

## Vietnam's New Privacy Law: Key Regulations and A Comparative Analysis of Existing Frameworks

Asia & Data Protection Newsletter

July 9, 2025

Authors:

[Tomonobu Murata](#)

[to.murata@nishimura.com](mailto:to.murata@nishimura.com)

[Nguyen Thi Thanh Ngoc](#)

[n.t.t.ngoc@nishimura.com](mailto:n.t.t.ngoc@nishimura.com)

[Nguyen Tuan Anh](#)

[n.t.anh@nishimura.com](mailto:n.t.anh@nishimura.com)

### Introduction

Recognizing the critical importance of digital data and the sensitivity of privacy issues in the digital age, Vietnam has taken a proactive approach to development of legislative tools and establishment of a framework to facilitate domestic and international data flow, with the goal of driving economic growth while safeguarding human safety and security. About two years after the enactment of the country's first comprehensive personal data protection regulations (Decree No. 13/2023/ND-CP dated April 17, 2023 ("**PDPD**")), on June 26, 2025, the National Assembly of Vietnam adopted the long-awaited Law on Personal Data Protection (Law No. 91/2025/QH15 ("**PDPL**")), which is a significant step toward strengthening data privacy in Vietnam, streamlining management policy and clarifying existing regulations. The landmark legislation is set to take effect on January 1, 2026, and is significantly more developed than the PDPD.


This newsletter summarizes some of the key regulations in the PDPL by comparison with the relevant requirements in the PDPD, their implications for businesses, and critical compliance considerations for relevant stakeholders.

### Key Regulations and Comparative Analysis of PDPD Regulations

#### 1. Clearer and Narrower Scope of Extraterritorial Application (Yet Still Overly Broad)

Both the PDPD and PDPL contain provisions establishing extraterritorial authority, and both laws govern offshore entities and individuals in certain circumstances. However, the PDPL limits the scope of its extraterritorial application to entities and individuals directly involved in or related to the processing of personal data of citizens of Vietnam and/or persons of Vietnamese origin who reside in Vietnam and have been granted identification certificates. Although the interpretation of "directly involved in" and "related to" remains somewhat vague, the fact that the scope of the PDPL is limited to the processing of personal data of Vietnamese citizens or persons of Vietnamese origin who reside in Vietnam is considered more positive than the similar provision in the PDPD, and is expected to narrow the scope of extraterritorial application, as well as to clarify the current extraterritorial application of the PDPD, which includes offshore entities or individuals directly involved in or related to personal data processing activities in Vietnam.

Despite this positive change, the extraterritorial application of the PDPL continues to pose challenges for offshore entities or individuals that process the personal data of Vietnamese citizens in minimal quantities or whose businesses have no other nexus with Vietnam. For example, entities that employ a single Vietnamese



individual or engage in a simple exchange of business cards with persons from Vietnam. Notwithstanding the limited scope of data processing involved, those entities are still required to fulfill various obligations under the PDPL, including but not limited to submission of a data processing impact assessment.

In addition, at this early stage it remains unclear how the authorities will enforce the PDPL against foreign organizations and individuals, especially in situations involving violations of the PDPL, as discussed in more detail later in this article.

## **2. Expanding Forms of Personal Data**

The PDPD's definition of "personal data" is limited to data in digital form. This definition has confused many stakeholders about the applicability of relevant PDPD requirements to personal data retained in tangible form (e.g., papers). The PDPL clarifies this issue by redefining "personal data" to include digital data or information in any other form that identifies or helps to identify a specific person. This means that all personal data or information is subject to the PDPL, regardless of the manner in which it is stored (e.g., in hard copy or electronically).

