



The right to personal data protection in the digital era: legal challenges, international experience and recommendations for Vietnam

Nguyen Dang Nghia

Ho Chi Minh City Open University, Vietnam

DOI: <https://doi.org/10.66856/ijl.2026.12.4.12325>

Abstract

The shift of social, commercial, and administrative life onto digital platforms has turned personal data into an economic asset and, at the same time, into a primary object of risk. This article examines the right to personal data protection in the digital era, analysing the roles of data subjects, data controllers and processors, and platform operators, and comparing Vietnam's framework with those of the European Union, the United States, and Singapore. It shows that, although Vietnam's recent legislative developments, notably the Law on Personal Data Protection (Law No. 91/2025/QH15) and the Law on Data (Law No. 60/2024/QH15), have raised the protection of personal data to the statutory level, these instruments still operate alongside the Law on Cybersecurity, the Civil Code, and consumer-protection rules without a fully integrated mechanism. As a consequence, the standards of consent, the allocation of liability among the actors in the data chain, and the accessibility of remedies for individuals do not yet match the scale of potential digital harm. To address this, the article proposes five solutions that would connect these instruments into a coherent protection framework. These measures aim to make the key actors in the digital market accountable for how they collect, use, transfer, and secure personal data. Ultimately, closing these gaps would better safeguard individuals online while sustaining the trust on which the digital economy depends.

Keywords: Personal data protection, data subject rights, consent, digital platforms, cross-border data transfer, privacy, Vietnam

Introduction

Almost every transaction in contemporary life, from opening a bank account and ordering food to using a social network or a learning application, generates personal data. Names, phone numbers, identity numbers, locations, biometric templates, purchasing histories, and patterns of browsing are collected continuously, combined with one another, and used to predict and influence behaviour. In the digital economy, such data is no longer a by-product of services but a core input of business models built on targeted advertising, credit scoring, recommendation systems, and the training of artificial intelligence. These observations are general in nature and are not drawn from a specific statistical source.

This development carries a structural downside. The individual to whom the data relates is typically the party with the least information and the least bargaining power. Consent is requested through lengthy notices that few people read; the purposes for which data is later used are often broader than those the individual had in mind; and once data has been leaked, copied, or sold, the harm is difficult to reverse. When these features are exploited, for example through bundled consent, undisclosed profiling, or the unlawful trading of customer databases, the conduct may amount to more than a technical breach of regulations. It may infringe a fundamental right to privacy and cause concrete losses such as fraud, impersonation, harassment, and reputational damage. The right to privacy and the right to personal data protection overlap rather than coincide, however, since not every act of data processing interferes with private life, and not every privacy intrusion involves personal data in the technical sense.

Until recently, Vietnamese law protected personal information mainly through scattered provisions. The

Constitution 2013 and the Civil Code 2015 recognised the inviolability of private life and personal secrets ^[1, 2], while specific obligations on the handling of personal information appeared in sector-specific legislation and, more systematically, in Decree No. 13/2023/ND-CP on personal data protection ^[3]. This arrangement left open questions about the legal force of the rules, the position of those who process data, and the remedies available to individuals. The 2024–2025 legislative developments have begun to narrow this gap. The Law on Data (Law No. 60/2024/QH15, effective 1 July 2025) establishes a general framework for the creation, management, and exploitation of digital data ^[4]. The Law on Personal Data Protection (Law No. 91/2025/QH15, effective 1 January 2026) elevates the regime for personal data to the level of a dedicated statute, setting out the rights of data subjects, the obligations of controllers and processors, and rules on cross-border transfer and sanctions ^[5]. These instruments nonetheless sit alongside the Law on Cybersecurity 2018 ^[6], the Civil Code 2015, and the Law on Protection of Consumer Rights 2023 ^[7], so the question is one of coordination between norms rather than a simple absence of rules. No unified mechanism yet ensures that a single incident, such as a breach affecting consumers' data on an e-commerce platform, is assessed consistently under all of these regimes.

