PANORAMIC

DATA PROTECTION & PRIVACY

Vietnam

LEXOLOGY

Data Protection & Privacy

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Generated on: December 17, 2025

Contents

Data Protection & Privacy

SHARING AND CROSS-BORDER TRANSFERS OF PI

RIGHTS OF INDIVIDUALS

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

SPECIFIC DATA PROCESSING

UPDATE AND TRENDS

Contributors

Vietnam

Tilleke & Gibbins

Waewpen Piemwichai	waewpen.p@tilleke.com
Anh Ha Mai Ho	haanh.h@tilleke.com
Quang Minh Vu	quang.v@tilleke.com

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Vietnam's regulations on personal data protection and privacy are dispersed across multiple legal instruments; however, the issuance of Decree No. 13/2023/ND-CP on Personal Data Protection (PDPD) on 17 April 2023 marked the country's first comprehensive legislation solely dedicated to personal data protection. This decree was a significant milestone, laying the groundwork for aligning Vietnam's data protection regime with the GDPR requirements. Building on this foundation, Law No. 91/2025/QH15 on Personal Data Protection (PDPL) was passed by the National Assembly on 26 June 2025 and will take effect on 1 January 2026. While many provisions remain consistent with the PDPD, the PDPL, with extraterritorial effect, introduces new concepts, exemptions and obligations beyond those in the PDPD.

In addition, the country also has Law No. 60/2024/QH15 on Data (Data Law), passed by the National Assembly on 30 November 2024 and effective on 1 July 2025, which governs both personal data and non-personal data. The Data Law also sets out additional obligations for data processing activities, especially with respect to core data and important data.

Law stated - 3 December 2025

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

Currently, the Department of Cybersecurity and Hi-tech Crime Prevention (A05) under the Ministry of Public Security (MPS) serves as the principal authority overseeing the enforcement of Vietnam's personal data protection laws.

The MPS is granted the power to conduct inspection of cross-border data transfer activities of enterprises and individuals once per year, except for cases of detecting violations of personal data protection regulations or cases of disclosure or loss of personal data of Vietnamese citizens. The MPS is also tasked generally to inspect, examine and settle complaints and denunciations, and handle violations of regulations on personal data protection in accordance with the law, which may broadly grant investigation powers to fulfil their tasks.

Law stated - 3 December 2025

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The PDPD provides general regulations on international cooperation on personal data protection, including, among others:

- the development of an international cooperation mechanism to facilitate the effective enforcement of the laws on personal data protection;
- participation in mutual legal assistance in personal data protection of other countries, including notification, requests for complaint, investigation assistance and information exchange, with appropriate measures to protect personal data; and
- organisation of bilateral and multilateral meetings to exchange experience on law-making and practices on personal data protection. This shows the cooperation of Vietnam's regulators with other data protection authorities.

Law stated - 3 December 2025

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Both the PDPD and the PDPL set out that agencies, organisations and individuals that violate regulations on personal data protection, depending on the severity, may be subject to administrative sanctions or criminal penalties as regulated by law. In addition, where harm is caused, violators may also be liable for compensation in accordance with the law.

The PDPL further stipulates the framework for administrative sanctions, and sets out the following maximum administrative fines applicable to an organisation:

- for violations related to personal data trading: up to 10 times the revenue gained from the act of unlawful personal data trading;
- for violations related to cross-border personal data transfers: up to 5 per cent of the violator's revenue in the preceding fiscal year; and
- for other violations in the field of personal data protection: up to 3 billion dong (approximately US$115,387).

The method to calculate revenue arising from violation of personal data protection regulations will be further prescribed by the government under the PDPL's forthcoming guiding or implementing decree.

Law stated - 3 December 2025

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

PI owners have the right to lodge complaints and denunciations and initiate lawsuits in accordance with the law. In addition, according to Law on Administrative Proceedings, individuals may sue over administrative decisions or administrative acts if they disagree with the decisions or acts, or if they have filed complaints with competent authorities, but the complaints were not resolved within the time limit prescribed by law, or the complaints were resolved but they disagree with the resolution.

Law stated - 3 December 2025

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Vietnam's personal data protection framework, comprising the Personal Data Protection Decree (PDPD) and the Personal Data Protection Law (PDPL), applies broadly to all sectors and types of organisations, both public and private. The PDPD and the PDPL provide many clear exemptions for the operations of regulators and for national security-related purposes.

In addition, Vietnam has other sector-specific legislation (such as regulations on banking, e-commerce and consumer protection) that may add specific deviations to the general framework.

Law stated - 3 December 2025

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Vietnam's data protection law partially covers issues related to the interception of communications, electronic marketing, and the monitoring and surveillance of individuals. These matters are not only regulated under the PDPD and PDPL, but are also governed by other legislation, notably:

- Criminal Code No. 100/2015/QH13, passed by the National Assembly on 27 November 2015; as amended from time to time (Criminal Code);
- Law No. 24/2018/QH14 on Cybersecurity, passed by the National Assembly on 12 June 2018 (Cybersecurity Law); and
- Decree No. 91/2020/ND-CP of the Government dated 14 August 2020 on fighting spam messages, spam emails and spam calls (Decree 91).

