

ANALYZING THE SCOPE OF APPLICATION AND FUNDAMENTAL CONCEPTS OF PERSONAL DATA PROTECTION IN THE DIGITAL ERA: FROM MALAYSIA'S PERSPECTIVE AND EXPERIENCE FOR VIETNAM

NGUYEN HOANG PHUOC HANH

Faculty of Commercial Law, Ho Chi Minh City University of Law, Vietnam

Email: nhphanh@hcmulaw.edu.vn

PHAM PHUONG THAO

The Supreme People's Court of Vietnam, Vietnam

Email: phuongthao.tatc@gmail.com

Abstract

Over the past decades, the Malaysian government has acknowledged the pressing need to regulate personal data protection, becoming the first country in Southeast Asia to recognize this urgent requirement, and as a result, the 2010 Malaysian Personal Data Protection Act was enacted and later entered into force in 2013 in response to the increasing importance of personal data protection in this digital age. On 24 December 2024, the 2024 Malaysian Personal Data Protection (Amendment) Act was enacted and came into force in 2025. The most fundamental step in evaluating a piece of legislation is understanding its scope and application. For this reason, this article covers key aspects of the Malaysian 2024 Personal Data Protection Act, including its scope of application in Malaysia and several fundamental concepts, namely personal data, sensitive personal data, and the roles of data controller and data processor. Furthermore, this article compares Malaysia's approach with the current situation in Vietnam to offer insights for the development of Vietnam's data protection policies, with the hope of highlighting the importance of regulatory clarity and cross-border data handling, to contribute to Vietnam's legal improvements in personal data protection amidst a rapid digital revolution.

Keywords: data subject, personal data, data processor, sensitive data, Vietnam, Malaysia

Received: 30 September 2024

Revised: 23 February 2025

Accepted: 16 April 2025

Malaysia and Vietnam, as developing countries, both experienced a series of remarkable economic and technological advancements in alignment with the Fourth Industrial Revolution. Experts predict that, in the near future, technology will gradually dominate over every aspect of life, including society, education, economy.¹ Given this anticipated shift, it is critical to evaluate whether the current data protection frameworks in Malaysia and Vietnam are sufficient to ensure the security and privacy of personal data in this rapidly evolving landscape. In Malaysia, the implementation of the 2010 Personal Data Protection Act and later the 2024 Amendment Act ("PDPA")

¹ Lee, R., Janna, A. (2023 June 21). *As AI spreads, experts predict the best and worst changes in digital life by 2035*. Pew Research Center. <https://espas.secure.europarl.europa.eu/orbis/document/ai-spreads-experts-predict-best-and-worst-changes-digital-life-2035>

has laid a foundational framework for data protection, yet challenges remain in its enforcement and compliance.²

In 2020, Vietnam began to launch a digital transformation campaign on a national scale, which includes three pillars: digital government, digital economy and digital society.³ The key element of digital transformation is the development of technology based on the rapid growth of information and data. E-commerce transactions, however, carry many potential concerns, especially regarding the protection of personal information. In practice, very few businesses have safeguards for the sensitive information voluntarily provided by their employees.⁴ The Department of Cyber Security and High-Tech Crime Prevention under the Ministry of Public Security⁵ stated that in the last 5 years, the world has witnessed a series of cases of personal data infringement. For example, the personal data of 235 million Instagram, TikTok, Youtube accounts were leaked online.⁶

To deal with this situation, the Ministry of Public Security was drafting and collecting opinions from agencies, ministries, and departments. In 2023, the Government issued Decree No. 13 on protecting personal data (“Decree No. 13”), which came into effect officially on 01 July 2023. The Decree regulates the protection of personal data and the responsibilities of relevant agencies, organizations and individuals in protecting personal data. According to the Deputy Head of the Banking Association, some provisions of Decree No. 13⁷ are too general, such as Article 9, which stipulates the rights of data subjects, only provides general provisions on the rights, but lacks specific ones on the right to transfer data or the right to request data modification. Moreover, Decree No. 13 completely lacks specific limitations on AI systems, big data, or Blockchain. This Decree has not yet been consistently and broadly implemented into practice since its promulgation.⁸ For instance, the operations

- 2 Bach, T.N.N. (2023). Addressing the challenges of Data Privacy Protection Law in Vietnam. *VNU Journal Of Science: Legal Studies*, 39(1). <https://doi.org/10.25073/2588-1167/vnuls.4413>
- 3 Decision No. 749/QĐ-TTg dated June 3, 2020 approving the National Digital Transformation Program through 2025, with orientations toward 2030.
- 4 Ebert, I., Wildhaber, I., & Adams-Prassl, J. (2021). Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection. *Big Data & Society*, 8(01). <https://doi.org/10.1177/20539517211013051>
- 5 Minh, T. (2020 January 3). Department of Cyber security and Hi-tech Crime Prevention requested to effectively prevent cyber crimes. *Public Security News*. <https://en.cand.com.vn/public-security-forces/Department-of-Cyber-Security-and-Hi-tech-Crime-Prevention-requested-to-effectively-prevent-cyber-crimes-i549548/>
- 6 Hai, T. (2020 December 22). Hoàn thiện khung pháp lý bảo vệ dữ liệu cá nhân. *Báo điện tử Đại biểu Nhân dân* [Completing the legal framework to protect personal data. *Electronic newspaper of People's Deputies*]. <https://daibieunhandan.vn/Giai-dap-phap-luat/Hoan-thien-khung-phap-ly-bao-ve-du-lieu-ca-nhan-i257562/>
- 7 Nhue, M. (2023 June 29). Nghị định 13 sẽ rất vướng mắc nếu áp dụng cứng nhắc và không có quan điểm hướng dẫn thống nhất. *Đầu tư & Phát triển* - Trang chuyên của Báo Đầu tư. [Decree No. 13 will be very problematic if applied rigidly and without a unified guiding perspective. *Stock Investment A Special Page of Investment Newspaper*]. <https://www.tinnhanhchungkhoan.vn/nghi-dinh-13-se-rat-vuong-mac-neu-ap-dung-cung-nerhac-va-khong-co-quan-diem-huong-dan-thong-nhat-post324861.html>
- 8 Hoang, L. (2023 June 29). “Xung đột” pháp luật trong triển khai Nghị định 13 về bảo vệ dữ liệu cá nhân. *Báo Công Thương* [Legal conflicts in implementing Decree 13 on personal data protection. *Industry*

