border data flows and sovereignty-protective impulses. Singapore, Thailand and

Vietnam impose no general localization mandates (since 2025), facilitating unrestricted cross-border flows subject to protective safeguards under transfer frameworks. This approach aligns with the presumption in Chapter v. of the *GDPR* that data may flow internationally, provided adequate protection mechanisms ensure continuity of rights.

Malaysia maintains sector-specific localization for government data, reflecting administrative preferences for domestic control over public sector information without imposing comprehensive restrictions that would impede private sector digital trade (Alibeigi and Munir, 2020). Indonesia's 'Government Regulation No. 71' requires localization for public electronic system providers, serving dual purposes of national security protection and industrial policy promotion (Wong, 2019). The regulation mandates that government agencies and their partners process and store data domestically, creating captive demand for domestic cloud infrastructure and data center industries while maintaining governmental data access for security and regulatory purposes.

Singapore and Vietnam have demonstrated significant evolution in their trade and digital policy frameworks. Both ASEAN economies are actively pursuing deep free trade arrangements with the European Union and positioning themselves as regional digital economy hubs, thereby requiring seamless international data exchange to attract foreign investment in fintech, e-commerce, cloud services and AI development. Vietnam, in particular, has undertaken substantial reforms in building its framework for data governance following the signing of the *EVFTA* (Artzt and Tran, 2022, p. 41) and has also launched innovative regulatory initiatives aimed at governing AI systems that process personal data. Thailand's similar policy direction reflects a recognition that strict data localization measures impede integration into global digital supply chains. In contrast, Indonesia employs data localization strategically as an instrument of industrial policy, accepting the associated trade frictions to advance technological sovereignty and promote domestic technology industry development (Wong, 2019).

3.3.2 Institutional models: independence versus coordination

Singapore and Malaysia establish statutory bodies with regulatory and enforcement authority over data protection. Singapore's Personal Data Protection Commission (*S-PDPA*, 2012, Section 5) and Malaysia's Personal Data Protection Commissioner (*M-PDPA*, 2010, Section 5) possess powers to investigate violations, issue directions and impose administrative

penalties, while remaining accountable to relevant ministries. Thailand's framework establishes dual oversight through a Personal Data Protection Committee for policy-making and an Expert Committee for enforcement (*T-PDPA*, 2019, Sections 8, 38). The Philippines establishes the National Privacy Commission as an independent statutory body with fixed-term commissioners and removal protections (*P-DPA*, 2022, Section 7), though the Commission remains administratively attached to the Department of Information and Communications Technology for policy coordination.

Indonesia and Vietnam assign primary authority for data protection oversight to ministerial bodies, reflecting preferences for executive control and integration with broader governmental functions. In Indonesia, the Ministry of Communication and Informatics (Kominfo) serves as the central regulatory authority under the *I-PDPL*, responsible for supervision, guidance, and coordination of implementing regulations, while the establishment of an independent supervisory agency remains pending. In Vietnam, the Ministry of Public Security—through its Department for Cybersecurity and Prevention of Hi-tech Crime (Department A05)—acts as the designated data protection authority under 'Decree 13/2023/ND-CP' and reaffirmed under the *V-PDPL*. Accordingly, the data protection mandate of the Department A05 integrates personal data protection oversight with broader cybersecurity and public security functions. The ministerial models adopted by Indonesia and Vietnam consolidate administrative coordination and enable whole-of-government implementation approach; however, they also raise concerns that privacy protection may be subordinated to broader state priorities, including national security, administrative efficiency and economic development.

These path dependencies limit comprehensive *GDPR* transplantation despite the pressures of the Brussels Effect. The *GDPR* presumes independent supervisory authorities as accountability mechanisms preventing governmental interference with privacy protection ('Regulation (EU) 2016/679', 2016, Articles 51–59). Yet, institutional models reflect constitutional fundamentals and administrative traditions resistant to external regulatory influence. The optimal institutional design depends on broader governance context, independent authorities suit liberal democratic systems with strong rule of law and judicial review constraining arbitrary authority (Yeung and Bygrave, 2022, p. 147–148), while ministerial models may function effectively in developmental states with coordinated industrial policy frameworks, provided adequate procedural safeguards and judicial review mechanisms constrain discretion (Bradford, 2020, p. 279).

3.3.3 Cross-border transfer mechanisms: regulatory innovation

Cross-border transfer mechanisms exhibit both convergence on *GDPR* Chapter V's basic architecture and distinctive adaptations reflecting regulatory innovation and strategic positioning.

All ASEAN-6 frameworks require either adequacy determination or appropriate safeguards for international transfers, reflecting the influence of the *GDPR* influence on the fundamental structure of transfer regulation. Singapore accepts APEC CBPR certification as an adequate safeguard alongside adequacy assessments, embedding regional mechanism within global framework and signaling commitment to Asia-Pacific economic integration alongside European alignment (PDPC Singapore, 2021). Malaysia uniquely requires controller-conducted transfer impact assessments that are reviewed triennially, decentralizing adequacy assessment to individual organizations rather than relying solely on governmental determinations, placing responsibility on data controllers while maintaining regulatory oversight through periodic review requirements (Alibeigi and Munir, 2020).

Thailand maintains a governmental whitelist of adequate countries while recognizing SCCs and BCRs as alternative safeguards, closely paralleling EU's dual-track approach in adequacy safeguards (Baker McKenzie, 2024b). Indonesia adopts a *GDPR*-proximate framework requiring adequacy or safeguards including SCCs, BCRs and certification mechanisms (ASEAN Briefing, 2024). Vietnam diverges through post-transfer impact assessment model transfers permitted initially, with controllers required to file impact assessments within 60 days and update upon material changes, representing trust-but-verify approach prioritizing business facilitation over precautionary ex-ante restriction (analyzed comprehensively in the following Section 4).

This variation reflects strategic calculations balancing sovereignty, compliance costs and business facilitation. Singapore's adequacy pursuit requires demonstrating comprehensive *GDPR* compatibility, incentivizing close alignment. Malaysia's TIA model distributes compliance burden to controllers while avoiding governmental capacity constraints in conducting adequacy assessments for numerous third countries. Vietnam's post-filing model reflects developmental state orientation favoring business enablement and AI development, which require seamless cross-border data flows, over precautionary restrictions that might impede digital economic growth.