## **3. Unspecified Scope of Basic Personal Data and Sensitive Personal Data**

Like the PDPD, the definition of "personal data" in the PDPL includes both basic data and sensitive data. However, the PDPL does not contain lists of specific personal data that is considered "basic" or "sensitive," and tasks the government with determining and issuing detailed lists for each category. As a principal framework for the government to follow, the PDPL generally defines these types of personal data as follows:

- (i) Basic personal data: personal data reflecting common personal identity factors and background factors that are frequently used in transactions and social relationships.
- (ii) Sensitive personal data: personal data that is closely related to an individual's privacy, any violation of which would directly affect the legitimate rights and interests of both organizations and individuals.

Despite the distinction, the PDPL does not include many different requirements for processing the two types of personal data.

## **4. Introduction of Anonymization**

The PDPL introduces the concept of "anonymization," which is not contained in the PDPD. Anonymization is the process of changing or removing information to create new data from which a specific person cannot be identified in any circumstances. Anonymized data is not personal data. To ensure successful anonymization of personal data, the PDPL imposes certain responsibilities on entities or individuals performing an anonymization process, such as close monitoring or control of the process, preventing unauthorized access to, copying or appropriation of, or leaks or losses of personal data while anonymizing it, and an obligation not to de-anonymize anonymized data, unless permitted by law. The PDPL does not contain many provisions relating to this new process; however, it seems to offer a safe harbor to stakeholders if they want to prevent the PDPL from applying to certain personal data.

## 5. New Non-Consent-Based Forms of Personal Data Processing

The PDPL takes a less consent-oriented approach to personal data processing than the PDPD, and introduces some new situations in which data processing can be performed without consent.

### *Reasonable protection of legitimate interests*

The PDPL allows organizations or individuals to process personal data without the data subjects' consent in order to, among others, protect their legitimate rights and interests, or those of others, against infringement in an appropriate manner. This consent exception originates in the principle of personal data protection in the PDPL, which exists to harmonize protection of the personal data of data subjects with assuring the lawful rights and interests of others. To facilitate this non-consent-based processing, the PDPL obligates data subjects not to create difficulties or prevent data controllers, data processor-controllers, and data processors from exercising their lawful rights and obligations. This approach is expected to address concerns about data subjects abusing their rights to challenge processing activities performed for lawful purposes, for example, when an employer uses an employee's personal data to initiate a lawsuit against the employee for causes arising from the employee's noncompliance with company policies, where the employee's breach adversely impacts the legitimate business interests of the employer.

### *Transfers of personal data in certain circumstances*

The PDPL further clarifies the situations where data transfers can occur without the data subjects' consent, including (i) internal sharing of personal data within departments and divisions of an agency or organization, for processing for specified purposes, (ii) transfers of personal data in the event of business reorganizations, (iii) transfers of personal data between data controllers/data processor-controllers and data processors or third parties for processing, and (iv) transfers of personal data performed pursuant to a request from a competent authority. Although the language in these cases is not crystal clear and easy to interpret, it suggests that lawmakers are taking a more practical approach, in an attempt to resolve some common situations in which consent may serve as a bottleneck to data processing. More guidance on these situations will be provided by the government in its upcoming decree.

### *Specific responsibility for non-consent-based cases*

In recognition of the potential imbalance in, and misuse of, non-consent-based processing, the PDPL strikes a balance intended to protect the rights and interests of data subjects by requiring agencies, organizations, and individuals that process personal data on legal bases for which consent is not required to establish several monitoring regimes to oversee personal data processing that is performed without consent (e.g., creating procedures and rules for data processing, determining the responsibilities of relevant parties, implementing appropriate data protection measures, performing regular risk assessments, performing periodic inspections and assessments of legal compliance, and setting up a mechanism to receive and handle complaints and requests from relevant agencies, organizations, and individuals).

## 6. Cross-border Transfers of Personal Data

### *Redefining cross-border transfer models*

The PDPL provides for three types of cross-border data transfers, including (i) transferring data stored in Vietnam to a storage system located outside of Vietnam, (ii) transfers of personal data by an organization or individual based in Vietnam to offshore persons or entities, and (iii) use of a platform outside of Vietnam, by an onshore or offshore organization or individual, to process personal data collected in Vietnam. Unlike the PDPD, which governs only cross-border transfers of the personal data of citizens of Vietnam, the PDPL covers cross-border transfers of any personal data that originates in Vietnam.