of credit institutions are regulated by specialized legal regulations, and there is already a complete legal framework for implementing and complying with the protection of customer data as stipulated above. However, with the introduction of Decree No. 13, a conflict of laws has arisen.

In response to these challenges and the evolving needs for stronger data governance, Vietnam's National Assembly is working on two significant new pieces of legislation. The Draft Law on Personal Data Protection,⁹ aimed at creating a comprehensive legal framework for the protection of personal data, was passed in 2025 ("2025 Law on PDP"). This law provides clearer and more specific provisions on personal data handling, consent, and protection measures, which are seen as critical in an increasingly digital economy. Alongside this, the 2024 Law on Data also addresses broader issues related to data management, data sharing, and the use of data as a national resource.¹⁰ This law is anticipated to play a key role in regulating the collection, storage, and cross-border transfer of data, ensuring both individual privacy and national security in the digital age.

Although both Vietnam and Malaysia recognize that data governance is a crucial element of digital transformation, Malaysia has adopted a more comprehensive and unified legal foundation to regulate the protection of personal data. In Malaysia, before 2010, personal data was governed mainly by industry-specific legislation.¹¹ In May 2010, the PDPA was enacted. However, the enforcement date of the Act was delayed several times and finally entered into force on 15 November 2013, after three and a half years.¹² Along with the PDPA, five pieces of subsidiary legislation were also implemented. In addition, Section 21 of the data controller forums was established for specific industries, including communications, banking and finance.¹³ Pursuant to Article 23, each data controller forum was directed by the Commissioner to develop its own codes of practice for data controllers in its sector. In 2024, Malaysia's Minister of Digital announced the dates on which the provisions of the Malaysian 2024 PDPA Amendment would take

and Trade Media]. <https://conghuong.vn/xung-dot-phap-luat-trong-trien-khai-nghi-dinh-13-ve-bao-ve-du-lieu-ca-nhan-260154.html>

- 9 Le, A. (2024 November 2). Dự thảo Luật Dữ liệu: Xác định rõ phạm vi điều chỉnh. *Cổng thông tin điện tử Quốc hội Việt Nam* [Draft Data Law: Clearly defining the scope of regulation. *National Assembly's Electronic Portal of the Socialist Republic of Vietnam*]. <https://quochoi.vn/hoatdongdbqh/Pages/tin-hoat-dong-dai-bieu.aspx?ItemID=90617>
- 10 Minh, T. (2024 November 11). Quốc hội thông qua Luật Dữ liệu [National assembly passes the Data Law]. *Government Electronic Newspaper on Policy and Legal Development*. <https://dbnonghean.vn/quoc-hoi-thong-qua-luat-du-lieu-14580.htm>
- 11 Chia, J. Y. P., Yew, B. (2026 July 2). Malaysia – Privacy Overview. *Data Guidance Note*. <https://www.dataguidance.com/notes/malaysia-privacy-overview>
- 12 The Personal Data Protection Bill was passed by the Malaysian Parliament in May 2010 and received the Royal Assent on 2 June 2010. The PDPA came into force on 15 November 2013, with a three-month grace period ending on 14 February 2014.
- 13 World Bank (2025). Digitalizing SMEs to boost competitiveness. *World Bank*. <https://doi.org/10.1596/38108>

effect.¹⁴ It is the newest data protection law within ASEAN, which clearly shows the most noticeable reason why the authors focus on analyzing the PDPA of Malaysia in order to make comparisons and proposals for Vietnam.

This paper addresses one central research question: to what extent can the scope of application rules and the definitional framework of Malaysia's PDPA inform the reform and implication of Vietnam's personal data protection regime? To answer it, this paper adopts a micro-comparative legal approach,¹⁵ which does not attempt to compare the whole legal systems of Malaysia and Vietnam but focuses on relevant provisions of the PDPA and the 2025 Law on PDP in two main issues: (i) the scope of application and (ii) fundamental concepts comprising of the principles and definitions on which the entire law is built, such as what constitutes personal data, what constitutes data processing, and the roles of data controllers and data subjects. Without a thorough grasp of these elements, one risks misinterpreting the law, leading to potential non-compliance or misuse of data, which could result in legal penalties or harm to individuals' rights.