3.3.4 AI governance: regulatory gap

While ASEAN-6 states have converged toward *GDPR*-inspired data protection frameworks, their approaches to AI governance reveal striking divergence, creating a regulatory landscape where automated decision-making proliferates across finance, employment, healthcare and public administration with limited legal oversight.

Singapore represents the soft-law paradigm. Its *Model AI Governance Framework* (2020, updated in 2022) comprises voluntary best practices and implementation guidance that emphasizes industry self-regulation with governmental oversight (PDPC Singapore, 2020). The Framework articulates the principles of transparency, explainability and human oversight, but lacks coercive force for non-compliant actors. Organizations may choose not to implement provisions without legal consequences, relying instead on reputational incentives and market pressures. This approach offers flexibility, rapid updates without legislative amendment, experimentation encouraging innovation, sector-specific customization, but produces uneven adoption, with leading firms implementing comprehensively while smaller organizations, or those prioritizing short-term profits, may disregard the provisions.

Malaysia, the Philippines, Thailand and Indonesia exhibit regulatory gaps. None possess comprehensive AI governance provisions despite rapid AI deployment across critical sectors. Credit-scoring algorithms, recruitment-screening platforms, biometric identification systems and government-benefit eligibility determination systems operate without specific regulatory safeguards addressing algorithmic accountability, bias mitigation or automated decision-making transparency. Generic data protection laws provide indirect constraints in consent requirements, purpose limitation and accuracy obligations but lack AI-specific provisions addressing the distinctive challenges of technology: opacity of algorithmic decision-making, capacity for large-scale inference beyond original collection purposes and potential for discriminatory outcomes amplifying existing social biases (Barocas and Selbst, 2016, pp. 671–672, 674, 692; Tran, 2024, p. 31). Vietnam alone integrates AI governance within data protection law through Article 30 of the *V-PDPL*, representing a novel regulatory architecture examined comprehensively in the following section.

4. Vietnam's emerging framework for personal data protection: between caution and innovation

Within the trajectory of the development of personal data protection legislations among the ASEAN-6, Vietnam constitutes a distinctive case. Since the *Doi Moi* (Renovation) reforms, the country has consistently pursued a liberal market-opening policy, seeking to balance economic growth with the preservation of national sovereignty (Artzt and Tran, 2022, p. 40). With the rise of the digital economy, Vietnamese policymakers have faced three concurrent challenges: (i) fostering the growth of the data and digital economy, (ii) safeguarding national sovereignty in cyberspace and (iii) ensuring information security for participants in the digital ecosystem. Vietnam's regulatory trajectory demonstrates both the gravitational pull of the *GDPR* principles transmitted through the Brussels Effect mechanisms and a process of legal "localization", calibrated to domestic priorities in digital transformation and national security. Most significantly, Vietnam stands alone among ASEAN-6 states in explicitly integrating AI governance provisions into its personal data protection law, representing a novel regulatory architecture that diverges from both the EU's dual-framework model and Singapore's soft-law approach while attempting to avoid the regulatory gaps observable in Malaysia, Philippines, Thailand and Indonesia.

4.1 From fragmentation to integration: strategic drivers of regulatory evolution

Over the past decade, Vietnam has undergone a profound transformation in its approach to personal data governance. Having moved from a cautious, security-oriented stance toward promoting the adoption of a more open legal framework that enables cross-border personal data transfer, the government has simultaneously begun to lay the regulatory foundations for AI systems processing personal data. The evolution of Vietnam's personal data protection regime has not followed a linear trajectory but has instead been shaped by three mutually reinforcing strategic imperatives.

1. International trade commitments created external alignment pressures. The CPV Politburo's 'Resolution No. 52-NQ/TW', introduced in 2015, set ambitious targets for the digital economy—20% of the GDP by 2025 and more than 30% by 2030—signaling that digital transformation was not simply a reaction to global trends but a strategic priority endorsed at

the highest political level. This trajectory was reinforced by Vietnam's conclusion of two new-generation trade agreements, the *EVFTA* and the *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (*CPTPP*), both aimed at promoting the liberalization of e-commerce. The *EVFTA*, effective since 2020, explicitly embeds obligations on personal data protection, requiring both parties to "adopt or maintain" laws providing "high level of protection" of personal data and "endeavor to ensure that their respective rules are interoperable" (*EVFTA*, 2020, Article 8(62)). While not mandating the adoption of the *GDPR* verbatim, the *EVFTA* created direct compliance imperatives that subsequently manifested in 'Decree 13/2023/ND-CP' and the *V-PDPL*.

2. AI-driven digital transformation imperatives demanded coherent governance frameworks. Vietnamese policymakers recognized that contemporary data management systems increasingly deploy AI to enhance efficiency, with AI systems operating on large-scale personal data at high velocity, capable of inferring attributes beyond original collection purposes and raising risks including re-identification of anonymized data, behavioral profiling, automated decision-making with significant effects, algorithmic bias and secondary uses contravening purpose limitation and data minimization principles. The submission of the Ministry of Public Security to the government on the dossier of the *V-PDPL* development explicitly identified these AI-specific challenges as necessitating integrated governance rather than fragmented sectoral approaches. The digital economy targets of 'Resolution No. 52-NQ/TW' could not be achieved through data protection law alone—AI development constitutes the technological foundation for digital transformation across finance, healthcare, public administration and industrial sectors, requiring unified rather than parallel regulatory oversight.

3. Institutional learning has developed from the recognized shortcomings of state-centric personal data protection regulations. In 2023, the government of Vietnam promulgated 'Decree 13/2023/ND-CP' as Vietnam's first dedicated regulation directly addressing personal data protection. While welcomed as a progressive step drawing inspiration from international models including *GDPR*, 'Decree 13/2023/ND-CP' exposed critical shortcomings: it remained state-centric rather than governance-oriented, offering little granularity for complex multi-party processing typical of platform ecosystems; it adopted *GDPR*-style bifurcation between "basic personal data" and "sensitive personal data" through enumerated lists rather than functional definition,

with Article 11(8) requiring both informed consent and explicit notice of sensitivity, casting consent as primary safeguard while leaving risk-based and contextual controls underdeveloped; it designated the Department A05 of the Ministry of Public Security as the lead authority but did not establish dedicated procedural avenues for data subjects, with rights to complain, denounce, sue or seek damages referenced only to "comply with the law" without bespoke enforcement pathways; and for cross-border transfers, it introduced transfer impact assessment requirements but retained domestic storage obligations under the *Cybersecurity Law (Vietnam)*, not applying *GDPR*-style "adequacy" or "appropriate safeguards" models (Dat and An, 2024). The government of Vietnam assessed 'Decree 13/2023/ND-CP' as insufficiently effective and not enabling Vietnamese citizens to exercise their legally conferred rights in practice, creating imperative for dedicated legislative reform through the *V-PDPL*, adopted on 26 June 2025.