### *Cross-border transfer impact assessments and exceptions*

Similar to the PDPD, the PDPL requires data transferors to prepare and retain a dossier of information about cross-border transfers of personal data, and to submit the dossier to the competent authority within 60 days of the first transfer of data, in the form established by the government. However, the PDPL is considered more practical and business-friendly, because it also introduces exceptions, pursuant to which the transferor is exempt from this requirement. The exceptions include, but are not limited to, an organization's storage of its employee data in cloud storage services, and other exceptions established by the government.

### *Form of impact assessment reports and composition of the dossier*


The PDPL does not establish any regulatory forms or dossiers for cross-border data transfer impact assessment reports, and assigns the government the responsibility to provide further details on these matters. Since the government has not issued regulations, there currently are no requirements for cross-border data transfer agreements between relevant stakeholders. However, this does not preclude the possibility that such an agreement may be mandated in the government's forthcoming guiding decrees or pursuant to other relevant data privacy laws. Therefore, it remains uncertain whether the Ministry of Public Security will introduce significant changes to the report forms; the answer will be determined when the relevant guidance is issued.

### *Data subject consent to cross-border transfers of personal data*

Unlike the PDPD provision on cross-border transfers of personal data, which expressly requires data subject consent as part of the cross-border transfer impact assessment dossier, the PDPL does not specify the need to obtain data subjects' consent to perform cross-border transfers of data. Therefore, it might be construed that cross-border transfers of data, which are a data processing activity, might fall within the non-consent-based cases set out in the PDPL, depending on the purposes of processing and circumstances surrounding the transfers.

### *Updates to cross-border transfer impact assessment dossiers*

Once prepared and submitted, cross-border transfer impact assessment reports must be (i) updated every six months if any changes are made to the information submitted, or (ii) updated immediately, in the event of a reorganization, termination of operation, dissolution, bankruptcy, change to the personal data protection service



provider, addition to or change of lines of business or services related to personal data processing already mentioned in the impact assessment dossier. This provision is considered more practical, and aims to reduce compliance costs incurred by businesses by comparison with the requirements in the PDPD, which obligate businesses to update and submit dossiers upon any change, without specifying a reasonable period within which they must do so.

#### *Other notable points*

Compliance with the transfer impact assessment requirement exempts data transferors from the obligation to perform a separate impact assessment for cross-border personal data transfers under data protection laws and regulations. This provision seeks to streamline administrative procedures and alleviate the compliance burden on, and associated costs incurred by, businesses.

### **7. Data Processing Impact Assessment**

The PDPL contains the same requirements for data processing impact assessments as the PDPD. Together with the impact assessment for cross-border transfers of personal data, the PDPL provides the same clear schedule for updates to the data processing impact assessment, and an exemption from risk assessments of personal data processing under data laws and regulations once this obligation is fulfilled. As with cross-border transfer impact assessment reports, it remains necessary wait for issuance of the guiding decree to determine whether or not there will be any major changes to the form of the data processing impact assessment dossier.

### **8. Limiting the Scope of Data Breaches Subject to Notification Requirements**

Under the current regulations, data controllers are required to notify competent authorities of any noncompliance with personal data protection regulations within 72 hours of discovering the noncompliance. The PDPD established an unreasonably broad scope of data breaches that were subject to this requirement, which created significant challenges to its implementation and enforcement. However, the PDPL streamlines the 72-hour notification requirement, by instructing data controllers to report only noncompliance that could (i) harm national defense and security, or social safety and order, or (ii) infringe the life, health, honor, dignity, and/or property of data subjects. While the precise data breaches that are subject to this notification requirement remain vague, this change in the PDPL demonstrates that the legislators were trying to harmonize Vietnam's new privacy rules with international regulations.