1. Scope of application under Malaysia's PDPA - Comparison with Vietnam's 2025 Law on Personal Data Protection

Firstly, the fundamental goal of the PDPA is to protect personal data by imposing requirements on data controllers and giving data subjects specific rights over their personal data.¹⁶ Given that there are over 33 million internet users in Malaysia,¹⁷ the PDPA clearly affects a significant number of people. Section 2.1 of the PDPA prescribes the scope of application to two types of subjects, namely (i) any person who processes, and (ii) any person who has control over or authorises the processing of any personal data in respect of commercial transactions. The 2010 Act itself contained no exclusion for deceased individuals. It is the 2024 PDPA Amendment that, by amending the definitions in Section 4, narrows the scope of "personal data" so as to exclude the personal data of deceased individuals. Specifically, according to Section 2.2, that person must be a data controller and satisfy the following conditions about establishment within the territory of Malaysia and processes personal information: (i) whether or not in the context of that establishment; (ii)

14 Ang, W., Lua, J., Silva, T. D. (2025 January 17). New horizons in data protection: Malaysia's personal data protection (amendment) act 2024. *Norton Rose Fulbright*. <https://www.dataprotectionreport.com/2025/01/new-horizons-in-data-protection-malysias-personal-data-protection-amendment-act-2024/>

15 Samuel, G. (2014). *An introduction to comparative law theory and method*. Hart Publishing, p. 45-64.

16 Long title of the 2010 Personal Data Protection Act (Laws of Malaysia, Act 709) "An Act to regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto".

17 Simon K. (2023 February 13). Digital 2023: Malaysia. *DataReportal*. <https://datareportal.com/reports/digital-2023-malaysia>

employing a third party; (iii) the data controller is not established in Malaysia but uses equipment located in Malaysia to process the personal information.

“Personal information” mentioned above includes either manual data (filing system),¹⁸ or electronic personal data, collected and used merely for the purpose(s) of commercial transactions by private sector users.¹⁹ Therefore, the PDPA applies solely to commercial transactions. Under Section 4 of the PDPA, the term “commercial transaction” refers to any commercial dealing of contractual or non-contractual nature,²⁰ with respect to supply or exchange of goods and services.²¹ Furthermore, Section 45.1 of the PDPA exempts personal, family and household affairs, as well as recreational purposes, from its application. This approach is similar to that used by Asia-Pacific Economic Cooperation²² and the European Union’s Directive 95/46/EC in excluding the processing of personal information by individuals “in the course of a purely personal or household activity”.²³ Furthermore, Section 45 provides partial exemptions for certain activities in which some principles or provisions of the PDPA will not apply, such as processing of personal data for journalistic, literary or artistic activities,²⁴ which is in line with freedom of expression and also freedom of the press.

Vietnam has 78.44 million internet users and 72.7 million social media users as of January 2024. Vietnam’s internet penetration rate stood at 79.1% of the total population at the beginning of 2024.²⁵ Therefore, the development of a comprehensive Law on PDP is of utmost importance to complete the legal framework for personal data protection and meet international and regional standards, while promoting the lawful use of personal data to serve socio-economic development.²⁶ Personal data protection and responsibilities of relevant agencies, organizations and individuals for protection of personal data are the areas where the Malaysian PDPA (Sections 2, 3) and Decree No. 13 (Article 1.1) of Vietnam most closely resemble each other in terms of their respective areas of application. Besides, both also adopt a rights-based

18 Filing system means paper based which is an old system of data recording.

19 Alibeigi, A., Munir, A. B. (2020). Malaysian Personal Data Protection Act, a mysterious application. *University of Bologna Law Review*, 05(02), p. 3. <https://ssrn.com/abstract=3792672>

20 Most of the times, contractual transactions appear in the clearer form of written contracts.

21 Section 4 of the PDPA defines commercial transactions as “any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act (2010)”.

22 Asia-Pacific Economic Cooperation Privacy Framework §10 (Nov. 2004) provides that: “It also excludes an individual who collects, holds, processes or uses personal information in connection with the individual’s personal, family or household affairs”.

23 Article 3(2) of the Council Directive 95/46, 1995 OJ (L 281).

24 Section 45(2)(f) of the 2010 Personal Data Protection (Laws of Malaysia, Act 709).

25 Trang, T. (2024). Improving the personal data protection law to accelerate the development of the national data strategy. *Economy and Forecast Review of the Ministry of Planning and Investment*.

26 Dự thảo Luật Bảo vệ dữ liệu cá nhân Việt Nam năm 2024 [the 2024 Proposal for the development of the Personal Data Protection Law of Vietnam].

approach by recognising enforceable rights for data subjects and regulating the entire lifecycle of personal data processing. There are, nevertheless, a few significant distinctions between them. Compared with Malaysia's PDPA, Decree No. 13 and the later 2024 Law on Data and the 2025 Law on PDP do not apply solely to commercial transactions, nor is there any exemption for applications such as Section 45.1 of the PDPA. According to distinctions between them. Compared with Malaysia is PDPA, Decree No. 13 and the later 2024 Law on Data and the 2025 Law on PDP do not apply solely to commercial transactions, nor is there any exemption for applications such as Section 45.1 of the PDPA. According to Article 3.1 of the 2005 Vietnamese Commercial Law, commercial activities are defined as activities for the purpose of generating profits. Vietnamese legislators address the scope of application by regulating industry-specific personal information under different pieces of legislation, a method considered to have both advantages and disadvantages compared to Malaysia's approach.

First of all, instead of separating legal aspects into commercial and non-commercial activities, as in Malaysia, each type of personal information in Vietnam is regulated by specific fields of law, such as the 2025 Law on Digital Transformation, the 2018 Law on Cybersecurity, and the 2016 Law on the Press, among others. Not to mention, the 2025 Law on PDP introduced new sector-specific provisions regarding the protection of personal data on advertising, Artificial Intelligence (AI), big data, cloud computing.²⁷ Despite these promising developments, one potential challenge is the lack of a clear distinction between commercial and non-commercial data activities in the existing Vietnamese legal framework. This is an area where Vietnam could benefit from learning from other jurisdictions, such as Malaysia. A clearer division between commercial and non-commercial uses of personal data would help prevent overregulation in non-commercial sectors and streamline compliance requirements for businesses handling consumer data.