These three drivers—international alignment pressures transmitted through the legal channel of the Brussels Effect, AI governance imperatives arising from digital transformation strategy and institutional learning from regulatory experimentation—converged to produce Vietnam's current distinctive integrated approach. The *V-PDPL* has been drafted as part of a broader integrated corpus of data governance legislation including the new *Law on the Digital Technology Industry (Vietnam)* (*V-DTIL*), adopted in 2025, and amendments to the *Law on Cybersecurity*, with an express aim of minimizing conflicts and overlaps among these instruments. This coordinated approach contrasts with the fragmented evolution observable in other ASEAN-6 states, where data protection frameworks developed independently from AI governance considerations.

4.2 The *V-PDPL*: structural analysis and distinctive features

4.2.1 Core regulatory innovations

The V-PDPL introduces three foundational innovations that distinguish it from both the *GDPR*-influenced frameworks across ASEAN-6 and the EU's dual *GDPR–AI Act* model.

1. Regarding the scope of application, the *V-PDPL* provides greater clarity relative to 'Decree 13/2023/ND-CP' in its applicability to foreign

organizations, agencies and individuals. For entities not based in Vietnam, the *V-PDPL* applies only when such entities directly process or are involved in processing personal data of Vietnamese citizens or persons of Vietnamese origin with undetermined nationality residing in Vietnam. The *V-PDPL* resolves 'Decree 13/2023/ND-CP' limiting of "personal data" to data in digital form by defining personal data to encompass digital data and any other form of information that identifies, or helps identify, a specific individual, regardless of storage medium. The *V-PDPL* introduces the concept of "anonymization", absent from 'Decree 13/2023/ND-CP', defining it as the process of altering or removing information to create new data from which a specific individual cannot be identified in any circumstances, with anonymized data defined as "not personal data". To ensure effective anonymization, the *V-PDPL* imposes duties on entities performing the process, including close oversight and controls, prevention of unauthorized access during anonymization and prohibition on re-identifying anonymized data unless permitted by law, creating a safe harbor for processed information to meet irreversibility standards while requiring technical standards define irreversibility thresholds in implementation.

2. The regulation of obligations of data subjects in parallel with rights constitutes unique legal theoretical innovation stemming from deep awareness of social context and citizen capability levels. While Western legal systems that are built on the foundation of liberal individualism, assume that individuals possess complete autonomy in protecting their data as personal asset (Berg, 2018, pp. 38, 41), Vietnam recognizes that in a society undergoing a rapid digital transformation, the majority of citizens lack sufficient knowledge and skills to protect themselves effectively without complementary obligation frameworks that would establish baseline protective behaviors. This philosophy stems from the distinctive treatment of "human rights" alongside the "basic rights and obligations of citizens" in Vietnamese legal theory, which conceives citizen rights as inseparable from social responsibility (Tran, 2011). Articles 14 and 15 of the *Constitution (Vietnam) 2013* establish the principle that human rights and citizens' rights are associated with citizens' obligations to the state and society. In the context of personal data, this is embodied in Article 4(2) of the *V-PDPL*, which establishes six obligations of data subjects: (1) self-protection of personal data; (2) demanding protection from relevant organizations and individuals; (3) respecting and protecting others' personal data; (4) providing complete and accurate personal data when consenting to processing; (5)

participating in propagation and dissemination of data protection skills and (6) complying with legal provisions on personal data protection and participating in prevention and combat of violations. This constitutional grounding distinguishes Vietnam's approach from pure *GDPR* transplantation, which establishes comprehensive data subject rights ('Regulation (EU) 2016/679', 2016, Articles 12–23) without corresponding individual obligations beyond cooperation with supervisory authorities during investigations. This difference represents not only regression from international standards but creative adjustment consistent with legal transplantation theory, wherein reception of foreign laws requires "localization" to suit indigenous social conditions (Watson, 1993, p. 97; Tran and Le, 2022, p. 181).

3. The transformation from pre-inspection to post-inspection in cross-border data management reflects the maturity of Vietnam's governance thinking on personal data protection. The *Cybersecurity Law (Vietnam) 2018*, which mandates domestic data storage, has faced criticism for potentially impeding the growth of the digital economy and limiting international integration (Le, 2021, pp. 97–99). The *V-PDPL* addresses concerns of both domestic and international businesses regarding data localization requirements by adopting markedly open approach: adequacy assessments of "equivalent protection" are not required for cross-border transfers; businesses need only complete outbound transfer impact assessment within 60 days from commencement of processing, which means that transfers may occur first and be assessed thereafter (*Personal Data Protection Law (Vietnam)*, 2025, Article 20(2)). The TIA's primary function facilitates inspections and regulatory oversight aimed at preventing data-security violations rather than establishing ex-ante approval requirement. Article 39(2) of the *V-PDPL* provides that impact assessment dossiers on personal data processing and cross-border transfers submitted under 'Decree 13/2023/ND-CP' before the effective date of the Law shall remain valid, reflecting the principle of non-retroactivity and respect for the legitimate expectations of compliant enterprises, thereby ensuring legal stability in the business environment and reducing unnecessary compliance burdens. Consistent with this orientation, the current draft of the new Law on Cybersecurity no longer imposes data-localization obligations, instead refocusing on safeguarding national security and countering technology-enabled threats to public order and social safety (*Draft Law on Cybersecurity (Vietnam)*, 2025). Article 20(6) of the *V-PDPL* also defines six categories where cross-border transfers are not permitted, focusing on

governmental data and sensitive public-sector information rather than general commercial data, maintaining security controls over genuinely sensitive information while liberalizing commercial data flows. This regulatory evolution is likely to support SMEs and technology start-ups that rely on cross-border data flows and international cloud services for commercial purposes, which are subject only to restrictions for core datasets implicating national security interests.