### **9. New Regulations for Personal Data Protection in Specific Activities and Business Sectors**

In addition to general personal data protection requirements that apply to all processing activities and business sectors, as discussed above, the PDPL introduces specific data protection requirements applicable to new areas and services (e.g., recruitment, employee management and deployment, health information, insurance business, finance, banking and credit information activities) or specific types of data (e.g., location data and biometric data), and improves the specific regulations in the PDPD (e.g., those relating to children's data, advertising businesses, and CCTV). Some of the notable requirements are as follows:

| Activity/business sector  | Key notes   |
|---|---|
| Personal data of children   | <ul style="list-style-type: none"> <li>• All of a child's data subject rights must be exercised by the child's legal representatives (e.g., if consent is required, the consent of the child's legal representative must be obtained.)</li> <li>• The consent of children of 7 years old or older also must be obtained before announcing or disclosing information about the child's private life or personal secrets. The PDPL reduces the cases in which data processing is subject to additional consent of children in comparison with the PDPD.</li> </ul>  |
| Personal data of a legally incapacitated person, or a person with limited cognition or behavior control | <ul style="list-style-type: none"> <li>• This is a new group of data subjects, compared with the PDPD.</li> <li>• All of the data subjects' rights of these individuals must be exercised by the data subject's legal representatives (e.g., if consent is required, the consent of the legal representative must be obtained.)</li> </ul>  |
| Recruitment   | <ul style="list-style-type: none"> <li>• Collected data must be limited to or served for recruitment purposes or other purposes agreed to by candidates.</li> <li>• Collected data of failed candidates must be deleted or destroyed, unless the failed candidates agree otherwise.</li> </ul>  |
| Employee management and deployment  | <ul style="list-style-type: none"> <li>• Employees' personal data must be deleted or destroyed upon termination of employment, unless otherwise provided by law or agreed upon by employees.</li> <li>• In the event of processing employee personal data collected using technical or technological measures, only measures in alignment with law and which ensure employee's rights and benefits can be used, with employees' full awareness of the relevant measures. It is noteworthy that express consent is not required in this context.</li> </ul>  |
| Health information and insurance business   | <ul style="list-style-type: none"> <li>• Entities and individuals doing business in the health sector must not provide personal data to third parties that are organizations engaged in the health care business, health insurance, or life insurance business, except where the data subject requests that the data be provided, in writing, or provision of the data is performed pursuant to non-consent-based cases.</li> <li>• Businesses engaged in re-insurance and reinsurance cession businesses that transfer personal data to their partners must specify that they do so in the contracts with relevant customers.</li> </ul> |
| Finance, banking and credit information activities  | <ul style="list-style-type: none"> <li>• Service providers must not use a data subject's credit information for credit scoring and rating, evaluation of credit information, or evaluation of the creditworthiness of the data subject without obtaining the data subject's prior consent.</li> <li>• Service providers must inform data subjects of leaks or losses of bank account details, financial data, and credit information</li> </ul>   |
| Advertising business  | <ul style="list-style-type: none"> <li>• Advertising businesses must provide a mechanism that enables data subjects to request that they cease receiving advertisements, and the businesses must stop sending advertisements upon receipt of such a request.</li> <li>• Advertising businesses must not outsource or agree to let other organizations or individuals perform all advertising services using personal data on their behalf.</li> <li>• Organizations and individuals using personal data to perform targeted advertising, behavioral advertising or personalized advertising must (i)</li> </ul>                           |