Malaysia's commercial approach is clearly regulated under the PDPA, which provides strong legal assurances for businesses by limiting the processing of personal data to commercial transactions. This distinction makes it easier for organizations to identify when PDPA is in effect, thereby reducing ambiguity in compliance. In contrast, Vietnam adopts a more general model, in which the protection of personal data applies to all forms of processing, regardless of whether they are commercial. While this broad approach enhances overall protection by covering most personal data processing practices, it also increases the risk of regulatory overlap with specialized laws such as the 2025 Law on Digital Transformation and the 2018 Law on Cybersecurity. Therefore, organizations may find it difficult to determine the relationship between

27 Articles 25–30 of the 2025 Law on PDP.

these regulations, especially after the 2025 Law on PDP came into effect. From a comparative perspective, Malaysia's approach encourages legal clarity, simplifies regulations, and reduces compliance costs by applying the PDPA only to commercial activities. However, this limitation may mean that some forms of non-commercial data processing are not protected by the PDPA, leaving privacy risks to be addressed through other legal mechanisms or, in some cases, remaining unresolved. Conversely, Vietnam's comprehensive model provides broader protection for individuals by regulating personal data processing across both commercial and non-commercial contexts. Nevertheless, such broad coverage can lead to legal complexity and create overlaps between different regulations, potentially impacting consistency and enforcement. Therefore, it is nearly impossible to determine which approach is clearly superior. If the priority is to minimize uncertainty in compliance and promote business activity, then a trade-based legal system offers significant benefits; if the goal is to ensure comprehensive protection of personal data regardless of the processing context, then Vietnam's broad approach would be more appropriate for that objective.²⁸

Second, there are two exemptions relating to the scope of application. According to Section 3, PDPA shall not apply to the Federal government and State governments, and any personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia.²⁹ However, commercial companies owned by the government, such as Khazanah Nasional Berhad and Government-Linked Companies, are subject to the Act.³⁰ In Vietnam, Article 1 of Decree No. 13 applies to Vietnamese agencies, organisations, and individuals both at home and abroad, and to foreign agencies, organisations, and individuals operating in Vietnam or otherwise directly processing or involved in processing personal data in Vietnam.

Compared to the Draft Decree in 2021, which only states, "This Decree applies to agencies, organisations and individuals related to personal data", legislators have updated the scope of applicability to be more detailed in the Decree No. 13, extending to four categories of subjects (a) to (d) as quoted above. However, Article 1.2 of the 2025 Law on PDP narrows this scope to only three categories: Vietnamese agencies, organizations, and individuals; foreign subjects in Vietnam or directly participating in or involved in the processing of personal data of Vietnamese citizens and persons of Vietnamese origin without determined nationality residing in Vietnam who have been

28 Ali, A. (2020), *supra* note 19.

29 Articles 1-4 of the Federal Constitution of Malaysia incorporating all amendments up to P.U.(A) 164/2009.

30 Greenleaf, G. (2013). Malaysia: ASEAN's first data privacy act in force. *Privacy Laws & Business International Report*. UNSW Law Research Paper No. 2014-12. pp. 11-14.

issued with identification certificates. Notably, the 2025 Law on PDP omits Decree No. 13's separate category for Vietnamese agencies, organizations, and individuals operating abroad, and it also reformulates the fourth category: rather than covering any foreign entity that "directly processes or is involved in processing personal data in Vietnam," Article 1.2.c confines the 2025 Law on PDP application to foreign entities processing the personal data specifically of Vietnamese citizens and persons of Vietnamese origin who hold identification certificates, a narrower, subject-based test. This narrowing raises its own interpretive questions. On one hand, the 2025 Law on PDP more precise subject-based formulation may reduce the ambiguity that arose under the broader "directly process or are involved in processing" language of Decree No. 13. On the other hand, by removing the separate category for Vietnamese entities operating abroad, the Law remains unclear whether Vietnamese organizations processing personal data outside Vietnam's territory remain subject to the Law at all, or whether such processing now falls entirely outside its scope.

Comparatively, the 2025 Law on PDP lacks an article on exemptions, which might cause confusion and debate regarding whether or not the Government, Ministries, other governmental agencies of Vietnam, or foreign personal data processed outside of Vietnam are subject to the provisions of the Law or not. For example, Vietnam's government bodies and state-owned enterprises may require separate legal provisions for data processing, particularly related to national security, public administration, and law enforcement. If these bodies are not exempt, they may inadvertently be subjected to private-sector compliance standards, which may not align with their operational needs. Another instance is that while the Law includes provisions related to the processing of foreign data within Vietnam, because Article 1.2.c is subject-based rather than territorial, it may in fact extend extraterritorially to foreign entities processing Vietnamese citizens' data abroad, though whether Vietnamese authorities have practical means to enforce this extraterritorial reach remains a separate question. This could lead to enforcement challenges, particularly when data is transferred and processed across multiple jurisdictions, making it harder to regulate and ensure compliance. From the authors' standpoint, for any data protection regime to be effective, it is crucial that the scope of application and any exemptions be well defined.