Accordingly, this article poses three research questions. First, what is the legal content of the right to personal data protection, and how should the responsibilities of the data subject, the controller or processor, and the platform operator be distinguished? Second, using the main data-processing practices of digital platforms as a frame of reference, which practices are most likely to infringe that right, and on what criteria can they be assessed against the Vietnamese rules? Third, what specific lessons do the

legislative experiences of the European Union, the United States, and Singapore offer for improving Vietnam's legal framework?

Materials and Methods

The article uses doctrinal analysis of the relevant Vietnamese legal instruments, cited by their titles and numbers: the Constitution 2013; the Civil Code 2015 (Law No. 91/2015/QH13); the Law on Cybersecurity 2018 (Law No. 24/2018/QH14); the Law on Protection of Consumer Rights 2023 (Law No. 19/2023/QH15); the Law on Data (Law No. 60/2024/QH15); the Law on Personal Data Protection (Law No. 91/2025/QH15); and Decree No. 13/2023/ND-CP together with the implementing guidance issued under the new Law. Because several of these instruments are recent and their implementing documents are still developing, the specific provisions, effective dates, and sanction levels discussed below should be verified against the official promulgated texts before being relied upon. A comparative legal method is applied to the frameworks governing personal data in the European Union (Regulation (EU) 2016/679, the General Data Protection Regulation, GDPR), the United States (the California Consumer Privacy Act as amended by the California Privacy Rights Act, together with the enforcement powers of the Federal Trade Commission under Section 5 of the FTC Act), and Singapore (the Personal Data Protection Act 2012). These jurisdictions were selected because they represent, respectively, a comprehensive rights-based model, a sectoral and state-level model complemented by consumer-protection enforcement, and a regional model with an accountability-oriented design. Finally, analytical and evaluative methods are used to identify the gaps in Vietnamese law and to propose solutions suited to the fast-changing nature of digital technologies.

Results and Discussion

1. The legal nature of the right to personal data protection

The modern idea of protecting private life is commonly traced to Warren and Brandeis's account of a "right to be let alone" in the late nineteenth century^[8], and was later developed by Westin into the notion of informational self-determination, the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others^[9]. Solove's taxonomy of privacy shows, further, that harms in the information age arise not only from disclosure but also from aggregation, secondary use, and exclusion of the individual from knowledge about how data is handled^[10]. These ideas explain why the right to personal data protection is not merely a subset of the right to privacy. It is a procedural and structural right: it equips individuals with a set of entitlements (to be informed, to consent, to access, to correct, to delete, to object) and imposes on those who process data a set of duties (lawfulness, purpose limitation, minimisation, security, accountability) that operate even where no private secret has been revealed.

The Vietnamese framework reflects this dual character. At the constitutional and civil level, private life and personal secrets are protected as personal rights^[1, 2]. At the statutory level, the Law on Personal Data Protection defines personal data, distinguishes basic from sensitive personal data, and sets out the rights of data subjects, which, as the authors

read the Law, include the rights to be informed, to consent or withhold consent, to access, to withdraw consent, to request deletion or restriction of processing, to object, to lodge complaints, to claim compensation, and to self-protection^[5]. The Law also defines the principal roles in the data chain: the data controller, who determines the purposes and means of processing; the data processor, who processes data on behalf of the controller; and the controller-cum-processor, who performs both functions^[5]. The precise wording and numbering of these provisions should be checked against the official text.

2. The allocation of responsibility among actors in the data chain

When personal data is mishandled, at least three kinds of actors are usually involved: the controller, typically a business that decides why and how data is collected and obtains the direct commercial benefit; the processor or service provider, which stores, analyses, or transmits data on the controller's behalf; and the platform operator, which provides the infrastructure, the interface through which consent is requested, and often the advertising and analytics ecosystem in which data circulates. On the model of responsibility allocation adopted here by the authors, none of these actors holds all of the information and all of the control. The controller may not understand the technical flows inside a third-party software development kit embedded in its application; the processor may not know the purposes for which the controller intends to use the data; and the platform may be unable to verify whether every application distributed through it respects the representations made to users. The individual, by contrast, can neither observe nor audit any of these processes. This is a multi-party attribution structure in which responsibility must be distributed among actors with asymmetric information and control.

