

“Strengthening Vietnam’s legal framework for personal data protection and social responsibility: Lessons from Japan’s experience”

AUTHORS

Thi Phuong Cham Nguyen 

ARTICLE INFO

Thi Phuong Cham Nguyen (2026). Strengthening Vietnam’s legal framework for personal data protection and social responsibility: Lessons from Japan’s experience. *Knowledge and Performance Management*, 10(3), 67-79.
doi:[10.21511/kpm.10\(3\).2026.05](https://doi.org/10.21511/kpm.10(3).2026.05)

DOI

[http://dx.doi.org/10.21511/kpm.10\(3\).2026.05](http://dx.doi.org/10.21511/kpm.10(3).2026.05)

RELEASED ON

Friday, 31 July 2026

RECEIVED ON

Sunday, 08 February 2026

ACCEPTED ON

Wednesday, 08 July 2026

LICENSE



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

JOURNAL

"Knowledge and Performance Management"

ISSN PRINT

2543-5507

ISSN ONLINE

2616-3829

PUBLISHER

LLC “Consulting Publishing Company “Business Perspectives”

FOUNDER

Sp. z o.o. Kozmenko Science Publishing



NUMBER OF REFERENCES

48



NUMBER OF FIGURES

0



NUMBER OF TABLES

0

© The author(s) 2026. This publication is an open access article.



BUSINESS PERSPECTIVES



LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine
www.businessperspectives.org

Type of the article: Research Article

Received on: 8th of February, 2026Accepted on: 8th of July, 2026Published on: 31st of July, 2026

© Thi Phuong Cham Nguyen, 2026

Thi Phuong Cham Nguyen, Ph.D.,
Lecturer, Faculty of Private Law,
University of Law, Vietnam National
University, Vietnam.

Thi Phuong Cham Nguyen (Vietnam)

STRENGTHENING VIETNAM'S LEGAL FRAMEWORK FOR PERSONAL DATA PROTECTION AND SOCIAL RESPONSIBILITY: LESSONS FROM JAPAN'S EXPERIENCE

Abstract

The rapid development of digital transformation, artificial intelligence, and data-driven economic models has heightened concerns about personal data protection and social responsibility in Vietnam. In this context, this study aims to assess Vietnam's legal framework for personal data protection and propose policy reforms to enhance social responsibility. Social responsibility is understood as responsible data governance achieved through the implementation of principles of transparency and accountability, thereby enhancing trust, and through risk-based governance that both respects traditional rights and ensures that data flows are not hindered in the digital context. The study employs theoretical legal analysis and comparative law methods to examine comprehensive legal frameworks for personal data protection, particularly Vietnam's Personal Data Protection Law 2025 and Japan's Personal Information Protection Law. The results show that Vietnam's personal data protection regime remains hampered by fragmented regulations and an overly consent-based approach, and that the fundamental principles of the legal framework for protecting personal data are merely symbolic and formal on paper due to weak enforcement and monitoring mechanisms. In contrast, Japan's experience demonstrates the effectiveness of a centralized supervisory body, a guidance-based management model, risk-based governance, and regular legal review cycles in promoting socially responsible data use. Based on these findings, the study proposes policy recommendations for Vietnam, focusing on improving the structure of a synchronized and unified legal framework for personal data protection; establishing a data governance mechanism based on risk management principles; and creating an independent agency to coordinate the development, monitoring, and implementation of the law nationwide.

Keywords

digital age, personal data, legal framework, policy reform, sustainable development, Vietnam, Japan

JEL Classification

K15, K24, K39, O38

INTRODUCTION

In recent years, Vietnam has made significant advances in science and technology, digital transformation, and the development and application of artificial intelligence (Le & Duong, 2024). In particular, personal data – including basic data, sensitive data, anonymized and de-identified data – has emerged as a key resource that may serve not only individual interests but also broader public and social objectives when used through advanced digital technologies (Srivastava & Siddiqui, 2024; Nguyen & Ha, 2025). At the same time, the rapid expansion of data-driven technologies has heightened concerns about privacy, security, and the misuse of personal data (Bui et al., 2025; Nguyen, 2023). Technologies such as facial recognition and behavioral analytics enable increasingly precise inferences about individuals' preferences,



This is an Open Access article,
distributed under the terms of the
[Creative Commons Attribution 4.0
International license](https://creativecommons.org/licenses/by/4.0/), which permits
unrestricted re-use, distribution, and
reproduction in any medium, provided
the original work is properly cited.

Conflict of interest statement:

Author(s) reported no conflict of interest

health conditions, economic status, and social behavior (Le et al., 2024; Radanliev, 2025). These developments significantly increase the risk that misuse of personal data could lead to serious violations of individual rights and interests, fueling growing public anxiety over data security and privacy protection (Tran, 2024b). Moreover, the globalization of economic and social activities has intensified cross-border data flows, raising additional challenges related to data governance, geopolitical risks, and divergent regulatory approaches (Yeung & Bygrave, 2021; Pham et al., 2023).

The lack of transparent, effective, and responsible data-processing control mechanisms poses broader societal risks (Yeung & Bygrave, 2021). Inadequate governance of personal data can lead to discrimination, injustice, and erosion of public trust, discouraging participation in digital and social relationships and undermining sustainable development (Tran, 2024b). These challenges highlight a broader scientific problem regarding the capacity of legal systems to reconcile the growing social and economic value of personal data with the protection of fundamental rights and the maintenance of public trust in a digital society (Muralinathan, 2025).

In response to these challenges, Vietnam adopted the Law on Personal Data Protection on June 26, 2025, which takes effect on January 1, 2026 (National Assembly of Vietnam, 2025). While this law marks an important milestone in establishing a comprehensive legal framework, comparative experience shows that personal data protection laws must continually adapt to rapid technological change and evolving social risks (Rezac, 2022; To, 2024; Nguyen, 2026b). As illustrated by Japan's experience, effective personal data protection requires not only substantive legal rules but also robust enforcement mechanisms, coherent governance structures, and institutional capacities to promote social responsibility in data processing. Recent studies on Japan indicate that its personal data protection system is comprehensive and unified (covering both public and private sectors), while maintaining a balance between protection and economic development. It is aligned with international standards (OECD, GDPR) and oriented toward secure data globalization (Ishiwaka, 2025). This makes it highly compatible with Vietnam's current policy direction and, therefore, one of the models that should be studied seriously and comprehensively.