| Activity/business sector  | Key notes   |
|---|---|
|   | <p>collect personal data via tracking applications, information portals or websites with data subject consent, (ii) establish a mechanism that enables data subjects to refuse to share data, (iii) specify the data retention period, and (iv) delete or destroy the data when it is no longer used.</p>   |
| Social network services and online communications services                        | <ul style="list-style-type: none"> <li>• Service providers must not request the provision of images or videos of identity documents—either in full or in part—as part of account authentication processes.</li> <li>• Service providers must offer users the ability to opt out of cookie sharing, including options to disable tracking or permit activity tracking only with express consent.</li> <li>• Service providers are prohibited from unauthorized surveillance practices—such as eavesdropping, wiretapping, call recording, or accessing text messages—without the data subject's consent</li> </ul>   |
| Big data, artificial intelligence (AI), blockchain, metaverse and cloud computing | <ul style="list-style-type: none"> <li>• All systems and services that employ these technologies must integrate appropriate personal data security measures and employ appropriate authentication, identification, and access authorization methods for personal data processing.</li> <li>• AI-based personal data processing must be classified based on risk level to ensure implementation of appropriate protection measures.</li> <li>• It is prohibited to develop or use systems involving big data, AI, blockchain, metaverse, or cloud computing that utilize personal data in ways that could harm national defense or security, threaten the social order and safety, or infringe any individual's right to life, health, honor, dignity, or property.</li> </ul>   |
| Location data and biometric data  | <ul style="list-style-type: none"> <li>• In terms of location data, (i) tracking a data subject's location using RFID cards or other technologies is banned, unless the data subject agrees otherwise, or where tracking is requested by competent authorities or required by law, and (ii) mobile app platform providers must notify users of use of personal location data and take measures to prevent the collection of personal location data by unrelated parties and provide users with location tracking options.</li> <li>• Organizations and individuals that collect and process biometric data must take physical security measures to protect devices that store and transmit biometric data, restrict access to biometric data, and have monitoring systems in place to prevent and detect biometric data breaches. If biometric data processing causes harm to a data subject, the processing entities must notify the data subject of the same, as guided by the government.</li> </ul> |
| CCTV  | <ul style="list-style-type: none"> <li>• Organizations and individuals are entitled to record voice and video, and process and collect voice and video data in public places in certain situations without data subjects' consent, for example, for purposes of protecting their lawful rights and interests.</li> <li>• In these situations, organizations and individuals must notify or otherwise inform data subjects of the fact that their voices or images are being recorded, unless otherwise permitted or required by law.</li> </ul>   |

However, some of the specific requirements above are vague. Businesses might find it challenging to comply without further guidance from the government or competent authorities.



## 10. Data Protection Officers (“DPO”) and Data Protection Service Providers

The appointment of a DPO was a necessary measure to protect sensitive personal data in certain situations under the PDPD. By contrast, the PDPL requires all organizations that process personal data to appoint a DPO. However, the PDPL offers an alternative, in that it allows organizations to hire a data protection service provider instead of a DPO. Additional details about the qualifications and duties of DPOs and personal data protection service providers will be provided in the guiding documents to be issued by the government.

## 11. Severe Sanctions for Noncompliance

Designed as “trial phase in terms of personal data protection in Vietnam,” although the PDPD has been in effect for about two years, as a matter of practice, the enforcement of the PDPD — particularly with regard to penalties for violations — remains limited, due to the absence of codified penalty mechanisms. Accordingly, businesses have been enjoying relaxing enforcement. However, the enforcement status of the personal data protection regulations will change soon and businesses might be strictly monitored and inspected by authorities. The PDPL establishes frameworks for handling noncompliance with personal data protection regulations, pursuant to which severe administrative sanctions, as well as civil and criminal penalties, may apply. Notably, certain types of noncompliance may be subject to fines based on revenue levels or established fixed amounts:

| Violation  | Maximum monetary fine  |
|--|--|
| Illegal trade in personal data                             | 10 times the proceeds illegally earned due to noncompliance or VND 3 billion, whichever is higher.     |
| Noncompliance with cross-border data transfer requirements | 5% of the violator's revenue for the immediately preceding year or VND 3 billion, whichever is higher. |
| Other forms of noncompliance                               | VND 3 billion.   |

The thresholds above apply to organizations that violate the law; penalties equal to half of those set forth above will be applicable to individuals who commit the same types of noncompliance. Based on these principles and the maximum thresholds in the PDPL, the government is assigned to issue a decree detailing each noncompliance with corresponding fine.