The Law on Personal Data Protection begins to address this problem by imposing independent obligations on controllers and processors, including obligations to process data lawfully and for specified purposes, to obtain valid consent where consent is the legal basis, to apply security measures, to notify the competent authority and, where required, affected individuals of breaches, to carry out impact assessments for certain processing activities, and to comply with conditions on cross-border transfer^[5]. The authors read the requirement of valid consent as demanding that consent be given voluntarily, in a clear and specific manner, for identified purposes, and that silence or the absence of a response not be treated as agreement; this reading should be confirmed against the statutory text and implementing guidance. Liability for violations is best understood as administrative in the first instance, without prejudice to civil liability for damages or to criminal liability in serious cases such as the unlawful trading of personal data. The Law on Data adds a complementary dimension by regulating data as an asset and by setting rules for data held by the public sector and for data products and services^[4], while the Law on Cybersecurity continues to govern matters such as data localisation and the responsibilities of service providers in cyberspace^[6].

3. Common digital practices measured against the right to personal data protection

Data-protection rules are often discussed in abstract terms, but infringements occur through concrete and recurrent

practices. Where these practices cause harm, their legal nature may extend beyond a technical regulatory breach: they can engage the right to privacy in the Civil Code, the consumer's right to be protected from unfair terms and

misleading conduct under consumer law, and, in serious cases, criminal liability. Table 1 maps some common practices on digital platforms against the corresponding rights and duties under the new data-protection regime.

Table 1: Common digital practices mapped against data-protection rights and duties

Digital practice	Right or duty engaged	Typical manifestation on digital platforms
Consent collection	Consent must be voluntary, clear, and specific; silence is not consent	Pre-ticked boxes; bundling of consent for several purposes into a single "Accept all" button
Profiling and targeted advertising	Right to be informed of purposes; right to object to or restrict processing	Tracking of browsing behaviour across apps and sites to build advertising profiles without a meaningful opt-out
Trading of personal data	Prohibition of unlawful buying and selling of personal data	Leaked or scraped databases offered for sale through messaging groups and online forums
Security incidents	Security safeguards and breach-notification duties	Delayed or absent notice to affected individuals after unauthorised access to a customer database
Cross-border transfer and AI training	Transfer impact assessment and safeguards for data sent abroad	Use of users' content and behavioural data by offshore cloud or AI providers without clear disclosure
Children's data	Heightened protection and verified parental consent for minors	Games and short-video apps collecting minors' location, voice, and images with only a self-declared age

(Source: compiled by the author)

This mapping reveals two limitations. First, the practices in Table 1 are rarely isolated. A single product can combine bundled consent, behavioural profiling, offshore transfer, and weak security, so that the same conduct engages several instruments at once. Absent a clear coordinating rule, an enforcement authority may treat the matter narrowly, as a consumer-complaint issue, a cybersecurity issue, or a data-protection issue, even though the substance of the conduct is a systemic failure of accountability. Second, the consequences of a violation are borne primarily by individuals who find it difficult to prove causation and quantify loss. A person whose identity data has been used to open a fraudulent loan account can see the harm clearly but can rarely demonstrate which of the several organisations that held the data was responsible for the leak, which leaves the right to compensation largely theoretical.

4. International experience

European Union: The GDPR is the reference point for comprehensive, rights-based regulation^[11]. Its core consists of principles relating to processing (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability), a catalogue of data subject rights that includes access, rectification, erasure, restriction, portability, and objection, and detailed conditions for valid consent, which must be freely given, specific, informed, and unambiguous. Two features deserve emphasis. The first is its extraterritorial reach: the Regulation applies to organisations outside the Union that offer goods or services to, or monitor the behaviour of, individuals in the Union, which prevents the avoidance of obligations through the location of servers. The second is the principle of accountability, which requires controllers to be able to demonstrate compliance through records of processing, impact assessments, and, in defined cases, a data protection officer. Enforcement is backed by administrative fines that can reach the higher of EUR 20 million or four per cent of worldwide annual turnover for the most serious infringements, a design intended to make penalties proportionate to the scale of the undertaking rather than to a fixed national ceiling^[11]. The strength of this approach is its technological neutrality; the weakness often cited is the compliance burden, particularly for small enterprises.