1. LITERATURE REVIEW

Within Vietnamese legal scholarship, research on personal data protection has grown rapidly alongside national digital transformation and the expansion of the digital economy (Le et al., 2024; Bui et al., 2025). Existing studies primarily examine the constitutional foundations of privacy rights, sector-specific legal provisions, and the regulatory implications of emerging technologies, including artificial intelligence and big data (Nguyen, 2025; Le et al., 2024; Bui et al., 2025; Nguyen, 2026a). The literature consistently highlights significant shortcomings in Vietnam's current legal framework. Identified issues include fragmented and overlapping regulations, ambiguity in the definition and classification of personal and sensitive data, and limited guidance on the governance of de-identified or non-identifiable data (Le et al., 2024; Trinh, 2025; Hoang, 2026). Several scholars further argue that Vietnam's regulatory approach remains heavily formalistic, offering insufficient mechanisms for supervision and ac-

countability in practice (Nguyen & Ha, 2025; Tran, 2024a; To, 2024). Another dominant theme in the literature emphasizes the relevance of data ethics, human-centered artificial intelligence, privacy governance, and privacy-enhancing technologies as normative frameworks that can reconcile innovation with the protection of fundamental rights (Bui, 2024; Tran, 2024b; Nguyen, 2025; Nguyen, 2026a). In addition to studies that approach the issue from the perspective of Vietnamese law, many domestic studies compare international legal models to propose ways to improve Vietnam's legal system. A notable example is research analyzing personal data protection models in the EU, the UK, South Korea, and Poland, with particular emphasis on the principle of independence of data protection supervisory authorities (To, 2024).

Beyond Vietnamese research, scholars worldwide have focused on broader issues related to personal data protection. In international scholarship, personal data protection is widely recognized as a com-

plex regulatory challenge stemming from large-scale, automated data processing enabled by artificial intelligence, big data analytics, biometric technologies, and cloud computing (Zisu, 2025). These developments heighten the risks of profiling, discrimination, and the erosion of individual autonomy, thereby extending the implications of data protection beyond the individual level to broader social interests (Pham et al., 2023; Yeung & Bygrave, 2021). Within this line of reasoning, personal data protection is framed as a shared social responsibility involving the state, private entities, and data users (Srivastava & Siddiqui, 2024; Cahyani et al., 2025). Another dominant theme in the literature concerns the limitations of consent-based regulatory models in addressing systemic risks associated with contemporary data processing practices (Vamsi, 2025). Some studies indicate that the absence of transparent and accountable data governance mechanisms is often associated with declining public trust and reduced participation in digital ecosystems, ultimately undermining social cohesion and sustainable development (Balboni & Francis, 2025).

Japanese literature frequently refers to Japan's personal information protection regime as an adaptive and institutionally robust model. Analyses of the Act on the Protection of Personal Information emphasize Japan's evolutionary legislative approach, characterized by periodic amendments and continuous institutional reform in response to technological change and globalization (Matsuno, 2006; Kitakara, 2007; Nasu, 2025). Particular attention is devoted to the role of the Personal Information Protection Commission as an independent supervisory authority empowered to issue guidelines, conduct inspections, and enforce compliance (PPC, 2022, 2025a). The extensive use of legally influential guidelines is widely regarded as an effective tool for translating abstract legal principles into sectorspecific regulatory practices (Katagiri et al., 2005).

Japanese scholarship further highlights the importance of selfgovernance and multilayered compliance mechanisms, including certified personal information protection organizations that complement state enforcement and encourage voluntary compliance among businesses (Tada, 2006; Katagiri et al., 2005). The introduction of differentiated categories such as personally related information, pseudonymized data, and anonymized pro-

cessed information is often cited as an innovative regulatory response that facilitates data use while maintaining socially acceptable levels of risk (Nasu, 2025; PPC, 2025a). These studies present Japan's approach as one that integrates personal data protection with corporate social responsibility and sustainable data governance (Katagiri et al., 2005).

Although the number of research papers on personal data protection in Vietnam and Japan is increasing, some gaps remain. First, studies in Vietnam rarely employ a systematic comparative legal approach, not only comparing legal texts but also examining enforcement structures and governance mechanisms. Second, there is currently no comparative study of Japan's legal framework for personal data protection, even though Vietnam's civil law shares many similarities with Japanese law, Japan's experience is often cited as a reference point, and Vietnam has chosen a development direction similar to Japan's.

Research comparing Japan's legal framework with others will address current legal gaps, and learning from Japan's experience is invaluable for resolving policy and development shortcomings: recognizing the social responsibility of stakeholders, such as guiding the development of a personal data protection ecosystem, and always balancing it with the development of science and technology and innovation.

In light of these research gaps, this study aims to evaluate Vietnam's legal framework for personal data protection and examine how it can better promote social responsibility. Drawing on lessons from Japan's legislative evolution, enforcement institutions, and governance mechanisms, the study seeks to develop policy recommendations for improving the effectiveness, coherence, and sustainability of Vietnam's personal data protection regime.

2. METHODOLOGY

This study employs doctrinal and comparative legal analysis. Doctrinal legal analysis is used to examine and evaluate Vietnam's personal data protection framework, with a particular focus on the Law on Personal Data Protection 2025. The analysis assesses Vietnamese law through fundamental

principles of personal data protection in relation to social responsibility, namely legality, transparency, accountability, purpose limitation, data minimization, accuracy, integrity, and confidentiality.

The same method is applied to Japan's legal framework, focusing on the Act on the Protection of Personal Information, Cabinet Orders, regulations and guidelines issued by the Personal Information Protection Commission, the Basic Policy on the Protection of Personal Information, and relevant policy documents. These materials were selected because they directly regulate or guide the implementation of Japan's personal information protection regime. The Japanese analysis focuses on the law's guiding philosophy, the structure of the legal framework, risk-based governance, supervisory mechanisms, and implementation guidelines.

Comparative legal analysis is mainly applied in the discussion section. It compares Japan's experience with Vietnam's current framework to identify regulatory gaps and institutional weaknesses in Vietnam. On this basis, the study proposes two groups of recommendations: solutions that can be directly transferred from Japan's experience and those that require adaptation to Vietnam's legal, institutional, and socio-economic context.