Third, the lack of basic principles in a data protection framework might lead to ambiguity, inconsistency, legal uncertainty, and elevated risks for individuals and organizations. PDPA comprises seven fundamental principles that guide businesses in maintaining legal compliance while safeguarding the privacy of data subjects. Surprisingly, there are also six fundamental principles

as stated in Article 3 of the 2025 Law on PDP. These six principles are: (i) compliance with the Constitution, this Law and other relevant legal provisions; (ii) collection and processing only within the correct scope and for specific, clear and lawful purposes; (iii) ensuring the accuracy of personal data, with modification, updating and supplementation where necessary, and storage for a period appropriate to the processing purpose; (iv) effective and synchronous implementation of institutional, technical and human measures and solutions to protect personal data; (v) proactively preventing, detecting, stopping and strictly handling violations of the law on personal data protection; and (vi) linking personal data protection to national interests, socio-economic development, national defence, security and foreign affairs, while ensuring harmony with legitimate rights and interests of agencies, organisations and individuals. Overall, there is a strong alignment between the core tenets, which emphasize:

(i) *General principle* states that “personal data shall be processed fairly and lawfully”. According to Article 3.1 of the 2025 Law on PDP, the same idea is stipulated as “The personal data shall be processed as prescribed by law”. Therefore, the Vietnam Law mirrors this baseline of Malaysia PDPA, requiring that personal data processing comply with the Constitution and relevant laws. Both principles anchor lawful processing as the threshold requirement for any data activity.

(ii) *Notice and choice principle*: Data subjects (individuals to whom the personal data relates) should be informed of the purpose for which their personal data is collected and processed, and consent should be obtained unless an exemption applies. Under the 2025 Law on PDP, this is no longer framed as a processing principle in Article 3, but instead as a right of the data subject under Article 4.1(a), which entitles the data subject “to be informed of the personal data processing.” The substantive protection is equivalent, though its placement as an individual right rather than a controller-facing principle reflects a different legislative technique.

(iii) *Disclosure principle* indicates personal data shall not be disclosed without the consent of the data subject, unless such disclosure is permitted under the PDPA or necessary for the performance of a contract. Similarly, Article 3.2 of the 2025 Law on PDP provides that personal data shall be “collected and processed only within a specific, clear, and lawful scope and purpose.” Both principles restrict processing to the purposes for which data was obtained.

(iv) *Security principle* requires organizations and data processors to adopt practical, robust technical and physical measures to protect personal data against loss, misuse, modification, or unauthorized access. Article 3.4 of the 2025 Law on PDP imposes an equivalent obligation, requiring that “institutional,

technical, and human measures and solutions” be “synchronously and effectively implemented to protect personal data.” Both principles converge on the same underlying concern: safeguarding data through concrete organizational and technical measures.

(v) *Retention principle* requires that personal data not be kept longer than necessary to fulfil the purpose for which it was collected. Article 3.3 of the 2025 Law on PDP addresses this within a single, broader clause, requiring that personal data be “stored for a period in conformity with the personal data processing purpose.” Notably, the 2025 Law on PDP merges this retention requirement with the accuracy requirement below into a single clause, rather than treating them as separate principles, as Decree No. 13 did.

(vi) *Data integrity principle* requires organizations to take reasonable steps to ensure that the personal data they hold is accurate, complete, not misleading, and up to date. The same Article 3.3 of the 2025 Law on PDP also covers this dimension, requiring that data’s accuracy “be ensured” and that data be “modified, updated, and supplemented if necessary.” As noted above, this shares a single clause with the Retention Principle, reflecting the 2025 Law on PDP more consolidated drafting style.

(vii) *Access principle* gives individuals the legal right to access personal data held about them by an organization and to request correction of inaccurate or outdated information. Under the 2025 Law on PDP, this is likewise relocated out of Article 3 and guaranteed instead as a right of the data subject under Article 4.1(c), entitling data subjects “to view, modify, or request modification of their personal data.” As with Notice and choice above, the Law on PDP recasts what the PDPA frames as a controller-facing principle into an individually enforceable right.

2. Regulations on basic concepts under PDPA - Comparison with Vietnam’s 2025 Law on Personal Data Protection

2.1. The concept of “personal data”

In Malaysia, pursuant to Article 4 of PDPA, data is qualified as personal only if it meets four conditions: (i) relate to commercial transactions; (ii) be processed wholly or partly by automated equipment; (iii) be recorded with the intention of being processed or recorded as part of a relevant filing system; and (iv) relate directly or indirectly to a data subject who is identified or identifiable from the information or other information held by data controller, including sensitive personal data and expression of opinion.

Firstly, under the PDPA, “commercial transactions” are defined as transactions of a commercial nature and include any matter relating to the supply or exchange of goods or services, agency, investments, financing, banking, and insurance. It is currently unclear whether an employment relationship is considered to be a commercial transaction and whether employment-related

information would come under the scope of the PDPA.³¹ The definition of “personal data” appears to be sufficiently wide to cover the usual types of personal information collected in day-to-day transactions, such as name, address, telephone number, email address, banking details, and photographs.

Secondly, such information must be processed in full or in part. Processing covers a wide range of data operations, from collection and storage through use, disclosure, and even erasure³². The PDPA regulates that the processing of personal data must be done by automated means, which include the recording and storing of personal data in a computer or online database, as well as the use or disclosure of personal data on the data controller’s email, mailing list or website.

Thirdly, such information must be recorded as part of a relevant filing system or with the intention that it would form part of a relevant filing system. Article 4 of the PDPA defines “relevant filing system” as any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose as mentioned in condition (ii) above, the set of information is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Fourthly, the 2024 PDPA Amendment defines “sensitive personal data” under Article 4.13 “any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him biometric data of any offence or any other personal data as the Minister may determine by order published in the Gazette”.³³ In addition, there are currently no express provisions or guidance in the 2010 PDPA version on “biometric data” or “health data”. However, according to the revision of section 4 of 2024 PDPA Amendment, the lawmakers inserted, following the definition of “register”, a definition of “biometric data”, meaning any personal data resulting from technical processing relating to the physical, physiological, or behavioural characteristics of an individual. Furthermore, “sensitive personal data” does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the 2010 Credit Reporting Agencies Act.