4.2.2 AI integration: rationale, architecture and critical gaps

Vietnam's integration of AI governance within the *V-PDPL* distinguishes it globally and regionally. While the EU employs parallel instruments (the *GDPR* and the *AI Act*) and Singapore addresses AI through soft-law *Model AI Governance Framework*, separate from *PDPA*, the *V-PDPL* (Article 30) directly regulates AI systems processing personal data within primary data protection statute. This choice reflects both pragmatic and principled considerations. The integrated approach stems from a recognition that contemporary AI systems fundamentally constitute data processing operations. Machine-learning algorithms require vast personal data for training, automated decision-making systems process individual information to generate outputs affecting data subjects and generative AI may reproduce personal data embedded in training sets. Separating AI governance from data protection would create artificial distinctions between inseparable operations. Vietnam's approach acknowledges this technological reality that AI is data processing and therefore belongs within data protection law rather than serves as a parallel regulatory instrument.

Legislative context reinforces this logic. Vietnam concurrently enacted the *V-DTIL* and *Law on Data (Vietnam) 2025*, creating an integrated corpus for digital governance. The *V-DTIL* addresses AI systems comprehensively, establishing classification frameworks, high-risk AI systems versus AI systems with significant impact per Article 43 and sector-specific obligations for AI developers and deployers. Article 30 of the *V-PDPL* complements this by focusing specifically on personal data dimensions, ensuring that AI data processing respects individual rights and implements appropriate safeguards. This division of labor prevents duplication while ensuring comprehensive coverage as the *V-DTIL* governs AI system safety, performance and market conduct and the *V-PDPL* governs personal data protection dimensions of AI deployment.

Integration offers potential advantages over separation observable in the EU's dual-regulation model. It prevents coordination challenges determining

jurisdictional boundaries between the authorities of the *GDPR* and the *AI Act*, reconciling overlapping requirements (data quality standards, transparency obligations, automated decision-making provisions) and managing separate enforcement proceedings where single AI system violates both frameworks. For businesses, single-framework compliance reduces transaction costs relative to navigating parallel regimes with potentially conflicting interpretations. For individuals, a unified rights regime provides clearer pathways for redress when AI processing violates data protection principles—a single supervisory authority (Ministry of Public Security) rather than coordinating between data protection authorities and AI oversight bodies.

Article 30 of the *V-PDPL* establishes three core requirements governing AI systems processing personal data.

1. Article 30(1) mandates that all systems and services employing AI technologies must integrate appropriate personal data security measures and employ appropriate authentication, identification, and access authorization methods for personal data processing. This general obligation parallels Article 32 of the *GDPR* on security requirements and Article 15 of the *AI Act* on accuracy, robustness and cybersecurity provisions, but lacks specificity what constitutes "appropriate" for AI contexts and remains undefined, necessitating implementing regulations establishing concrete standards.

2. Article 30(2) requires AI-based personal data processing to be classified according to risk level to ensure that appropriate safeguards are implemented. This risk-based approach aligns with international best practice. The EU *AI Act* employs risk stratification, Singapore's *Model AI Governance Framework* uses similar tiering, and OECD's *AI Principles* emphasize proportionate governance matching risk levels. Yet, Article 30 of the *V-PDPL* provides no classification criteria or risk-level definitions. The dual categorization, high-risk AI systems of the *V-DTIL* (Article 43(1)), defined by use case and application domain, versus AI systems with significant impact (Article 43(2)), defined by deployment scale and affected population, does not align perfectly with risk-level logic that would require hierarchical stratification.

3. Article 30(3) prohibits AI processing that poses a threat to national defense, security, public order, safety or infringes on individual rights to life, health, honor, dignity or property. This prohibition establishes boundaries through general principles rather than specific enumerated

practices, comparable to the detailed prohibition practices outlined in Article 5 of the *AI Act*, thus raising concerns about potential overreach where authorities construe broadly to restrict legitimate AI applications.

Critical gaps emerge from this analysis beyond definitional ambiguities. Article 30 of the *V-PDPL* lacks AI-specific data subject rights that would address significant protection deficit in automated decision-making relative to international standards. Article 22 of the *GDPR* provides the right not to be subject to decisions based solely on automated processing that have legal or similarly significant effects, establishing individual autonomy protection against algorithmic determinism. EU's *AI Act* supplements this through human oversight requirements, outlined in Article 14, and transparency obligations in Article 13 enabling affected persons to understand decision logic. Singapore's *Model AI Governance Framework*, though non-binding, recommends providing explanations for AI decisions and establishing human review mechanisms. Vietnam's *PDPL* contains no equivalent provisions. Its Article 9 establishes general data subject rights (information, consent, access, rectification, erasure, portability, objection) and Article 10 addresses consent withdrawal and restriction, but neither provision specifically addresses automated decision-making scenarios. Data subjects may not know when AI makes decisions that affect them (no disclosure requirement), cannot demand human intervention in algorithmic determinations (no override right) and lack entitlements to understand decision logic or contest outcomes (no explanation or review rights). An individual denied credit based on AI scoring, rejected for employment through automated screening or subjected to differential pricing via algorithmic profiling possesses no specific legal remedies under the *V-PDPL* beyond general access and rectification rights insufficient for addressing algorithmic harms. Institutional responsibilities in Vietnam present certain ambiguity. The *V-DPPL* designates the Ministry of Public Security as the law general supervisory (Article 30) and enforcement authority (Article 36), whereas the *V-DTIL* assigns oversight of AI systems to the Ministry of Science and Technology (Articles 43–47). Therefore, when AI systems process personal data—which the vast majority of AI applications do—it remains unclear which ministry holds primary jurisdiction. Article 30 of the *V-PDPL* provides no inter-ministerial coordination mechanism, nor does the law establish clear jurisdictional allocation principles, creating potential risk of overlapping mandates, enforcement gaps and duplicative proceedings that could impose excessive burdens on regulated entities.