United States: The United States has no single federal statute equivalent to the GDPR. Protection is built from sectoral laws, state legislation, and general consumer-protection enforcement. At the state level, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, grants residents rights to know, delete, correct, and opt out of the sale or sharing of their personal information, and created a dedicated enforcement agency^[12]. At the federal level, the Federal Trade Commission uses Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, to act against companies that misrepresent their privacy practices or fail to maintain reasonable security^[13]. The significance of this approach lies in its focus on the gap between what a company promises and what it does: a privacy notice becomes a representation that can be enforced. Its limitation is fragmentation, which produces uneven levels of protection depending on sector and residence.

Singapore: Singapore's Personal Data Protection Act 2012 illustrates an accountability-oriented model in a regional context^[14]. It is built on consent, purpose, and reasonableness obligations, requires organisations to appoint a data protection officer, and, following amendments, introduced mandatory notification of data breaches that meet prescribed thresholds and strengthened financial penalties, which may be calculated by reference to annual turnover for larger organisations. Greenleaf's comparative study of Asian data-privacy laws shows that the region has moved steadily toward GDPR-inspired features while retaining distinctive local choices on enforcement and on the role of the state^[15]. The Singapore model is instructive for Vietnam because it pairs relatively clear obligations with an administrative regulator able to act quickly, and because it treats breach notification as a core duty rather than an optional courtesy.

A comparison of the three models reveals a common approach that transcends their differences in legislative technique. First, each treats the individual's control over personal data as a protected interest in its own right, supported by enforceable entitlements and not merely by the controller's goodwill. Second, each makes obligations concrete: valid consent, breach notification, impact assessment, and data-subject requests are accompanied by

procedures, content requirements, and, in many cases, time limits, rather than resting on a generic duty of care. Third, each attaches responsibility to the organisations that actually control the data, calibrates sanctions to the size of the undertaking or the gravity of the harm, and gives a specialised authority the means to investigate and act. Taken together, these features express a coherent regulatory philosophy: meaningful protection requires reaching the actors who shape data flows, defining their obligations with technical precision, and ensuring that sanctions are large enough to change behaviour. It is against these three lessons that the gaps in Vietnamese law, examined next, come into sharp relief.

5. Some gaps in Vietnamese law

Measured against the three lessons drawn above, the Vietnamese framework currently exhibits four principal gaps, spanning the coordination of norms, the standards of consent, the allocation of liability among actors, and the accessibility of remedies and enforcement. These gaps are mutually reinforcing rather than isolated, and together they make the protection of personal data in practice uneven.

As to coordination of norms: The first gap is one of missing connecting rules rather than missing norms. The Law on Personal Data Protection, the Law on Data, the Law on Cybersecurity, the Civil Code, and the consumer-protection legislation each address part of the problem, but there is no explicit mechanism that determines which authority leads when one incident engages several regimes, how their definitions of personal data and data processing relate to one another, or how sanctions imposed under one instrument are to be reconciled with those under another. This does not mean that protection is absent; the difficulty is the absence of an express bridge, which leaves the handling of complex incidents contestable and slow. In a digital environment where data moves across organisations and borders within seconds, a fragmented institutional response risks leaving precisely the most serious, multi-party violations without a clear owner.

As to consent standards: The second gap, by contrast, is one of missing guidance rather than missing norm. The statutory requirement that consent be voluntary, clear, and specific has not yet been made concrete for the interfaces through which consent is actually collected. As a result, compliance is assessed without a unified yardstick. It remains uncertain whether a pre-ticked box satisfies the requirement, whether a single “Accept all” button can validly cover several unrelated purposes, whether a link to a long privacy policy amounts to being informed, and what constitutes verifiable parental consent for a child using a mobile application. This ambiguity hampers the regulator’s ability to prove violations and allows those who wish to evade the obligation to adopt a formalistic mode of compliance that leaves individuals without real control over their data.