In Vietnam, Article 2.1 of the 2025 Law on PDP defines “personal data” as digital data or information in other forms that identifies or assists

31 Chia, J. Y. P., Yew, B. (2024), *supra* note 11.

32 European Commission (2020). What constitutes data processing?. *Reform of EU data protection rules*. https://commission.europa.eu/law/law-topic/data-protection/reform/what-constitutes-data-processing_en

33 National Privacy Commission of Republic of the Philippines (2012). Implementing Rules and Regulations of Republic Act No. 10173, known as the 2012 Data Privacy Act.

in identifying a specific individual, encompassing both basic personal data and sensitive personal data, and clarifies that personal data, once de-identified, is no longer considered personal data. This marks a shift from the earlier definition under Decree No. 13, which had defined personal data as electronic information in the form of symbols, letters, numbers, images, sounds, or their equivalents associated with or used to identify an individual.

Notably, the 2025 Law on PDP also departs from Decree No. 13 in both terminology and legislative technique. The Decree used the term “general personal data” and enumerated its constituent categories directly in the text, including 14 categories ranging from full name and date of birth to tax, social security, and digital account information. Besides, Article 2.2 of the 2025 Law on PDP replaces this with the narrower term “basic personal data”, defined only in general terms as personal data reflecting common personal details and background information frequently used in transactions and social relations, with the detailed enumeration left to be specified by the Government of Vietnam in subsequent implementing regulations. The same delegation applies to “sensitive personal data” under Article 2.3, which is defined by reference to personal data associated with individuals’ privacy rights whose infringement directly affects legitimate rights and interests, again without an itemized list in the Law itself. Article 39 of the 2025 Law on PDP further provides that personal data processing activities and impact assessment dossiers already conducted or filed under Decree No. 13 before the effective date of the 2025 Law on PDP remain valid, so the Decree’s detailed categories are likely to inform, if not be directly carried over into, the Government’s forthcoming implementing decree.

Moreover, Article 3.13 of Decree No. 52/2013/NĐ-CP on e-commerce stipulates that “personal information is information that contributes to the identification of a specific individual, including name, age, home address, phone numbers, medical information, account numbers, information about personal payment transactions, and other information that the individual wishes to keep confidential.” However, the Decree also notes that personal information “does not include work contact information and information that individuals have self-published in the media.” On the other hand, the 2024 Law on Data also provided a new definition of data as “the digital representation of behaviors, objects, events, and information, including forms such as sound, images, numbers, text, symbols, or other similar formats.” Instead of providing the concept of “personal data,” the 2024 Law on Data defines “non-personal data” as data that is not associated with a specific individual or does not aid in identifying a specific individual.

Unlike Vietnam's law, the concept of "personal data" in the PDPA is regulated with four specific conditions that can be useful for competent state agencies in practical application. The 2025 Law on PDP would be strengthened by introducing specific exemptions and clearer guidelines on the scope of personal data, similar to the PDPA's four conditions. This would help simplify compliance for both businesses and regulators, and ensure that personal data protection is not unnecessarily burdensome for data types that do not require such extensive safeguards.

However, the definition of "sensitive personal data" provided in Decree No. 13 and the 2025 Law on PDP is more detailed than the same concept in the PDPA. Article 2.4 of Decree No. 13 lists ten categories, ranging from political and religious opinions, health and genetic data, and racial or ethnic origin, to biometric characteristics, sexual orientation, criminal records, financial customer information, and location data, plus a residual category covering any other personal data that the law identifies as requiring special protection.

By contrast, Article 2.3 of the 2025 Law on PDP no longer reproduces this itemized list within the text of the Law itself. Instead, it defines "sensitive personal data" only in general terms as personal data associated with individuals' privacy rights that, if infringed, directly affects the legitimate rights and interests of agencies, organizations, and individuals and expressly delegates the detailed enumeration of specific categories to implementing regulations to be issued by the Government of Vietnam. This is a shift in legislative technique: whereas Decree No.13 fixed the categories of sensitive personal data directly in a legal instrument, the 2025 Law on PDP leaves this content to be filled in by a forthcoming decree, which had not yet been promulgated at the time of writing.

Similar to Article 2.3 of Decree No. 13, and Article 9 of General Data Protection Regulation (GDPR)³⁴ establishes several categories of "sensitive data", including racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sexual orientation and the handling of sensitive data subject to the explicit consent of the data subject, in the absence of the consent of the data subject, the data sensitivity cannot be infringed unless the competent authority intervenes.

In summary, the existing Vietnamese legal requirements regarding the concept of "personal data" are not uniform across various specialised pieces of legislation, in contrast to Malaysia's PDPA. The PDPA defines

³⁴ The General Data Protection Regulation is a European Union regulation on information privacy in the European Union and the European Economic Area.

“personal data” under four precise guidelines that, in practice, may be helpful to governmental agencies dealing with such matters. Whether the 2025 Law on PDP preserves or improves upon that level of detail cannot yet be fully assessed, however, because the Law delegates the specific categories of sensitive personal data to an implementing decree. Assessing Decree No.13 against international benchmarks such as the GDPR suggests that Vietnam’s approach under the 2025 Law on PDP’s to defining sensitive personal data was, at that stage, broadly comparable to Malaysia’s; whether this remains true once the 2025 Law’s implementing decree is finalized is a question that will need to be revisited once that decree is available.