Vietnamese and Japanese legal materials were examined primarily in their original languages. English translations were used only as supporting references where available. Japanese legal texts were translated into English for analytical purposes, and the accuracy of the translations was checked against the original Japanese texts, official PPC terminology, and relevant Japanese legal commentaries.

3. RESULTS

3.1. Legal framework for personal data protection and challenges to realizing social responsibility in Vietnam

Decree No. 13/2023/ND-CP, issued on April 17, 2023, and effective as of July 1, 2023, establishes a comprehensive legal framework for personal data protection in Vietnam, covering the collection

and processing of personal data. Notably, on June 26, 2025, the National Assembly passed the Law on Personal Data Protection (hereinafter, PDPL), which strengthens and improves the legal framework governing personal data protection.

Nevertheless, provisions of the PDPL are considered ineffective and inconsistent with the Civil Code and other specialized laws (Bui et al., 2025; Nguyen & Ha, 2025; Nguyen, 2026b). Moreover, from basic principal perspectives, challenges in PDPL and social responsibility include the following.

First, the principle of legality rests on the theories of individual autonomy and the social contract (Schubert & Barrett, 2024). Individuals have the right to self-determination regarding their "digital identity." Article 11 stipulates that "personal data must be collected with the data subject's consent prior to collection, except where otherwise provided by law." Thus, the data subject's consent is the legal basis for the collection and processing of personal data. In addition, Article 19 of the law provides exceptions that allow the collection and processing of personal data without consent. Articles 9 and 10 define and detail the requirements for consent: consent must be voluntary and informed (including the type of data, purpose, processing entity, and the subject's rights and obligations). Consent must be explicit, purpose-specific, withdrawable, and silence does not constitute consent. However, Vietnam affirms consent as the primary basis of legality (Article 11) but has not provided a distinct framework for other legal bases. Some exceptions are indirectly mentioned (Articles 19, 26, 28), but they remain limited (Nguyen, 2026a, 2026b). As such, the legal grounds beyond consent have not been diversified, which is particularly important in the context of digital transformation and artificial intelligence, where a balance is needed between protecting personal data and promoting the use of data resources (Miyake & Partners, 2026). Compared with international standards, Vietnam still lacks a general "legitimate interests" mechanism, creating challenges for businesses implementing new technologies that are not yet clearly regulated, which allows processing where the interests do not override fundamental rights and freedoms of individuals (Verdoodt et al., 2024).

In addition, the PDPL establishes certain basic rights for individuals, such as the right to withdraw consent (Article 10) and the right to access, correct, and delete their data (Articles 13 and 14). However, there is no explicit right to access all personal data being processed, nor a clear right to lodge complaints with an independent supervisory authority (only a general right to lodge complaints under procedural law).

Regarding enforcement mechanisms and sanctions, the PDPL designates the Ministry of Public Security as the competent authority for personal data protection (Article 24), along with provisions on breach notification (Article 23) and strict penalties (Trinh, 2025; Hoang, 2026). Article 8 states that violators may face administrative penalties or criminal liability and must compensate for damages caused. Fines can reach up to 5% of revenue for violations involving cross-border data transfers and up to VND 3 billion for other violations. However, the enforcement authority has not been institutionally separated from broader cybersecurity objectives (McCoy et al., 2022). Furthermore, there is a lack of specific provisions on compensation liability tailored to data protection harms; disputes are still handled under general non-contractual liability rules. Complaint mechanisms also lack clarity regarding responsible authorities and procedural steps (Hoang, 2026; Nguyen, 2026b).

Second, regarding the principle of transparency, although the PDPL does not explicitly use the term “transparency,” it requires disclosure of information about processing. Under Article 9, the data subject must be informed of the purpose, scope, and data processors to give valid consent. Article 15 requires organizations to provide individuals with their data upon request (except in cases of national security or public interest), thereby partially reflecting the right of access. However, the law lacks clear obligations to publish privacy policies, does not establish a common compliance culture for businesses, and does not mandate prior notification before processing. Overall, the transparency principle is not fully articulated (Nguyen, 2026b).

To enhance accountability, the law requires the preparation of data protection impact assessments and submission to the competent authority (Article 21). However, Vietnam does not mandate the appointment of Data Protection Officers (DPOs) or

the establishment of internal data protection units. The presence of a DPO or a data governance structure indicates effective data management, helping to monitor compliance and safeguard data subjects’ rights internally (Schubert & Barrett, 2024). The absence of such requirements leaves Vietnamese businesses without a professional “privacy gatekeeper”. Third-party oversight and periodic reporting mechanisms are also not clearly defined. Advanced international standards require companies – especially large technology platforms – to publish annual independent audit reports on systemic risks and security measures (Wylde et al., 2023; Zang, 2026). Vietnam does not yet mandate such transparency reports or independent oversight for high-risk processing activities.

Third, regarding the principle of purpose limitation, the law requires that data processing be limited to agreed or legally permitted purposes (Article 11) and sector-specific regulations (Article 25a). Article 17 permits data transfers within the original purpose (e.g., between departments within the same organization). Thus, purpose limitation is partially codified through sectoral provisions. However, challenges remain in managing and adjusting purposes after data collection (Nguyen, 2026b).

Fourth, regarding data minimization, certain sectoral provisions (Articles 25 and 27) require the collection of “only necessary information.” However, the law lacks a general obligation requiring controllers to assess data minimization, and existing rules are fragmented without detailed implementation guidance (Nguyen, 2026b).

Fifth, regarding data accuracy, Article 13 requires data controllers to correct personal data upon request and to ensure its accuracy. If correction is not possible for legitimate reasons, the data subject must be notified. However, technical measures to ensure accuracy are not specified (Nguyen, 2026b).

Lastly, regarding security and integrity, the PDPL mandates technical and organizational safeguards. Article 18(1) requires appropriate storage and protective measures for personal data. Provisions on encryption (Article 12) and breach notification (Article 23) also relate to security. However, the law does not clearly prescribe requirements for encryption, anonymization, or pseudonymization.

Nor does it provide sector-specific technical standards or workforce training guidelines, making enforcement and assessment difficult (Nguyen & Ha, 2025; Nguyen, 2026b).