As to shared liability: The framework allocates substantial responsibility to controllers and processors, but it lacks a clear mechanism for the joint responsibility of the several organisations that jointly determine or contribute to a processing operation, such as an application owner, an advertising network, an analytics provider, and a cloud host.

It should be emphasised that this is a gap to be filled and not a rule to be described: the present allocation makes it difficult for an individual to identify who must answer for a leak or an unlawful use, and it weakens the incentive for each party to scrutinise the practices of its partners. Where a controller can point to a processor, and the processor to a subcontractor, the individual’s claim dissolves into a chain of referrals.

As to remedies and enforcement: The Law on Personal Data Protection provides for administrative penalties and recognises a right to claim compensation^[5], but the practical accessibility of these remedies remains limited. Individuals face significant evidentiary burdens in proving causation and quantifying non-material loss, the costs of individual litigation often exceed the value of the claim, and there is no developed mechanism for collective redress where a single breach affects very large numbers of people. At the same time, the effectiveness of sanctions depends on their proportionality: where the commercial benefit of unlawful processing, or the saving from neglecting security, exceeds the penalty, the sanction loses its deterrent function and may be treated as a foreseeable cost of doing business. Whether the new sanctioning regime, as implemented, achieves this proportionality for the largest data-driven enterprises remains to be tested in practice.

The four gaps outlined above show that the Vietnamese framework, although it has advanced considerably at the statutory level, has not yet kept pace with the complexity of data processing in the digital economy. Addressing all four together is a necessary precondition for securing a trustworthy environment for individuals and businesses alike.

Recommendations for improving the law of Vietnam

On the basis of the analysis above, the article proposes five groups of solutions, offered as recommendations *de lege ferenda* rather than as descriptions of law currently in force. They are designed to be implemented along a roadmap tied to decrees and guiding circulars, so as to avoid the need to amend several statutes simultaneously. This approach favours legislative feasibility while allowing the new rules to enter practice without waiting for the often protracted process of statutory amendment.

First, issue an inter-agency guiding document on coordinated enforcement: The competent authorities should consider issuing an inter-agency guiding document, jointly developed by the Ministry of Public Security as the authority principally responsible for personal data protection and by the ministries responsible for consumer protection, e-commerce, and information and communications, to clarify how the Law on Personal Data Protection, the Law on Data, the Law on Cybersecurity, and consumer-protection rules apply to a single incident. Such a document should identify a lead authority for multi-regime incidents, harmonise key definitions, and establish procedures for information-sharing and for avoiding duplicated sanctions. Because the current instruments do not clearly allocate overlapping competence, such a document is itself a legislative proposal rather than a restatement of existing authority.

Second, issue consent and notice standards for each interface and context: The competent authority should adopt operational standards on consent and privacy notices,

on the model of the context-specific approach seen in comparative practice. The following requirements are put forward as the author's proposal, not as a description of current law: that consent for separate purposes be requested separately and not bundled; that pre-ticked boxes and silence not be accepted as consent; that a short, layered notice setting out purposes, recipients, and retention be presented at the point of collection, with the full policy available by link; that withdrawing consent be as easy as giving it; and that applications directed at minors apply an age-assurance and parental-consent procedure proportionate to the risk. Concretising consent by context would create a unified yardstick for assessing compliance and reduce formalistic compliance.

Third, establish a mechanism of shared liability along the data chain: A mechanism of shared liability among controllers, joint controllers, processors, and platform operators should be introduced, this being a proposal for reform, since no such general mechanism presently exists. Where several organisations jointly determine the purposes or means of processing, they should be required to allocate their responsibilities in a transparent arrangement made available to the data subject, and the data subject should be able to exercise rights against any of them. Controllers should remain accountable for the conduct of the processors they select and should be required to conduct and document due diligence before engaging them. When responsibility is allocated in proportion to each party's capacity to control the data, each is encouraged to ensure lawful handling, which protects individuals while clarifying obligations for businesses.