2.2. The concept of “data controller” and “data processor”

According to Article 4 of the PDPA, a “data controller” is a person who, either alone, jointly, or in common with other persons, processes any personal data, or has control over, or authorises the processing of, any personal data. Essentially, the “data controller” acts as the decision-maker, defining why and how personal data should be handled. On the other hand, a “data processor” under the PDPA means any person, other than an employee of a data controller, who processes personal data solely on behalf of the data controller and not for any of their own purposes. To sum up, a “data controller” is an entity that determines the reasons and methods for processing personal data, while a “data processor” is an entity that actually performs data processing on the user’s behalf. A “data controller” does not include a “data processor”.

This distinction carries practical consequences in Malaysia, where the PDPA imposes registration obligations specifically on data controllers operating in the classes of business prescribed by the PDPA, and failure to comply exposes the controller to criminal liability. On 3 May 2017, Khas Cergas Sdn Bhd, the company that owns Victoria International College, was charged in the Sessions Court for processing the personal data of the former employee without a valid certificate of registration issued by the PDPA. Specifically, this case breached Section 16 (1) of the PDPA, which requires the “data users” or “data controller” according to 2024 PDPA Amendment to register the applicant and issue a certificate of registration by the PDPA. After the Sessions Court judge, the charge under section 16(4) of the PDPA carries a maximum fine of RM 500,000 or imprisonment for up to three years, or both. This case serves as an important precedent in defining a data user or data controller under the PDPA. It underscores the principle that every company that decides how to handle personal data is legally required to comply with PDPA requirements, such as registration, security measures, and legitimate data processing. Non-compliance can result in significant

penalties, highlighting the need for rigorous adherence to the legislation in Malaysia's data protection regime.

Similarly, under Article 3.2 of the 2024 Law on Data, data processing is defined as “one or more activities affecting data,” encompassing a broad range of activities from collection through deletion. Vietnamese legislation, under Articles 2.7 and 2.8 of the 2025 Law on PDP, also provides comparable definitions. A “personal data controller” refers to an organization or individual that determines the purposes and methods for processing personal data. Meanwhile, a “personal data processor” is defined as an organization or individual that processes personal data on behalf of the personal data controller based on a contractual arrangement or agreement. The legislative frameworks in both Malaysia and Vietnam thus align in differentiating between two key roles: the entity that determines the purposes and methods of processing (referred to as the “data controller”) and the entity that processes data as instructed by the controller (the “data processor” or equivalent).

Moreover, there is another definition only appearing in Article 2.9 of the 2025 Law on PDP, which is “Personal data controller-cum-processor” referring to an agency, organization, or individual that decides on the purposes and means of personal data processing and directly processes personal data. This combined role applies to scenarios in which a single entity assumes both decision-making and operational responsibilities for the processing of personal data. Understanding these definitions and the relationships between data controllers and data processors is crucial for organizations to ensure compliance with data protection regulations and to establish clear lines of accountability for safeguarding personal information.

2.3. Comparative lessons from Malaysia: Towards a more effective personal data protection regime in Vietnam

The comparative analysis demonstrates that Malaysia's PDPA and Vietnam's personal data protection regime reflect distinct legislative priorities shaped by different regulatory philosophies. Malaysia prioritises legal certainty and regulatory efficiency by limiting the PDPA's application to commercial transactions and clearly distinguishing the roles of data controllers and processors within a well-defined statutory framework. Vietnam, by contrast, adopts a broader rights-based approach that extends protection across both commercial and non-commercial processing while increasingly relying on delegated legislation to accommodate technological change.

These differences carry important implications for the continued implementation of Vietnam's 2025 Law on PDP. The need to establish a more secure and effective framework for the storage and processing of personal data has also been recognised by the Department of Cybersecurity and High-tech Crime Prevention, which has noted that existing systems remain

vulnerable to exploitation by cybercriminals.³⁵ Basically, the provisions of the law protecting personal data were developed from the right to privacy as stipulated in Vietnam's 2013 Constitution.³⁶ The need for greater coherence in Vietnam's legal framework for personal data protection has also been recognised by the Institute for Legal Strategy and Science.³⁷ Although Vietnam has established a general legal framework governing personal data protection,³⁸ a preliminary review reveals that several legal instruments still use inconsistent terminology. For example, the concept of "personal data" overlaps with related terms such as "personal information", "private information", "digital information", "sensitive information in the network environment", as well as "personal secrets", "information concerning private life", and "family secrets", each of which may be subject to different legal interpretations. This terminological inconsistency creates uncertainty regarding the scope and application of personal data protection laws.

Notably, despite the rapid expansion of e-commerce in recent years, Vietnam's legal framework for personal data protection has not kept pace. Although the enactment of the 2024 Law on Data and the 2025 Law on PDP represents a significant step towards strengthening data governance, challenges remain in effectively enforcing personal data protection obligations in electronic transactions involving both organisations and individuals. These challenges stem, in part, from ambiguities surrounding the scope and application of personal data protection requirements in the digital environment.

As regional initiatives such as the ASEAN Framework on Personal Data Protection continue to promote regulatory convergence, Southeast Asian jurisdictions are placing greater emphasis on harmonising data protection standards. Malaysia's regulatory experience offers useful comparative insights for Vietnam. In particular, Vietnam could selectively adopt Malaysia's clearly defined commercial transaction threshold and its

35 Trương Sơn Lâm's speech at the National Conference - Exhibition on security in 2021 organized by the International Data Group in Vietnam (IDG Vietnam) on 25 March 2022. See also Thanh Hà (2021 March 25), Hơn 5.000 trang, cổng thông tin điện tử trong nước bị tấn công, *Hanoi Newspaper*. <http://www.hanoimoi.com.vn/ban-in/Oto-xemay/994531/hon-5000-trang-cong-thong-tin-dien-tu-trong-nuoc-bi-tan-cong>

36 Article 21 of the Constitution of Vietnam 2013: "Everyone is entitled to the inviolability of personal privacy, personal secrecy and familial secrecy and has the right to protect his or her honour and prestige".