4.2.3 Implementation pathways and prospects of regional harmonization

Effective implementation requires addressing the identified gaps through multi-level interventions. In the short term, implementing regulations must harmonize Article 30 of the *V-PDPL* with Article 43 of the *V-DTIL* by creating unified risk classification scheme integrating the categorizations of both frameworks. Building on this foundation, it would be appropriate to consider adopting a three-tier risk assessment scheme tailored to Vietnam's institutional context:

1. *Prohibited AI.* Practices incompatible with fundamental rights and public interests, including AI systems deploying subliminal manipulation or exploitation of vulnerabilities causing significant harm, social scoring by public authorities producing discriminatory effects, indiscriminate surveillance violating privacy without legitimate security justification and deepfakes or synthetic media designed to deceive and cause harm; (
2. *High-risk AI.* Systems requiring comprehensive safeguards including mandatory data protection impact assessments, human oversight mechanisms, transparency requirements, accuracy and robustness standards, as well as post-deployment monitoring, encompassing biometric identification and categorization systems, AI in critical infrastructure sectors, employment and education applications affecting individual opportunities, essential public and private services (healthcare, financial services, social services) and law enforcement applications;
3. *Lower-risk AI.* Systems subject to basic data security and transparency obligations without extensive procedural requirements, covering general-purpose AI not deployed in high-risk contexts, customer service chatbots and virtual assistants, personalization and recommendation systems with limited individual impact, as well as productivity tools that support human decision-making.

This scheme should explicitly map the categories of the *V-DTIL*, with "high-risk AI systems" generally corresponding to Tier 2 high-risk category, while "AI systems with significant impact" may span Tier 2 or Tier 3 depending on whether deployment domain qualifies as inherently high-risk under domain criteria or whether scale alone creates risk elevation that requires enhanced safeguards. Implementing regulations should establish a classification based on a decision tree: first assess whether system falls in prohibited category; if permitted, evaluate whether use case matches the high-risk

domain criteria; if not inherently high-risk domain, assess whether scale and potential impact warrant Tier 2 classification; otherwise default to Tier 3 with baseline requirements.

Regulations should also define "appropriate safeguards" concretely per risk tier, operationalizing general mandate of Article 30(2). High-risk AI must implement

- Mandatory data protection impact assessments conducted before deployment and updated annually or upon material system changes, evaluating algorithmic bias and discrimination risks, assessing data quality and representativeness, analyzing security vulnerabilities and identifying potential rights impacts;
- Human oversight mechanisms enabling intervention in automated decisions, providing meaningful human review for consequential determinations, establishing clear responsibility allocation between AI systems and human operators and ensuring oversight personnel possess requisite competence;
- Transparency requirements, including logic disclosure, explaining general decision-making principles, providing individual explanations for specific decisions affecting data subjects, documenting training data sources and preprocessing methods and publishing accuracy metrics and performance evaluations;
- Ongoing monitoring and audit procedures tracking system performance against established metrics, detecting accuracy degradation or bias emergence, logging significant decisions for review and conducting periodic independent audits; and
- Incident reporting obligations notifying the Ministry of Public Security within 72 hours when AI processing causes data breaches, produces systematically biased outcomes that are discovered post-deployment or generates decisions resulting in significant individual harm.

Institutionally, an inter-ministerial coordination mechanism should be established to address jurisdictional ambiguities between Ministry of Public Security and Ministry of Science and Technology. A joint committee on AI data processing oversight is proposed, with clearly delineated responsibilities:

- The Ministry of Public Security leads on personal data protection dimensions including data subject rights enforcement, consent and lawful basis compliance, cross-border transfer oversight and privacy-related sanctions;
- At the same time, the Ministry of Science and Technology leads on AI system safety and performance including technical standards

compliance, quality management systems, conformity assessment and market surveillance; and
- A joint authority for AI systems presents both data protection and safety concerns requiring coordinated investigation and enforcement, with procedural rules establishing lead agency designation, information sharing protocols, and unified enforcement decisions avoiding conflicting orders.

This model balances specialized expertise with coordinated enforcement—the Ministry of Public Security possesses expertise in data protection and established enforcement infrastructure through Department A05 and the Ministry of Science and Technology brings AI technical expertise and sectoral knowledge from the implementation of the *V-DTIL*.

Vietnam's integrated approach offers a potential template for the harmonization of the ASEAN, though adaptation will require accounting for the diverse institutional contexts and development priorities of the member states. The ASEAN *Digital Economy Framework Agreement* (DEFA) commits members to developing coordinated digital economy governance, establishing political grounds for the development of regional framework (ASEAN, 2023b). Vietnam's experience—both successes in establishing early AI governance framework and challenges requiring solutions to implementation—provides an empirical foundation for ASEAN learning. ASEAN could adopt a principles-based AI data governance framework that would build on Vietnam's integration logic while allowing flexibility in implementation:

- A risk-based approach establishing prohibited practices, high-risk obligations and baseline requirements, with member states defining specific risk categories matching domestic contexts; mandatory transparency for automated decisions affecting individuals;
- Human oversight for high-impact AI;
- Data quality and bias mitigation requirements; and
- Cross-border AI data flow mechanisms with appropriate safeguards enabling regional data exchange.

ASEAN member states could implement through preferred institutional models—integrated within data protection law (Vietnam's approach), separate AI legislation (EU's approach) or soft-law guidelines (Singapore's approach) while maintaining regional interoperability through shared foundational principles. Hence, rapid codification of personal data protection and governance rules will play a crucial role in promoting the effective and

secure development of e-commerce both within ASEAN and in its external trade relations.

5. Conclusion

The emergence of the *GDPR* as a global benchmark has profoundly shaped regulatory developments across ASEAN through the Brussels Effect mechanisms operating via economic, normative and legal channels. Yet, this influence produces selective translation rather than comprehensive transplantation—ASEAN-6 states adopt core data protection principles (consent mechanisms, data subject rights, breach notification, cross-border transfer safeguards) while resisting or adapting provisions threatening sovereignty, exceeding developmental capacities or conflicting with institutional path dependencies. This pattern manifests through temporal clustering—pre-*GDPR* frameworks (Singapore, Malaysia and Philippines) initially drew from the OECD–APEC templates before post-2018 amendments incorporated *GDPR*-influenced provisions, while post-*GDPR* frameworks (Thailand, Indonesia and Vietnam) explicitly modeled on European standards from inception. Persistent divergences on data localization, institutional models and cross-border transfer mechanisms reveal structural limits to regulatory diffusion imposed by national security imperatives, constitutional traditions and strategic economic positioning.

Vietnam's integrated approach to data protection and AI governance marks a distinctive innovation in ASEAN. By embedding AI oversight within Article 30 of the *V-PDPL* rather than adopting separate legislation, Vietnam recognizes AI as a form of personal data processing that requires unified supervision. This contrasts with the EU's dual *GDPR–AI Act* model and Singapore's non-binding soft-law framework. The evolution from fragmentation toward integration in Vietnam's regulatory trajectory illuminates broader dynamics of legal transplantation in the digital age, demonstrating how emerging economies navigate global regulatory pressures and domestic governance imperatives, selectively adopting international standards while preserving institutional autonomy and developmental flexibility essential for an AI-driven digital transformation.