Particularly for cross-border data transfers, although the PDPL does not provide a dedicated article, it requires “cross-border data transfer impact assessments” (Article 22). Such transfers generally require consent or must serve specific purposes (Trinh, 2026). While the framework mandates risk assessment prior to transfer, it lacks detailed requirements or mechanisms for mutual recognition with other jurisdictions (Miyake & Partners, 2025).

In summary, the PDPL demonstrates alignment with most fundamental principles of data protection but remains incomplete and insufficiently detailed in several aspects, including transparency, data subject rights, alternative legal bases beyond consent, independent enforcement structures, and multi-layered complaint mechanisms.

3.2. Japan’s legislation on the enforcement of personal data protection laws promotes social responsibility

The development of the Act on the Protection of Personal Information (hereinafter, APPI) in Japan is situated within both domestic and international contexts. First, domestic factors include the rapid growth of large-scale computer and network processing of personal information in both the public and private sectors, along with major data breaches, which gave rise to public concerns about privacy and increased requirements for businesses to enhance information security measures (PPC, 2022). Second, in response to international factors, Japan faced pressure to align its legal framework with international standards, particularly the OECD 8 Principles on the protection of privacy and the flow of personal data, issued in 1980 (Ishiwaka, 2025). In addition, the EU Data Protection Directive, adopted in 1995, introduced adequacy requirements that contributed to legislative adjustments in Japan (Ishiwaka, 2025; Miyake & Partners, 2025). The draft APPI was introduced to the National Assembly in March 2001. In May 2003, APPI for enterprises was enacted, along with the “Five Laws concerning the protection of

personal information,” which govern administrative agencies and independent administrative organizations (Matsuno, 2006). In May 2004, the core regulations (Chapters 1 to 3), which cover the purpose, basic philosophy, and formulation of the Government’s basic policy, took partial effect (Matsuno, 2006). In April 2005, the APPI was fully enforced.

After full implementation, the law has undergone multiple significant amendments, reflecting developments in information technology, scientific progress, and the globalization of business activities (Matsuno, 2006). The first step was the 2015 amendment, effective from 2017. The amended law, announced in September 2015 and effective as of May 30, 2017, removed application thresholds that had previously excluded businesses handling fewer than 5,000 personal information records. As a result, APPI applies to all business operators (PPC, 2017b). The amendment clarified the definition of personal information by introducing personal identification codes, including symbols derived from physical characteristics (such as DNA, facial recognition data, and fingerprints) and public identifiers (such as passport numbers and driver’s license numbers) (Nasu, 2025; PPC, 2025b). In addition, anonymized processed information was formally incorporated into the regulatory framework to facilitate broader use of big data under conditions that prevent individual identification and re-identification (Nasu, 2025; PPC, 2025b). The second step was the 2020 amendments and the consolidation of personal data protection regulations. The amendment adopted in 2020 entered into force on April 1, 2022. A key feature of this reform was the consolidation of personal information protection regulations for both the public sector and the private sector within the APPI and under the Personal Information Protection Commission (PPC)’s authority (Nasu, 2025; PPC, 2025b).

The law mandates a periodic review every three years to assess international trends, technological advances, and the expansion of data-utilizing industries (PPC, 2017b). Demonstrating a strong capacity for adaptation in a legal document traditionally associated with stability. Instead of maintaining a rigid approach, these revisions reflect a trend toward viewing the personal data protection law as a “living document.” According to the “explanation of the policy for institutional revisions under the ‘so-called three-year review’ of the Act on the Protection of Personal

Information” on January 9, 2026, proposed amendments to Japan’s APPI include: waiving the consent requirement for personal information used solely for statistical purposes; relaxing the conditions for exceptions to the consent requirement; clarifying and tightening regulations concerning children’s personal information; establishing a new legal framework for facial feature data and similar data; and improving regulations for businesses processing information on a consignment basis (Miyake & Partners, 2026; TMI Associate, 2026). Relaxing the obligation to notify individuals of data leaks in certain cases; strengthening control over types of information that directly impact specific individuals; mandating verification of the recipient’s identity and intended use in opt-out systems; increasing flexibility in applying recommendations and orders from competent authorities; legalizing measures to address third parties who support or assist in violations; and strengthening and expanding penalties (Miyake & Partners, 2026; TMI Associate, 2026).

Another strength is that Japan’s legal system for protecting personal information is very comprehensive. Japan’s personal data protection system is structured hierarchically, with the Constitution at the apex, the APPI as the general law, and subordinate legal instruments, including Cabinet orders and PPC regulations (PPCS, 2025). The general law serves as the central normative reference, reducing regulatory overlap and establishing basic principles applicable across sectors. Regarding the basic philosophy and motto of the legal framework for personal data protection (Article 3 APPI), personal information must be handled with respect for personal dignity, ensuring appropriate management while considering its usefulness in social and business contexts (PPC, 2024; PPCS, 2025). The government has set a fundamental policy direction through Cabinet decisions and regulations, promoting consistent measures for protecting personal information. Within this framework, the PPC serves as the central supervisory authority, responsible for monitoring compliance, issuing guidance, conducting inspections, and ordering corrective measures when necessary (PPC, 2017b). Guidelines and supplementary rules play an important role. The guidelines issued by the PPC clarify statutory provisions and support effective implementation by administrative agencies, local authorities, and businesses. These guidelines cover general rules, restrictions on overseas data transfers, record-

keeping obligations, and specific rules for pseudonymized and anonymized information (PPC, 2024). Sector-specific guidance is developed in coordination with relevant ministries, taking into account sectoral characteristics in sectors such as finance, healthcare, and telecommunications. The guidelines further define mandatory and prohibited conduct and specify organizational, human, physical, and technical security measures, including tailored guidance for small and medium-sized enterprises (IPA, 2023).

Finally, Japan’s legal framework incorporates multi-layered supervision and enforcement mechanisms. First, the PPC serves as the primary supervisory authority, empowered to request reports, conduct inspections, issue recommendations, and issue legally binding orders (PPC, 2017a). Violations of PPC orders are subject to statutory penalties, including fines and imprisonment, depending on the nature of the violation (PPC, 2017a). Second, certified personal information protection organizations serve as complementary compliance mechanisms, tasked with handling complaints, developing voluntary rules, and overseeing member compliance within specific industries (PPC, 2025a). Third, mechanisms for individual participation are emphasized. The legal framework emphasizes self-governance and individual participation, enabling data subjects to request disclosure, correction, suspension of use, or cessation of provision of personal data through institutional complaint mechanisms (Matsuno, 2006). In cases involving significant data breaches, business operators are required to report incidents to the PPC and notify affected individuals, subject to statutory exceptions (PPC, 2017a).

