

PERSONAL DATA PROTECTION IN VIETNAM: CONSENT, CONTROLLER ACCOUNTABILITY AND EFFECTIVE REMEDIES

Tống Thị Thu Trang

Department of Law, TNU – University of Sciences, Thai Nguyen, Vietnam

ABSTRACT

The entry into force of Vietnam's Law on Personal Data Protection No. 91/2025/QH15 on 1 January 2026 marks a transition from a predominantly decree-based regulatory approach to a dedicated legislative framework. This article examines the doctrinal structure of personal-data protection, with particular attention to informed consent, lawful processing, controller and processor responsibility, cross-border transfers, sensitive information, children's data, and the practical availability of remedies. Through statutory interpretation and comparative analysis informed by international data-protection principles, it argues that the central implementation challenge is not merely obtaining formal consent but making data processing intelligible, contestable and accountable across complex digital services. The paper proposes risk-based compliance, more meaningful notices, auditable data governance, accessible complaint procedures and proportional safeguards for smaller organizations. It distinguishes binding Vietnamese law from comparative policy standards and identifies questions requiring judicial and administrative clarification.

Keyword: *Personal data; privacy; consent; data controller; accountability; cross-border transfer; Vietnam.*

1. INTRODUCTION

Personal information is a basic input into digital commerce, employment, education, finance and public administration. Identity records, location histories, purchase behavior and inferred preferences enable organizations to provide services, but they can also expose individuals to fraud, discrimination, surveillance or unwanted profiling. Unlike a conventional transfer of a physical object, disclosure of personal data rarely ends with one recipient. Data may be copied, combined, stored and re-used by several parties beyond the individual's direct knowledge.

Vietnam has moved toward a more systematic framework through the Law on Personal Data Protection No. 91/2025/QH15, effective 1 January 2026. Its significance is institutional as well as substantive: personal-data safeguards are no longer treated solely as a set of obligations appended to particular transactions or information systems. The statute provides a dedicated basis for allocating rights and responsibilities in data processing. However, formal rights require understandable procedures, credible enforcement and viable redress.

This article employs doctrinal analysis of the 2025 Law and the pre-existing regulatory architecture, supported by comparative consideration of the OECD Privacy Guidelines and the European Union's GDPR. Comparative references are analytical benchmarks, not claims that foreign requirements automatically apply in Vietnam. The argument is that meaningful accountability must be evaluated over the full data lifecycle, from collection through deletion or justified retention.

2. LEGAL FOUNDATIONS AND REGULATORY DESIGN

Personal-data protection concerns both individual autonomy and the duties imposed on entities that decide why and how information is processed. The 2025 Law establishes a statutory vocabulary for understanding those relationships. The starting point is to separate the substantive legitimacy of processing from its technological feasibility. The fact that a platform can capture information does not demonstrate a lawful or proportionate need to do so.

A data-governance framework must distinguish collection, storage, disclosure, analysis and destruction. Risks arise at different points: excessive initial collection, unauthorized

employee access, inadvertent third-party disclosure, inaccurate automated inference, or indefinite retention. An organization that secures its servers but cannot explain its processing purpose still has an accountability problem. Equally, one that provides a detailed privacy notice but neglects access controls fails to deliver meaningful protection.

Vietnamese law should be read alongside sector-specific requirements concerning cybersecurity, consumer transactions, electronic transactions and civil-law protection of personal interests. These legal regimes overlap but serve different purposes. A cybersecurity duty to protect an information system, for example, is not synonymous with a data subject's ability to challenge the use of information about them. Legal interpretation should keep these dimensions connected without collapsing them into one generalized compliance checklist.

3. CONSENT AND THE LIMITS OF FORMAL CHOICE

Consent is valuable because it recognizes that the individual has a stake in decisions affecting personal information. Yet consent is difficult to regard as meaningful where a lengthy notice is presented on a small screen, acceptance is bundled with unrelated uses, or refusal results in exclusion from an essential service. A valid consent framework therefore needs clarity about purpose, relevant categories of information, intended recipients and the consequences of refusal.

The distinction between genuine choice and formal assent is especially important in employment and education. Workers and students may have limited ability to negotiate the terms under which institutions collect attendance, performance, biometric or location information. In these relationships, the existence of a clicked box should not end the legal inquiry. Decision-makers should consider whether the processing purpose is legitimate, whether less intrusive means are available, and whether affected individuals have practical channels for objection or correction.

Consent management also becomes complicated when a service changes its business model. Permission to process information for completing a transaction should not be assumed to authorize indefinite behavioral profiling or unrelated commercial disclosures. Organizations should

maintain purpose-specific records, provide usable withdrawal mechanisms where applicable, and be able to demonstrate what notice and choice existed at the relevant time.

4. ACCOUNTABILITY OF CONTROLLERS, PROCESSORS AND THIRD PARTIES

The most important institutional question is who can explain and justify a processing decision. Data ecosystems often distribute tasks among a service provider, cloud host, analytics vendor, advertising intermediary and subcontractors. Assigning formal labels without mapping actual control can obscure responsibility. Accountability requires an organization to identify which actor determines processing purposes, which actor executes instructions, and which actor bears responsibility when those instructions are unlawful or security arrangements inadequate.