The effective implementation of the *V-PDPL* in Vietnam still depends on addressing some factors, particularly gaps in automated decision-making rights and coordination between relevant ministries. Nonetheless,

Vietnam's experience provides an empirical foundation for developing an ASEAN principles-based framework that balances regulatory flexibility with regional interoperability through shared elements—prohibited AI uses, high-risk obligations, transparency requirements and safeguarded cross-border data flows.

Acknowledgment

The research is funded by Vietnam National Foundation for Sciences and Technology Development (NAFOSTED) grant No. 505.01.2023.03.

Cong Tran Quoc Le is a lecturer of law at the International Law Faculty of Ho Chi Minh City University of Law (HCMUL), Vietnam, where he teaches international trade law, international commercial arbitration law and business law in the digital economy. He holds a Master of Laws, majoring in international and comparative business law, from the University of Bordeaux, France (2015). He is currently a PhD candidate at HCMUL. He was a research fellow at the Centre of Comparative, European and International Law and the Faculty of Law and Criminal Sciences (CDCEI), University of Lausanne (UNIL) under the European Commission financed Horizon 2020 Research and Innovation Staff Exchange Project (2018). His research is mainly related to legal issues in digital economy and e-commerce, including data privacy, AI liability, fintech and cyber security.

Dr **Viet Dung Tran** is an associate professor at Ho Chi Minh City University of Law (HCMUL), Vietnam. In addition to his role at HCMUL, he also lectures at several prestigious regional and global universities, including Chulalongkorn University, Chonnam National University, Dong-A University, Bristol Law School, the University of Toulouse, the University of Bordeaux, Paris II Panthéon-Assas, the National University of Singapore, Singapore Management University and Universitas Indonesia. He has served as a Deputy Editor-in-Chief of the *Vietnamese Journal of Legal Sciences* since 2019. As an international lawyer, Dr Dung combines academic knowledge with practical experience. He has practiced law in Singapore for Wong Partnership and KhattarWong over six years before becoming a senior consultant at DL & Partners, a leading law firm in Vietnam. He is also a chartered arbitrator of the Vietnam International Arbitration Centre (VIAC).

Dao Phuong Thuy Nguyen is a lecturer at the Faculty of International Law, Ho Chi Minh City University of Law (HCMUL), Vietnam. She holds an LLM from Bristol Law School (UWE) and currently pursues the PhD program at Palacký University Olomouc, Czech Republic. Her research focuses on international economic law, law and technology, responsible business practices and the interaction between trade and environmental governance. At HCMUL, she teaches courses on international trade law, ASEAN trade law, international sales of goods and e-commerce. She has participated in several academic projects and conferences in Europe and Southeast Asia, aiming to foster comparative perspectives on legal integration and sustainable governance in the global economy.

References

Alfred, D.N. (2020) *Navigating the road ahead: insights into the policy rationale of the PDP (Amendment) Bill 2020*. Singapore: Personal Data Protection Commission Singapore. Available at: https://www.pdpc.gov.sg/-/media/Files/PDPC/DPO-Connect/November-20/Navigating-the-Road-Ahead.html (Accessed: 20 May 2025).

Alibeigi, A. and Munir, A.B. (2020) 'Malaysian Personal Data Protection Act, a mysterious application', *University of Bologna Law Review*, 5(2), pp. 363–372. Available at: https://doi.org/10.6092/issn.2531-6133/12441

Amiludin, A., Nurhalisa, S., Prasetya Umara, U. and Hidayatullah, M. (2024) 'Comparison of protection laws private data in Indonesia, and the Philippines', *Jurisprudence*, 14(2), pp. 171–191. Available at: https://doi.org/10.23917/jurisprudence.v14i2.4266

APEC (2019) *APEC Cross-Border Privacy Rules (CBPR) policies, rules and guidelines* (revised September 2019). Available at: https://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf (Accessed: 20 May 2025).

Artzt, M. and Tran, V.D. (2022) 'Artificial intelligence and data protection: how to reconcile both areas from the European law perspective', *Vietnamese Journal of Legal Sciences* (Ho Chi Minh City University of Law), 7(2), pp. 39–58. Available at: https://doi.org/10.2478/vjls-2022-0007

ASEAN (2016) *ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN): framework on personal data protection*. Available at: https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf (Accessed: 20 May 2025).

ASEAN (2021) *ASEAN digital masterplan 2025*. Jakarta: ASEAN Secretariat. Available at: https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf (Accessed: 20 May 2025).

ASEAN (2023a) *Framework for Negotiating ASEAN Digital Economy Framework Agreement*. Available at: https://asean.org/wp-content/uploads/2023/09/Framework-for-Negotiating-DEFA_ENDORSED_23rd-AECC-for-uploading.pdf (Accessed: 20 May 2025).

ASEAN (2023b) *Leaders' statement on the development of the ASEAN Digital Economy Framework Agreement (DEFA)*. Available at: https://asean.org/wp-content/uploads/2023/09/Leaders-Statement-DIGITAL-ECONOMY-FRAMEWORK-AGREEMENT.pdf (Accessed: 20 May 2025).

ASEAN Briefing (2024) 'Navigating personal data protection in Indonesia'. Available at: https://www.aseanbriefing.com/news/navigating-personal-data-protection-in-indonesia (Accessed: 20 May 2025).

Baker McKenzie (2024a) 'Malaysia Personal Data Protection (Amendment) Act 2024 to come into force', *Baker McKenzie InsightPlus*. Available at: https://insightplus.bakermckenzie.com/bm/data-technology/malaysia-personal-data-protection-amendment-act-2024-to-come-into-force (Accessed: 7 October 2025).

Baker McKenzie (2024b) 'Thailand: new cross-border data transfer rules officially published as law', *Baker McKenzie InsightPlus*. Available at: https://insightplus.bakermckenzie.com/bm/data-technology/thailand-new-cross-border-data-transfer-rules-officially-published-as-law (Accessed: 13 March 2025).