4. DISCUSSION

4.1. Transferability and adaptation of Japan’s experience for Vietnam

The comparative findings should not be understood as suggesting that Japan’s personal information protection model can be transplanted wholesale into Vietnam, but rather that Japan provides a differentiated set of lessons for building a more coherent, adaptive, and socially responsible data governance system (PPC, 2022, 2025a).

The first transferable lesson is the need to consolidate Vietnam's personal data protection framework into a unified and hierarchical legal structure, because Vietnam's current framework remains affected by fragmentation, overlaps among sectoral laws, unclear data classification, and weak enforcement coherence (National Assembly of Vietnam, 2025; Nguyen & Ha, 2025; Nguyen, 2026b). Japan's APPI operates as a central legal framework, supported by Cabinet orders, PPC regulations, and sector-specific guidelines, and this structure is relevant to Vietnam because it helps reduce regulatory overlap while allowing sectoral implementation in fields such as healthcare, finance, telecommunications, education, e-commerce, and AI (PPC, 2024; IPA, 2023; Nguyen & Ha, 2025). However, this lesson requires adaptation, as Vietnam should not merely copy the APPI structure but clarify the relationships among the Law on Personal Data Protection, the Civil Code, cybersecurity law, consumer protection law, healthcare law, education law, and other sectoral instruments.

The second transferable lesson is the use of detailed administrative and technical guidelines, because Japan's experience shows that abstract statutory principles become effective only when translated into practical guidance for public authorities, large enterprises, small and medium-sized enterprises, and sector-specific data processors (PPC, 2022, 2024; IPA, 2023). This lesson is particularly relevant to Vietnam because enterprises still face uncertainty regarding the duties of data controllers and processors, the scope of data protection impact assessment, the standards for security measures, and the practical meaning of transparency, accountability, and the withdrawal of consent (Nguyen, 2026b).

The third transferable lesson is periodic legal review, because Japan's three-year review mechanism treats personal data protection law as a living framework capable of responding to AI, cloud computing, biometric identification, big data analytics, and cross-border data flows (PPC, 2017b, 2025b; Miyake & Partners, 2026). For Vietnam, a periodic review mechanism is necessary because technologies such as facial recognition, behavioral analytics, and AI-based profiling already create risks of privacy invasion, discrimination, and erosion of public trust.

A second group of lessons is transferable only with institutional adaptation, especially the establishment of an independent supervisory authority similar to Japan's Personal Information Protection Commission (PPC, 2017a, 2022, 2025a).

Japan's PPC has authority to issue guidance, request reports, conduct inspections, make recommendations, issue binding orders, and coordinate compliance, while Vietnam's current model places the specialized personal data protection function under the Ministry of Public Security without clearly separating data protection supervision from broader cybersecurity and public security objectives (PPC, 2017a; National Assembly of Vietnam, 2025; Trinh, 2025). Therefore, Vietnam may consider establishing an independent data protection authority, but this body must be aligned with Vietnam's administrative structure and coordinate with the Ministry of Public Security, sectoral ministries, local authorities, and agencies responsible for digital transformation and innovation (PPC, 2022). The lesson is not simply to create a "Vietnamese PPC," but to separate and clarify the functions of policy guidance, compliance supervision, complaint handling, enforcement, and technical support so that personal data protection is not absorbed entirely into cybersecurity or public security management (PPC, 2022, 2025a).

Risk-based governance is also transferable only with adaptation, because Japan's differentiated treatment of personal information, personally related information, pseudonymized information, anonymized processed information, and statistical use helps balance data protection with innovation (Nasu, 2025; PPC, 2025a, 2025b). Vietnam needs such an approach because its current framework still relies heavily on consent as the main legal basis for data processing, while exceptions and alternative legal grounds remain limited and insufficiently developed for AI, big data, and digital platform activities (National Assembly of Vietnam, 2025; Zhang, 2026). Nevertheless, risk-based exceptions should not be introduced as broad permission for data use, but should be limited by necessity, proportionality, purpose limitation, impact

assessment, transparency, technical safeguards, and the controller's burden to prove that fundamental rights are not undermined (PPC, 2025a; Verdoodt et al., 2024).

Some Japanese mechanisms cannot be directly transferred at the current stage, especially free circulation of anonymized processed information, certified personal information protection organizations, and sectoral self-regulation, because these mechanisms presuppose mature compliance capacity, reliable certification standards, and strong supervisory oversight (PPC, 2017b, 2025a; Katagiri et al., 2005). Vietnam should be cautious because de-identified or anonymized data may still be re-identified as technology develops, and the current legal framework has not yet provided detailed technical standards for anonymization, pseudonymization, de-identification, encryption, access control, and auditability (National Assembly of Vietnam, 2025).

Accordingly, Japan's experience should be used as a conditional reference rather than a ready-made model, and Vietnam should prioritize legal clarification, technical standards, sectoral guidance, supervisory capacity, and enterprise-level accountability before expanding risk-based or statistical-use exceptions (PPC, 2024; IPA, 2023; Miyake & Partners, 2026).

4.2. Institutional prerequisites and safeguards for effective implementation in Vietnam

Effective implementation requires institutional prerequisites, as personal data protection cannot rely solely on formal legal rights but must be supported by supervisory capacity, complaint mechanisms, technical guidance, and accountability duties within organizations (PPC, 2022, 2025a).

First, Vietnam should clarify the legal status of basic personal data, sensitive personal data, de-identified data, anonymized data, pseudonymized data, and personally related data, because unclear classification creates both over-protection that restricts socially valuable data use and under-protection for health, biometric, financial, children's, and other high-risk data (National Assembly of

Vietnam, 2025; Hohmann & Kollár, 2025; Nguyen, 2026b).

Second, Vietnam should develop binding or highly authoritative guidelines on consent design, withdrawal of consent, privacy notices, controller-processor contracts, data breach notification, cross-border transfer impact assessment, AI-related risk assessment, and sector-specific security measures (PPC, 2024; IPA, 2023; National Assembly of Vietnam, 2025).