Internal governance should include a processing inventory, clear authorization levels, retention rules, contractual controls over third parties, staff training, incident reporting and periodic review. These mechanisms transform legal standards into verifiable practice. The existence of a policy document alone is insufficient; auditors and regulators need evidence that the policy shapes operational choices. Procurement contracts should not allow an organization to evade public-facing obligations merely by outsourcing technical functions.

Small organizations present a proportionality challenge. Requiring an identical compliance infrastructure for a small clinic and a national platform may waste scarce resources without increasing protection. Risk-based guidance should focus on the sensitivity of records, volume of processing, possibility of harm and extent of onward transfer. Proportionality should concern the methods of compliance, not exemption from foundational duties of lawful processing and security.

5. CROSS-BORDER PROCESSING AND VULNERABLE DATA SUBJECTS

Cross-border data flows support cloud computing, international payroll systems and digital services, but they increase the difficulty of identifying effective safeguards and obtaining remedies. A transfer assessment should identify recipients, onward disclosures, technical protections and the practical capacity to investigate a breach. The legal

focus should be on accountable transfer conditions rather than an assumption that domestic storage alone guarantees control.

Children's data warrants careful institutional attention. Children may not anticipate the longer-term consequences of publishing personal information, while educational technologies can normalize continuous tracking. Age-sensitive notices, justified collection limits, stronger default settings and restrictions on secondary commercialization can reduce foreseeable harm. The precise statutory rules and applicable implementing measures must be checked for each processing context, rather than inferred from foreign legal models.

Sensitive information creates heightened risks even when collected for legitimate purposes. Health records, biometric identifiers and similarly consequential data can permit identification or inference that individuals cannot easily reverse. Institutions should use stronger access controls, purpose limitations, deletion schedules and documented necessity assessments. These controls are particularly important when databases are linked across agencies or vendors.

6. ENFORCEMENT PROBLEMS AND REFORM DIRECTIONS

The first challenge is evidentiary asymmetry. An individual may know that information was misused but not which company transferred it, when the transfer occurred, or what internal rules governed access. Effective complaint handling therefore depends on records that can be disclosed or examined without unnecessarily exposing other individuals' information. Regulators need technical competence, while courts require clear standards for evaluating causation, damage and corrective relief.

Second, transparency should be assessed for comprehension rather than the sheer length of privacy policies. Standardized layered notices could communicate core information immediately, with more detailed explanations available on demand. Where consequential automated decisions are involved, affected persons should have a meaningful way to seek clarification and correction within the applicable legal framework.

Third, organizations need a defensible process for correction, deletion, retention and disputes. A request mechanism that is technically available

but inaccessible, unresponsive or costly is not an effective remedy. Guidance should specify operational responsibilities, preserve evidence relevant to disputes and encourage timely, reasoned decisions. Public reporting on recurring patterns of violations may support deterrence without disclosing complainants' identities.

Finally, reform should preserve a distinction between legal certainty and operational flexibility. Statutes should define core rights, duties and liability, while detailed administrative guidance can address emerging technologies. Reforms should be evaluated against demonstrable reductions in unauthorized use, improved ability to exercise rights and predictable enforcement, not simply increasing numbers of compliance forms.

7. CONCLUSION

Vietnam's 2025 personal-data legislation provides a basis for strengthening individual rights and organizational responsibility in an increasingly data-intensive economy. Its effectiveness will depend on whether institutions can demonstrate lawful purposes, practical consent where required, reliable internal controls and meaningful remedies. Risk-sensitive implementation, clear inter-agency coordination and accessible complaint procedures are more likely to produce lasting protection than an exclusively documentary compliance culture. Future research should examine actual administrative decisions, organizational practice and judicial treatment of data harms as these develop under the new legislation.

8. ACKNOWLEDGEMENTS

The author would like to thank TNU- University of Sciences for supporting us to complete this article.

REFERENCES

- [1] National Assembly of Vietnam. (2025). Law on Personal Data Protection No. 91/2025/QH15 (26 June 2025).
- [2] Government of Vietnam. (2023). Decree No. 13/2023/ND-CP on personal data protection.
- [3] National Assembly of Vietnam. (2015). Civil Code No. 91/2015/QH13.
- [4] National Assembly of Vietnam. (2018). Law on Cybersecurity No. 24/2018/QH14.

- [5] National Assembly of Vietnam. (2023). Law on Electronic Transactions No. 20/2023/QH15.
- [6] OECD. (2013). The OECD Privacy Framework. OECD Publishing.
- [7] European Parliament and Council. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union.
- [8] United Nations General Assembly. (1948). Universal Declaration of Human Rights.
- [9] Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–564.
- [10] Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.
- [11] Bennett, C. J., & Raab, C. D. (2006). The Governance of Privacy: Policy Instruments in Global Perspective (2nd ed.). MIT Press.
- [12] Kuner, C. (2013). Transborder Data Flows and Data Privacy Law. Oxford University Press.