37 Ministry of Justice. (2025 February 6). *Đẩy mạnh sử dụng dữ liệu cá nhân đúng pháp luật phục vụ phát triển kinh tế, xã hội. Cổng thông tin điện tử Bộ Tư pháp*. [Promoting the lawful use of personal data for socio-economic development. *Electronic Portal of the Ministry of Justice*]. <https://moj.gov.vn/portal/tin-tuc/chi-tiet/ay-manh-su-dung-du-lieu-ca-nhan-ung-phap-luat-phuc-vu-phat-trien-kinh-te-xa-hoi-tctoca49c6.html>; Institute of Legal Strategy and Science. (2025 September 29). *Viện Chiến lược và Khoa học pháp lý. Cổng thông tin điện tử Bộ Tư pháp* [Institute of legal strategy and science. *Electronic Portal of the Ministry of Justice*]. <https://moj.gov.vn/portal/tin-tuc/chi-tiet/vien-chien-luoc-va-khoa-hoc-phap-ly-t3c11q.html>

38 Chu, T.H. (2020). Legal gaps on personal data protection. Legal report on personal data protection in Vietnam. Conference within the framework of the 2020 program "Strengthening the law and justice in Vietnam" (EU JULE), *The Ministry of Public Security coordinated with the United Nations Development Program*, p. 7.

sector-specific mechanisms for engaging data controllers, both of which enhance legal certainty and reduce compliance ambiguity for businesses. At the same time, Vietnam should avoid replicating Malaysia's broad exclusion of non-commercial data processing, as such an approach would unduly limit the scope of protection afforded under Vietnam's rights-based framework. Three drafting models in particular merit consideration. First, the forthcoming implementing decree could adopt a statutory definition of "commercial transaction" modelled on Section 4 of the PDPA as "any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance". It is not in order to limit the scope of the 2025 Law on PDP, but to demarcate a category of commercial processing to which the heavier registration, impact-assessment and record-keeping duties attach, leaving proportionately lighter obligations for non-commercial processing. Second, the 2025 Law on PDP contains no exemption provision, and Section 45 of the PDPA offers a workable template: a full exemption for personal data processed by an individual only for that individual's personal, family or household affairs, including recreational purposes (Section 45(1)), together with partial exemptions for processing for journalistic, literary or artistic purposes (Section 45(2)(f)). Transposing an equivalent clause would relieve households and the press of compliance burdens that the current drafting leaves ambiguous, without narrowing the Law's rights-based core. Third, as regards cross-border data handling, Article 20 of the 2025 Law on PDP relies on an ex post mechanism, requiring the transferring party to compile and submit an impact-assessment dossier within sixty days of commencing the transfer, whereas Section 129 of the PDPA, as restructured by the 2024 Amendment, abandons the former ministerial whitelist in favour of a risk-based test permitting transfer where the recipient jurisdiction has laws substantially similar to the PDPA or otherwise ensures an adequate level of protection. Supplementing Article 20 with such an adequacy-based test, accompanied by a published list of assessed jurisdictions, would give Vietnamese exporters an ex ante basis on which to plan transfers, reduce reliance on case-by-case administrative review, and improve interoperability with Malaysia and other ASEAN partners. Vietnam should adopt a selective comparative approach by incorporating foreign regulatory techniques that enhance clarity and enforceability while maintaining a comprehensive, rights-oriented model consistent with its constitutional, institutional, and socio-economic context. Such an approach would strengthen domestic governance and contribute to greater interoperability with evolving regional data protection standards. ●

References

- [1] Alibeigi, A., Munir, A. B. (2020). Malaysian Personal Data Protection Act, a mysterious application. *University of Bologna Law Review*, 05(02), <https://ssrn.com/abstract=3792672>
- [2] Chu, T.H. (2020). Legal gaps on personal data protection. Legal report on personal data protection in Vietnam, Conference within the framework of the 2020 program “Strengthening the law and justice in Vietnam” (EU JULE), *The Ministry of Public Security coordinated with the United Nations Development Program*
- [3] European Commission (2020). What constitutes data processing?. *Reform of EU data protection rules*
- [4] Greenleaf, G. (2013). Malaysia: ASEAN’s first data privacy act in force. *Privacy Laws & Business International Report*. UNSW Law Research Paper No. 2014-12
- [5] Samuel, G. (2014). *An introduction to comparative law theory and method*. Hart Publishing
- [6] Hai, T. (2020). Completing the legal framework to protect personal data. Electronic newspaper of People’s Deputies.
- [7] Ebert, I., Wildhaber, I., & Adams-Prassl, J. (2021). Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection. *Big Data & Society*, 8(01). <https://doi.org/10.1177/20539517211013051>
- [8] Lee, R., Janna, A. (2023 June 21). *As AI spreads, experts predict the best and worst changes in digital life by 2035*. Pew Research Center
- [9] Ang, W., Lua, J., Silva, T. D. (2025). New horizons in data protection: Malaysia’s personal data protection (amendment) act 2024. *Norton Rose Fulbright*.
- [10] World Bank (2025). Digitalizing SMEs to boost competitiveness. *World Bank*. <https://doi.org/10.1596/38108>

Author Contribution

All authors contributed to the study conception and design. All authors read and approved the final manuscript.

Declarations

Conflict of Interest: The authors declare no competing interests.

Disclaimer: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article or claim that may be made by its manufacturer is not guaranteed or endorsed by the publisher.



Copyright: © 2026 by the authors. Licensee VJLS, Ho Chi Minh City University of Law, Vietnam. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).