Third, any independent supervisory body must have legal authority, technical expertise, financial resources, investigatory powers, and coordination mechanisms, because formal independence without the capacity to exercise it may produce symbolic reform rather than effective protection (PPC, 2017a, 2022; To, 2024).

Fourth, Vietnam should strengthen enterprise-level accountability by requiring controllers and processors, especially in high-risk or large-scale processing, to maintain processing records, conduct impact assessments, designate responsible personnel, apply organizational and technical safeguards, and respond effectively to data subject requests (IPA, 2023; PPC, 2025a).

Fifth, Vietnam should establish a multi-layered complaint mechanism that begins with internal complaint handling by controllers, continues through sectoral or local support mechanisms, and ends with review by a specialized supervisory authority (PPC, 2025a; Matsuno, 2006).

Finally, Vietnam should treat statistical-use exemptions and anonymized or de-identified data as risk-governance issues rather than automatically harmless categories, because large datasets, sensitive attributes, repeated linkage, and AI analytics may still enable re-identification, group discrimination, profiling, or indirect harm to individuals (PPC, 2025b; Zhang, 2026; Radanliev, 2025). For this reason, statistical-use exemptions should be limited to non-individualized outputs, prohibited from supporting decisions that directly affect identifiable persons, accompanied by purpose limitation and anti-re-identification rules, and subject to audit, sanctions, and supervisory review (PPC, 2025a, 2025b; Verdoodt et al., 2024; Miyake & Partners, 2026).

CONCLUSION

This study aimed to assess Vietnam's legal framework for personal data protection from a social responsibility perspective and to identify legal and institutional reforms to strengthen its effectiveness. Drawing on lessons from Japan's legislative development, governance mechanisms, and enforcement practices, the study sought to develop recommendations for improving personal data governance in Vietnam.

This study demonstrates that Vietnam has made significant progress in establishing a formal legal framework for personal data protection, particularly through the enactment of the PDPL. However, the results also reveal several remaining weaknesses, including fragmented regulations, ambiguity in data classification, and a lack of a centralized enforcement mechanism. Personal data protection in Vietnam needs a broader perspective, aligned with the new era, that recognizes social responsibility in data processing as a system defined by legal and structural design, enforcement monitoring, and risk-based governance, aiming for trust rather than solely focusing on consent mechanisms. An analysis of Japanese law reveals many positive aspects that Vietnam can learn from to improve its personal data protection legal system. These include recognizing the flexible adaptability of personal data protection laws in the context of digital transformation, adopting governance based on risk rather than rigidly applying a general framework of consent mechanisms, and especially establishing independent agencies to perform tasks consistent with the institutional framework, ensuring that what is written on paper is effectively and consistently implemented in social life. Ultimately, it can be concluded that strengthening personal data protection in Vietnam requires not only strengthening formal legal frameworks but also building capacity to ensure effective, consistent, and coherent implementation in governance. Drawing on lessons from Japan's legal structure and enforcement mechanisms, this paper contributes to both academic and policy discussions on strengthening personal data protection, thereby promoting sustainable development in Vietnam.

DECLARATION OF GENERATIVE AI IN THE WRITING PROCESS

In preparing this manuscript, the author used Grammarly to assist with proofreading and used Copilot to translate some legal texts from Japanese and Vietnamese into English. After use, the author processed and edited the text and bears full responsibility for its contents.

FUNDING

This research has been done under the research project ĐHL.26.09.QT “Personal Data Protection Legal Framework in the Context of Digital Transformation: Lessons for Vietnam from the Japanese Case Study,” of Vietnam National University, Hanoi – University of Law.

AUTHOR CONTRIBUTIONS

Conceptualization: Thi Phuong Cham Nguyen.
Formal analysis: Thi Phuong Cham Nguyen.
Investigation: Thi Phuong Cham Nguyen.
Methodology: Thi Phuong Cham Nguyen.
Resources: Thi Phuong Cham Nguyen.
Software: Thi Phuong Cham Nguyen.
Supervision: Thi Phuong Cham Nguyen.
Validation: Thi Phuong Cham Nguyen.
Writing – original draft: Thi Phuong Cham Nguyen.
Writing – review & editing: Thi Phuong Cham Nguyen.