Baker McKenzie (2024c) 'Thailand: PDPA compliance and challenges—development of the insurance industry in 2024', *Baker McKenzie InsightPlus*. Available at: https://insightplus.bakermckenzie.com/bm/financial-institutions_1/thailand-pdpa-compliance-and-challenges-development-of-the-insurance-industry-in-2024 (Accessed: 13 March 2025).

Barocas, S. and Selbst, A.D. (2016) 'Big data's disparate impact', *California Law Review*, 104(3), pp. 671–732. Available at: https://doi.org/10.2139/ssrn.2477899

Berg, C. (2018) 'A classical liberal approach to privacy', in *The classical liberal case for privacy in a world of surveillance and technological change*. Palgrave Studies in Classical Liberalism. Cham: Palgrave Macmillan, pp. 47–68. Available at: https://doi.org/10.1007/978-3-319-96583-3_3

Bradford, A. (2020) *The Brussels Effect: how the European Union rules the world*. New York: Oxford University Press. Available at: https://doi.org/10.1093/oso/9780190088583.001.0001

Chik, W.B. (2013) 'The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform', *Computer Law & Security Review*, 29(5), pp. 554–575. Available at: https://doi.org/10.1016/j.clsr.2013.07.010

Ching, M.R.D., Fabito, B. and Celis, N.J. (2018) 'Data Privacy Act of 2012: a case study approach to Philippine government agencies' compliance', *Advanced Science Letters*, 24(10), pp. 7042–7046. Available at: https://doi.org/10.1166/asl.2018.12404

Dat, H.L.N.T. and An, C.T.T. (2024) 'The regulation of data transmission in the digital era: from the European Union's perspective and implications for Vietnam', *Vietnamese Journal of Legal Sciences*, 11(2), pp. 1–13. Available at: https://doi.org/10.2478/vjls-2024-0007

Data Privacy Act (Philippines) (2012) Republic Act No. 10173, Republic of the Philippines Congress of the Philippines, 15 August.

'Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems' (2020) (Schrems II), Case C-311/18, ECLI:EU:C:2020:559, 16 July.

'Decree No. 13/2023/ND-CP of the Government on personal data protection (Vietnam)' (2023) Government Socialist Republic of Vietnam, 17 April.

Desiderio, L. (2021) 'NPC pushes amendments to Data Privacy Act', *The Philippine Star*, 27 June. Available at: https://www.philstar.com/business/2021/06/27/2108309/npc-pushes-amendments-data-privacy-act (Accessed: 7 October 2025).

Digital Policy Alert (2024) 'DPA Digital Digest: Philippines'. Available at: https://digitalpolicyalert.org/digest/dpa-digital-digest-philippines (Accessed: 7 October 2025).

Draft Law on Cybersecurity (Vietnam) (2025) Available at: https://duthaoonline.quochoi.vn/dt/luat-an-ninh-mang/250714085609949149 (Accessed: 27 May 2025).

EDPB (2018a) *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, European Data Protection Board. Brussels: EDPB.

EDPB (2018b) *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)—version adopted after public consultation*, European Data Protection Board. Brussels: EDPB.

EDPB (2020) *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, European Data Protection Board. Brussels: EDPB.

EDPB (2023) *Guidelines 07/2022 on certification as a tool for transfers*, European Data Protection Board. Brussels: EDPB. Available at: https://www.edpb.europa.eu/system/files/2023-02/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf (Accessed: 10 January 2025).

European Commission (2021) 'Adequacy decisions'. Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions (Accessed: 7 October 2025).

European Commission, Directorate-General for Trade (2024) 'EU trade relations with Thailand'. Available at: https://policy.trade.ec.europa.eu/eu-trade-

relationships-country-and-region/countries-and-regions/thailand_en (Accessed: 6 October 2025).

Eurostat (no date) 'Population and population change statistics'. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Population_and_population_change_statistics (Accessed: 10 January 2025).

Framework Agreement on Comprehensive Partnership and Cooperation between the European Union and its Member States, of the One Part, and the Socialist Republic of Vietnam, of the Other Part (2016) *Official Journal* L 329/8, 3 December.

'Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)' (2019) Case C-507/17, ECLI:EU:C:2019:772, 24 September.

'Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' (2014) Case C-131/12, ECLI:EU:C:2014:317, 13 May.

Government of Vietnam (2024) 'Proposal for the development of the Law on Personal Data Protection'. Available at: https://chinhphu.vn/du-thao-vbqppl/ho-so-de-nghi-xay-dung-luat-bao-ve-du-lieu-ca-nhan-6312 (Accessed: 7 October 2025).

'Government Regulation No. 71 of 2019 on the organization of electronic systems and transactions (Indonesia)' (2019) *State Gazette of the Republic of Indonesia*, No. 185, 10 October.

Habibulloh, M. (2025) 'Digital governance and the right to privacy: a comparative analysis of AI regulation in Southeast Asia and the European Union', *Journal of Law, Policy and Global Development*, 1(1), pp. 19–35. Available at: https://doi.org/10.71305/jlpgd.v1i1.333

Infocomm Media Development Authority and Personal Data Protection Commission Singapore (2022) *Model AI governance framework*. 2nd edn. Available at: https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework (Accessed: 7 October 2025).

Islam, M.T. and Karim, M.E. (2020) 'Extraterritorial application of the EU General Data Protection Regulation: an international law perspective', *IIUM Law Journal*, 28(2), pp. 531–565. Available at: https://doi.org/10.31436/iiumlj.v28i2.495

Kamara, I. and De Hert, P. (2018) 'Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach', *Brussels Privacy Hub Working Paper*, 4(12). Available at: https://doi.org/10.2139/ssrn.3228369

Kesa, A. and Kerikmäe, T. (2020) 'Artificial intelligence and the GDPR: inevitable nemeses?', *TalTech Journal of European Studies*, 10(3), pp. 68–90. Available at: https://doi.org/10.1515/bjes-2020-0022

Kohl, U. (2022) 'The long-arm of the GDPR and its inherent weakness – the EDPB's Guidelines 05/2021 on the interplay of Article 3 and Chapter v. of the GDPR'. Available at: https://doi.org/10.2139/ssrn.4027796

Law No. 27 of 2022 on Personal Data Protection (Indonesia) (2022) Supplement to the *State Gazette of the Republic of Indonesia*, No. 6820.

Law No. 96/2025/QH15 on Digital Technology Industry (Vietnam) (2025) National Assembly, 26 June.