## 12. Special Exemptions for Micro Enterprises, Small Enterprises, and Start-ups

The PDPL acknowledges the limitations of certain types of businesses, in terms of compliance with these strict new requirements, by exempting micro-enterprises from compliance with the requirements relating to data processing impact assessments (including updates thereto) and appointment of a DPO or designation of a personal data protection service provider. Small enterprises and start-ups receive the same exemptions, but only for a limited term of five years, commencing on January 1, 2026. However, this favorable treatment does not apply to those businesses if they qualify as data processing service providers, if they directly process sensitive data, or if they process the personal data of a large number of data subjects. Detailed guidance will



be issued by the government. Since the PDPL does not provide detailed definitions of these types of enterprises, it is likely that the same determination criteria will apply as exist with regard to assistance for small and medium sized enterprises in other laws and regulations.

### 13. The Status of the PDPD After Enactment of the PDPL and Transition Provisions

#### *Status of the PDPD*

No provisions of the PDPL expressly invalidate the PDPD. However, by law, when legal documents contain different regulations governing the same matters, the document with higher legal validity shall prevail. Therefore, the PDPD will cease to apply on January 1, 2026. Moreover, since the government is tasked with detailing many issues within the general framework of the PDPL, it is likely that upcoming decrees giving guidance on the PDPL also will terminate the effectiveness of the PDPD.

#### *Transition Provisions*


Despite the potential termination of the PDPD, any personal data processing consented to or in line with agreements with data subjects entered into under the PDPD before January 1, 2026 shall continue to be effective, without the need to obtain consent again or enter into new agreements after January 1, 2026. Furthermore, businesses can continue to use and rely on any impact assessment dossiers created in line with the PDPD and received by the competent authorities before January 1, 2026 without the need to create new impact assessment dossiers under the PDPL. However, any changes to those dossiers made after January 1, 2026 must comply with the update requirements set forth in the PDPL.

## Conclusion

Overall, the regulations in the PDPL appear to be more practical and reasonable than those in the PDPD. However, many regulations are general and vague, and require further guidance from the government to ensure smooth implementation and enforcement in practice. Therefore, it is necessary to monitor the development of these government decrees and guidelines closely to ensure understanding of the legislative requirements and better prepare for compliance with the new law.

That said, since many of the provisions are similar to those in the PDPD, businesses that have taken efforts to comply with the PDPD should perform a comprehensive gap analysis and alter or improve their current personal data protection practices, while those that have not taken action to comply with PDPD regulations are encouraged to take appropriate action immediately and consider suitable roadmaps and plans to comply with the PDPL requirements within the next six months, to avoid serious consequences or sanctions.

Our firm is committed to supporting businesses through this dynamic period, and to providing insight into and tailored compliance strategies for the emerging personal data protection framework. Please feel free to reach out to us if you have any questions or would like assistance.



In order to respond to the business needs of our clients, we publish newsletters on a variety of timely topics. Back numbers can be found [here](#). If you would like to subscribe to the N&A Newsletter, please fill out [the N&A Newsletter subscription form](#).

This newsletter is the product of its authors and does not reflect the views or opinion of Nishimura & Asahi. In addition, this newsletter is not intended to create an attorney-client relationship or to be legal advice and should not be considered to be a substitute for legal advice. Individual legal and factual circumstances should be taken into consideration in consultation with professional counsel prior to taking any action related to the subject matter of this newsletter.

**Public Relations Section, Nishimura & Asahi** [newsletter@nishimura.com](mailto:newsletter@nishimura.com)