REFERENCES

- Balboni, P., & Francis, K. E. (2025). Data ethics and digital sustainability: Bridging legal data protection compliance and ESG for a responsible data-driven future. *Journal of Responsible Technology*, 22, 100099. <https://doi.org/10.1016/j.jrt.2024.100099>
- Bui, T. L., Tran, T. H. L., & Dang, T. H. (2025). Digital Technology and Data Security in Digital Education. *Journal of Science Hanoi Open University*, 7A, 446-455. (In Vietnamese). <https://doi.org/10.59266/houjs.2025.801>
- Bui, T. N. T. (2024). Một số giải pháp góp phần hoàn thiện dữ liệu cá nhân ở Việt Nam [Some solutions to improve Vietnam's personal data protection law]. *Vietnam Integration Journal*, 339, 26-30. (In Vietnamese). <https://doi.org/10.62829/VNHN.345.53.58>
- Cahyani, A., Rosi, E. E., Yasmin, M., Jufri, S., & Saleh, J. (2025). Exploring the dynamics of personal data protection policies within the sustainable digital ecosystem: A scientometric and systematic literature review perspective. *E3S Web of Conferences*, 657(57), 01003. Retrieved from <https://www.sciengine.com/QKW-E3SWC-E3SWC/doi/10.1051/e3sconf/202565701003>
- Hoang, M. K. (2026). Luật bảo vệ dữ liệu cá nhân và vấn đề thực thi – Kinh nghiệm từ một số quốc gia phát triển. [Personal data protection laws and enforcement issues – Lessons from several developed countries]. *Tạp chí Tòa án nhân dân điện tử – Electronic Journal of the People's Court*, 26/03/2026. (In Vietnamese). Retrieved from <https://tapchitoaan.vn/luat-bao-ve-du-lieu-ca-nhan-va-van-de-thuc-thi-kinh-nghiem-tu-mot-so-quoc-gia-phat-trien15184.html>
- Hohmann, B., & Kollár, G. (2025). Reflections on the data protection compliance of AI systems under the EU AI Act, *Cogent Social Sciences*, 11(1). 2560654. <https://doi.org/10.1080/23311886.2025.2560654>
- Information-technology Promotion Agency (IPA). (2023). *Information security measures for SMEs: Guideline Version 3.1*. IPA IT Security Center. Retrieved from https://www.ipa.go.jp/en/about/activities/gg62ps000000103j-att/Information_Security_Measures_Guidelines_for_Small_and_Medium-sized_Enterprises_Version_3-1.pdf
- Ishiwaka, K. (2025). Japan's Personal Information Protection Legal Framework and Its International Initiatives. *Joint Statement Initiative on E-Commerce Workshop*. Retrieved from https://www.wto.org/library/events/event_resources/ecom_0805202510/779_2422.pdf
- Katagiri, K., Sato, H., & Hirai, K. (2005). The position of personal information in CSR. *Ritsumeikan Business Review*, 43(5), 215-241. (In Japanese). Retrieved from <https://ritsumei.repo.nii.ac.jp/records/720>
- Kitahara, M. (2007). Issues in Japan's Act on the Protection of Personal Information. *Shudo Law Review*, 29(2), 23-46. (In Japanese). Retrieved from <https://shudo-u.repo.nii.ac.jp/record/1356/files/KJ00004592759.pdf>
- Le, N. Y., Nguyen, M. H., & Nguyen, T. N. L. (2024). Analysis of the issue of personal information security in Vietnamese legal documents. *Journal of Science of Dong Thap University*, 13(6), 113-120. (In Vietnamese). <https://doi.org/10.52714/dthu.13.6.2024.1280>
- Le, T. V. A., & Duong, T. L. (2024). Xu hướng phát triển số và sự tham gia của cộng đồng doanh nghiệp vào phát triển khoa học, công nghệ và đổi mới sáng tạo ở Việt Nam. [Digital economy development trends and the business community's participation in science, technology, and innovation development in Vietnam]. *Journal of Economics and Development*, 329(2), 47-55. (In Vietnamese). <https://doi.org/10.33301/jed.vi.1978>
- Matsuno, A. (2006). One year after the enforcement of the Act on the Protection of Personal Information]. *Sompo Research Report*, 77(2006), 45-68. (In Japanese). Retrieved from https://www.sonposoken.or.jp/media/reports/sonposokenreport077_2.pdf
- McCoy, M. S., Allen, A. L., Kopp, K., Mello, M. M., Patil, D. J., Ossorio, P., Joffe, S., & Emanuel, E. J. (2023). Ethical Responsibilities for Companies That Process Personal Data. *The American Journal of Bioethics*, 23(11), 11-23. <https://doi.org/10.1080/15265161.2023.2209535>
- Miyake & Partners. (2025). Latest trends in amendments to the Act on the Protection of Personal Information. *Personal Information Protection Law Newsletter*, 12. (In Japanese). Retrieved from <https://www.miyake.gr.jp/wp-content/uploads/2025/04/個人情報保護法改正の最新動向～「個人情報保護法」の制度的課題に対する考え方を読み解く～.pdf>
- Miyake & Partners. (2026). Articlebyarticle commentary on the 2026 amendment bill to the Act on the Protection of Personal Information – A detailed commentary based on the bill approved by the Cabinet on April 7, 2026. *Personal Information Protection Law Newsletter*, 15. (In Japanese). Retrieved from <https://www.miyake.gr.jp/wp-content/uploads/2026/04/令和8年改正個人情報保護法案-1.pdf>
- Muralinathan, S. (2025). Balancing data protection and human rights in the digital age: A review. *International Journal of Science and Research Archive*, 16(01), 505-515. <https://doi.org/10.30574/ijrsra.2025.16.1.2031>
- Nasu, S. (2025). Key issues in the Act on the Protection of Personal Information. *JILIS Report*, 1, 1-15. (In Japanese). Retrieved from <https://www.jilis.org/report/2025/jilisreport-vol7no5.pdf>
- National Assembly of Vietnam. (2025). *Law on Personal Data Protection*. (In Vietnamese). Retrieved from <https://datafiles.chinhphu.vn/cpp/files/vbpq/2025/7/91qh.signed.pdf>