LawAsia (2025) 'Thailand: data privacy laws'. Available at: https://law.asia/thailand-data-privacy-laws/ (Accessed: 6 October 2025).

Le, T.Q.C. (2021) 'Quy định về tự do dữ liệu trong hiệp định thương mại tự do thế hệ mới - tác động đối với pháp luật Việt Nam' (Regulations on freedom of data in new generation free trade agreements—impact on Vietnamese law), *Vietnamese Journal of Legal Sciences*, 146(07), pp. 95–106.

Lee, A. (2021) 'Personal data, global effects: China's draft privacy law in the international context', *Stanford University DigiChina Project*. Available at: https://digichina.stanford.edu/work/personal-data-global-effects-chinas-draft-privacy-law-in-the-international-context/ (Accessed: 7 October 2025).

McKean, R., Magee, J. and de Souze, R. (2025) 'DLA Piper GDPR fines and data breach survey: January 2025', *DLA Piper*. Available at: https://www.dlapiper.com/en-us/insights/publications/2025/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2025 (Accessed: 10 January 2025).

Ministry of Public Security (Vietnam) (2024) 'Submission No. 246/TTr-BCA-A05 to the Government on the dossier proposing the development of the Personal Data Protection Law', 17 June. Available at: https://congan.tayninh.gov.vn/vi/chi-tiet-tin-tuc?Id=225214 (Accessed: 24 April 2025).

Norton Rose Fulbright (no date) 'Overview of Thailand Personal Data Protection Act B.E. 2562 (2019)'. Available at: https://www.nortonrosefulbright.com/en/knowledge/publications/e29d223d/overview-of-thailand-personal-data-protection-act-be2562-2019 (Accessed: 6 October 2025).

OECD (2013) *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (Accessed: 24 April 2025).

OECD (2019) *Recommendation of the Council on artificial intelligence*. OECD Legal Instruments, OECD/LEGAL/0449. Paris: OECD Publishing.

PDPC Malaysia (2022) *Personal data protection guidelines on cross-border transfer of personal data (CBPDT)*, Personal Data Protection Commission Malaysia. Available at: https://www.pdp.gov.my/ppdpv1/en/akta/personal-data-protection-guidelines-on-cross-border-transfer-of-personal-data-cbpdt/ (Accessed: 7 October 2025).

PDPC Singapore (2020) *Model AI governance framework*, Personal Data Protection Commission Singapore. Available at: https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework (Accessed: 7 October 2025).

PDPC Singapore (2021) 'APEC Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems', Personal Data Protection Commission Singapore. Available at: https://www.pdpc.gov.sg/help-and-resources/2021/10/apec-cross-border-privacy-rules-and-privacy-recognition-for-processors-systems (Accessed: 15 March 2025).

Personal Data Protection Act (Thailand) (2019) B.E. 2562, *Government Gazette*, No. 136, chapter 69 Gor, 27 May.

Pitogo, V. (2019) 'National government agency's compliance on Data Privacy Act of 2012: a case study, Philippines', *Journal of Physics: Conference Series*, 1201(1), article 012021. Available at: https://doi.org/10.1088/1742-6596/1201/1/012021

Pramesti, I. and Afriansyah, A. (2020) 'Extraterritoriality of data protection: GDPR and its possible enforcement in Indonesia', in *Advances in Economics, Business and Management Research: Proceedings of the 3rd International Conference on Law and Governance (ICLAVE 2019)*. Paris: Atlantis Press, pp. 83–94. Available at: https://doi.org/10.2991/aebmr.k.200321.012

'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)' (2016) *Official Journal* L 119/1, 27.4.2016.

'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (2024) *Official Journal* L 2024/1689, 13.6.2024.

Rustad, M.L. and Koenig, T.H. (2019) 'Towards a global data privacy standard', *Florida Law Review*, 71(2), pp. 365–453. Available at: https://scholarship.law.ufl.edu/flr/vol71/iss2/3 (Accessed: 15 March 2025).

Shivhare, S. (2025) 'Malaysia charts its digital course: a guide to the new frameworks for data protection and AI ethics', *Future of Privacy Forum*, 6 July. Available at: https://fpf.org/blog/malaysia-charts-its-digital-course-a-guide-to-the-new-frameworks-for-data-protection-and-ai-ethics/ (Accessed: 7 October 2025).

Sudirman, L., Disemadi, H. and Aninda, A. (2023) 'Comparative analysis of personal data protection laws in Indonesia and Thailand: a legal framework perspective', *JED (Jurnal Etika Demokrasi)*, 8(4), pp. 497–510. Available at: https://doi.org/10.26618/jed.v8i4.12875

Tan, O.S.L., Vergara, R.G. and Khan, S. (2021) 'Digital tracing and Malaysia's Personal Data Protection Act 2010 amid the COVID-19 pandemic', *Asian Journal of Law and Policy*, 1(1), pp. 47–62. Available at: https://doi.org/10.33093/ajlp.2021.3

Tran, N.D. (2011) *Quyền con người, quyền công dân trong Nhà nước pháp quyền xã hội chủ nghĩa Việt Nam* (Human rights, citizens' rights in the socialist rule of law state of Vietnam*)*. Hanoi: National Political Publishing House.

Tran, V.D. (2024) 'Bàn về phát triển quy phạm đạo đức trong tiến trình xây dựng pháp luật về trí tuệ nhân tạo' (On the development of ethical norms in the process of building artificial intelligence legislation), *Vietnam Journal of Legal Sciences*, 9(181). Available at: https://doi.org/10.70236/tckhplvn.115

Tran, V.D. and Le, C.T.Q. (2022) 'Developing a regulatory framework for autonomous vehicles: a proximal analysis of European approach and its application to ASEAN countries', *TalTech Journal of European Studies*, 12(2), pp. 165–188. Available at: https://doi.org/10.2478/bjes-2022-0016

Watson, A. (1993) *Legal transplants: an approach to comparative law*. 2nd edn. Athens, GA: University of Georgia Press.

Wong, B. (2019) 'Data localization and ASEAN Economic Community', *Asian Journal of International Law*, 10(1), pp. 158–180. Available at: https://doi.org/10.1017/S2044251319000250

Yeung, K. and Bygrave, L.A. (2022) 'Demystifying the modernized European data protection regime: cross-disciplinary insights from legal and regulatory governance scholarship', *Regulation & Governance*, 16(1), pp. 137–155. Available at: https://doi.org/10.1111/rego.12401