Fourth, calibrate sanctions and widen access to remedies: Sanctions for serious violations should be calculated by reference to the revenue of the organisation or the benefit obtained, subject to appropriate caps, rather than relying solely on fixed monetary ceilings, so that penalties retain their deterrent effect against large enterprises. To the extent that the Law already provides for revenue-based sanctions in specified cases, the guiding documents should clarify their application; to the extent it does not, their adoption would require amendment of the governing rules and is proposed on that footing. In parallel, the State should consider procedural measures that facilitate redress: a rebuttable presumption of causation where an organisation that held the data failed to apply mandatory security measures, simplified complaint procedures, and a role for consumer and social organisations in bringing representative claims on behalf of affected groups.

Fifth, require records, breach logs, and capacity-building: Controllers and processors of significant scale should be required to maintain records of processing activities and logs of security incidents and of access to sensitive data for a minimum period, for example twenty-four months, so that the competent authority can reconstruct what occurred after a breach. So that this obligation does not itself create privacy risk, it should be grounded in an express legal basis specifying the purpose of retention and the safeguards applicable to any personal data contained in the logs. These duties should be complemented by support for small and medium-sized enterprises, including model templates and simplified compliance guidance, and by

public education programmes that strengthen individuals' ability to exercise their rights.

These five groups of solutions are closely linked and mutually reinforcing: the coordination document lays the basis for coherent enforcement; the consent standards and the shared-liability mechanism shape compliant conduct; calibrated sanctions and accessible remedies ensure deterrence and redress; and the recordkeeping obligation supplies the evidentiary foundation for the whole process. Implemented in a coordinated way along a roadmap of decrees and circulars, they would help Vietnam's personal data protection framework adapt to the realities of the digital economy.

Conclusion

The 2024–2025 wave of Vietnamese legislation marks an important shift from a position in which personal data was protected mainly through general privacy provisions and a sub-statutory decree to one in which the rights of data subjects and the duties of those who process data are set out in dedicated statutes. As matters stand, however, these instruments still operate alongside other regimes without a fully integrated mechanism for coordination, and the law does not yet address squarely the case in which a single act simultaneously breaches consent requirements, security duties, and consumer-protection rules while affecting very large numbers of individuals. The experience of the European Union, the United States, and Singapore points in a common direction: recognising individual control over personal data as an enforceable interest, making obligations concrete and procedural, and attaching responsibility and proportionate sanctions to the organisations that actually control the data. By way of reform, connecting Vietnam's existing instruments, making consent standards concrete, introducing shared liability along the data chain, calibrating sanctions and widening access to remedies, and requiring records and breach logs would together build a unified protection framework proportionate to the pace of digital development, promoting trust and legal certainty in the digital economy.

References

1. Constitution of the Socialist Republic of Vietnam 2013, Article 21.
2. National Assembly of the Socialist Republic of Vietnam. Civil Code (Law No. 91/2015/QH13), Article 38, 2015.
3. Government of the Socialist Republic of Vietnam. Decree No. 13/2023/ND-CP on personal data protection, 2023.
4. National Assembly of the Socialist Republic of Vietnam. Law on Data (Law No. 60/2024/QH15), 2024.
5. National Assembly of the Socialist Republic of Vietnam. Law on Personal Data Protection (Law No. 91/2025/QH15), 2025.
6. National Assembly of the Socialist Republic of Vietnam. Law on Cybersecurity (Law No. 24/2018/QH14), 2018.
7. National Assembly of the Socialist Republic of Vietnam. Law on Protection of Consumer Rights (Law No. 19/2023/QH15), 2023.
8. Warren SD, Brandeis LD. The Right to Privacy. *Harvard Law Review*, 1890;4(5):193–220.

9. Westin AF. Privacy and Freedom. New York: Atheneum,1967.
10. Solove DJ. Understanding Privacy. Cambridge, MA: Harvard University Press,2008.
11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union,2016.
12. California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act of 2020.
13. Federal Trade Commission Act, Section 5, 15 U.S.C. § 45.
14. Republic of Singapore. Personal Data Protection Act 2012 (as amended).
15. Greenleaf G. Asian Data Privacy Laws: Trade and Human Rights Perspectives. Oxford: Oxford University Press,2014.