20. Nguyen, L. M., & Ha, T. T. B. (2025). Enhancing personal data protection on E-Commerce platforms: A case study in Vietnam. *Veredas do Direito*, 22(2), e223116. <https://doi.org/10.18623/rvd.v22.n2.3116>
21. Nguyen, N. A. D. (2023). Online Personal Data Protection Focuses on The Path of Vietnam's Digital Transformation and The Next Stage. *International Journal of Religion*, 4(2), 166-172. <https://doi.org/10.61707/613eg160>
22. Nguyen, T. P. C. (2025). Application of artificial intelligence in the healthcare sector and legal challenges: A study in Vietnam. *Journal of Cultural Analysis and Social Change*, 10(2), 1952-1962. <https://doi.org/10.64753/jcasc.v10i2.1894>
23. Nguyen, T. P. C. (2026a). Vietnamese ethical and legal challenges in protecting patient privacy through informed consent. *Veredas do Direito*, 23(2), e234253. <https://doi.org/10.18623/rvd.v23.n52.4253>
24. Nguyen, T. P. C. (2026b). Comprehensive Examination of Patients' Data Privacy in Vietnam. *Washington International Law Journal*, 35(3), 30-64. Retrieved from <https://digitalcommons.law.uw.edu/wilj/vol35/iss3/4>
25. Personal Information Protection Commission (PPC). (2017a). *Introduction to the Act on the Protection of Personal Information*. (In Japanese). Retrieved from https://www.ppc.go.jp/files/pdf/simple_lesson_2022.pdf
26. Personal Information Protection Commission (PPC). (2017b). *Handbook on the Act on the Protection of Personal Information*. (In Japanese). Retrieved from <https://www.ibarakiken-pta.ne.jp/wp-content/uploads/2020/12/3d4390f0886cd065ab51c70a085034e6.pdf>
27. Personal Information Protection Commission (PPC). (2022). *Basic policy on the protection of personal information*. (In Japanese). Retrieved from https://www.ppc.go.jp/files/pdf/20220401_personal_basicpolicy.pdf
28. Personal Information Protection Commission (PPC). (2024). *Guidelines on the Act on the Protection of Personal Information*. (In Japanese). Retrieved from https://www.ppc.go.jp/files/pdf/241202_guidelines01.pdf
29. Personal Information Protection Commission (PPC). (2025a). *Guidelines on the Act on the Protection of Personal Information (General rules)*. (In Japanese). Retrieved from https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/
30. Personal Information Protection Commission (PPC). (2025b). *Considerations on institutional issues of the Act on the Protection of Personal Information*. (In Japanese). Retrieved from https://www.ppc.go.jp/files/pdf/seidotekikadaini-taisurukangaekatanitsuite_250305.pdf
31. Personal Information Protection Commission Secretariat (PPCS). (2025). *Policies related to the handling of personal information*. (In Japanese). Retrieved from https://www.cas.go.jp/jp/seisaku/digital_gyozaikaikaku/data8/data8_siryou7.pdf
32. Pham, T. H., Phan, T. A., Trinh, P. A., Mai, X. B., & Le, Q. C. (2023). Ảnh hưởng của cảm nhận về rủi ro bảo mật và quyền riêng tư đến niềm tin và hành vi kiểm soát quyền riêng tư của người dùng trên mạng xã hội [The effect of perceptions of security and privacy risks on users' trust and privacy control behaviors on social networks]. *Journal of Economics and Development*, 314, 35-45. (In Vietnamese). <https://doi.org/10.33301/jed.vi.1166>
33. Radanliev, P. (2025). Privacy, ethics, transparency, and accountability in AI systems for wearable devices. *Frontiers in Digital Health*, 7, 1431246. <https://doi.org/10.3389/fdgh.2025.1431246>
34. Rezac, F. (2022). The Role of Privacy Protection in Business Models for Sustainability: A Conceptual Integration from an Ecosystem Perspective. *Journal of Business Models*, 10(2), 31-57. <https://doi.org/10.54337/jbm.v10i2.6952>
35. Schubert, K. D., & Barrett, D. (2024). Chapter 5: Data Governance, Privacy, and Ethics. In M. C., Lacity & L. Coon (Eds.), *Human Privacy in Virtual and Physical Worlds: Multidisciplinary Perspectives* (pp. 87-110). Palgrave Macmillan. https://doi.org/10.1007/978-3-031-51063-2_5
36. Srivastava, P., & Siddiqui, S. (2024). Data Protection in the Age of Social Regulation: A Conceptual. *ShodhKosh: Journal of Visual and Performing Arts*, 5(6), 1919-1924. <https://doi.org/10.29121/shodhkosh.v5.i6.2024.2756>
37. Tada, T. (2006). Information security and corporate social responsibility. *Unisys Technology Review*, 86, 153-164. (In Japanese). Retrieved from
38. TMI Associate. (2026). *Commentary on the 'Policy for Institutional Reform of the Act on the Protection of Personal Information, the so-called Triennial Review' (January 9, 2026)*. Retrieved from <https://www.tmi.gr.jp/eyes/blog/2026/17876.html>
39. To, T. L. (2024). Some legal aspects of personal data protection in the world – experience for Vietnam. *Cogent Social Sciences*, 10(1), 2414872. <https://doi.org/10.1080/23311886.2024.2414872>
40. Tran, T. L. (2024a). Xây dựng khung pháp lý chung ASEAN về chuyển dữ liệu quốc tế: Kinh nghiệm từ Liên minh châu Âu [Developing a common ASEAN legal framework on international data transfers: Experiences from the European Union]. *Vietnam Journal of Legal Sciences*, 11(183), 68-80. <https://doi.org/10.70236/tckhplvn.163>
41. Tran, V. D. (2024b). 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 developing laws on artificial intelligence]. *Vietnam Journal of Legal Sciences*, 9(181), 30-39. (In Vietnamese). <https://doi.org/10.70236/tckhplvn.115>
42. Trinh, P. T. (2025). Những điểm nổi bật của Luật bảo vệ dữ liệu cá nhân mới của Việt Nam (Luật BVĐLCN 2025) [Key highlights of Vietnam's new Personal Data Protection Law]. Vietnam Busi-

- ness Law (Venture North Law). (In Vietnamese). Retrieved from <https://vietnam-business-law.info/blog-lut-kinh-doanh/2025/10/31/nhng-im-ni-bt-ca-lut-bo-v-d-liu-c-nhn-mi-ca-vit-nam-lut-bvdlcn-2025>
43. Vamsi, K. P. (2025). Privacy, Surveillance, and Consent in the Age of Automated Data Processing: Societal Implications of Enterprise Analytics. *European Modern Studies Journal*, 9(5), 976-983. [https://doi.org/10.59573/emsj.9\(5\).2025.89](https://doi.org/10.59573/emsj.9(5).2025.89)
 44. Verdoodt, V., Zang, Y., & Lievens. E. (2024). Safeguarding the child's right to privacy and data protection in the European Union and China: a tale of state duties and business responsibilities. *The International Journal of Human Rights*, 28(2), 125-147. <https://doi.org/10.1080/13642987.2023.2233917>
 45. Wylde, V., Prakash, E., Hewage, C., & Platts, J. (2023). Post-COVID-19 Metaverse Cybersecurity and Data Privacy: Present and Future Challenges. In C. Hewage, Y. Rahulamathavan, & D. Ratnayake (Eds.), *Data Protection in a Post-Pandemic Society: Laws, Regulations, Best Practices and Recent Solutions* (pp. 1-48). Cham: Springer. https://doi.org/10.1007/978-3-031-34006-2_1
 46. Yeung, K., & Bygrave, L. A. (2021). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance*, 16(1), 137-155. <https://doi.org/10.1111/rego.12401>
 47. Zhang, J. (2026). Research on legal issues of personal information protection in the context of big data. *Journal of Cases on Information Technology*, 28(1), 1-15. Retrieved from <https://www.sciencedirect.com/org/science/article/pii/S1548771726000291>
 48. Zisu, M.-A. (2025). Personal Data Protection in the Era of Artificial Intelligence: Legal Challenges and Solutions. *Anuarul Universității "Petre Andrei" din Iași, Fascicula: Drept, Științe Economice, Științe Politice*, 34, 251-259. <https://doi.org/10.63331/upalaw/34/23>