Law stated - 3 December 2025

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

In addition to the general data protection framework established under the PDPD, the PDPL introduces specific provisions addressing the processing of personal data in several areas such as employee monitoring, health records, the use of social media and credit information. Vietnam has other sector-specific legislation that supplements these provisions and governs data protection in these areas, such as regulations on banking, e-commerce and consumer protection.

Law stated - 3 December 2025

PI formats

What categories and types of PI are covered by the law?

Under the PDPD, 'personal data' is defined to include basic personal data and sensitive personal data (details of which are regulated in the PDPD as well), and is protected only when expressed in electronic form, such as symbols, letters, numbers, images, sounds or their equivalents. The PDPL expands the scope to cover personal data presented in digital form as well as other formats. However, the PDPL does not provide exhaustive lists of basic personal data and sensitive personal data. This information will be detailed in a guiding decree.

Law stated - 3 December 2025

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

Both the PDPD and the PDPL have extraterritorial effect. Their scopes are not limited to personal data controllers and processors physically established or operating in Vietnam, but also apply to foreign agencies, organisations, and individuals that are directly involved in or related to the processing of personal data of Vietnamese data subjects. Therefore, even if a data controller, processor or controller-processor has no physical presence or business operations in Vietnam, it will still be subject to the requirements of the PDPD and PDPL if it processes personal data of Vietnamese citizens.

Law stated - 3 December 2025

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

In Vietnam, all processing or use of PI is generally covered under the PDPD and the PDPL. These regulations apply to all acts that impact personal data, including collecting, analysing, disclosing, transferring, deleting, etc.

Vietnamese law distinguishes between entities that control or own personal data and those that process data on behalf of others and their obligations. Under the PDPL, 'personal data controller' means an agency, organisation or individual that decides on the purposes and means of processing personal data while 'personal data processor' means an agency, organisation or individual that processes personal data at the request of the personal data controller or the controller-processor through a contract.

Vietnam also has the concept of data controller-processor, which is the agency, organisation, or individual that decides on the purposes and means and also directly processes personal data. In addition, related 'third parties' are defined to be organisations and individuals other than personal data subjects, personal data controllers, personal data controller-processors, and personal data processors engaging in the processing of personal data in accordance with the law. Each party will have different duties as regulated by law.

Law stated - 3 December 2025

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Vietnam adopts a consent-centric approach. This means that regarding lawfulness, prior consent given by the data subject is the primary legal basis for personal data processing activities, except for certain exemptions as provided by law.

Particularly, under the Personal Data Protection Decree (PDPD), the processing of personal data without consent is permissible in the following circumstances:

- in urgent cases where it is necessary to immediately process relevant personal data to protect the life or health of the data subject or others;
- where the public disclosure of personal data is in accordance with the law;
- when the processing of data is done by competent state agencies in the event of a state of emergency on national defence and security, social order and safety, major disaster, or dangerous epidemic; or when there is a risk that threatens security and national defence but not to the extent where it is necessary to declare a state of emergency; or to prevent and combat riots, terrorism, crimes and violations of the law;
- to fulfil the contractual obligations of the data subject with relevant agencies, organisations and individuals as prescribed by law;
- for competent agencies and organisations to carry out audio and/or video recording and process personal data obtained from audio or video recording activities in public places for the purpose of protecting national security, social order and safety, or the legitimate rights and interests of organisations and individuals; or

- to serve the activities of state agencies as prescribed by sector-specific laws.

Under the Personal Data Protection Law (PDPL), the consent-exemption cases largely remain the same, with some new additions and clarification, which make the PDPL more enterprise-friendly.

Law stated - 3 December 2025

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

Vietnamese law regulates that personal data includes basic personal data and sensitive personal data. Sensitive personal data is subject to more stringent rules for its processing.

Under the PDPD, 'sensitive personal data' is defined as personal data associated with individual privacy which, if violated, will directly affect a person's legitimate rights and interests. In particular, the PDPD specifies sensitive personal data to include, among other things, political and religious views, health status and private life information as recorded in medical records (except for blood type), racial or ethnic origin, genetic characteristics, biometric characteristics, sexual orientation, criminal records, customer information of credit institutions, foreign bank branches or payment intermediary service providers, or location data identified via location services. When obtaining consent to process sensitive personal data, organisations must clearly inform the data subject that the data falls within a sensitive category. In addition to applying all protection measures for basic personal data, organisations processing sensitive personal data are also required to: (1) establish a dedicated data protection department; (2) assign a specific data protection officer; and (3) notify the A05 of the appointed department and responsible personnel.

While the PDPL retains the concept of sensitive personal data, it does not specify the exact types of data that fall within this category or set out specific processing requirements. Instead, the categories of sensitive personal data will be determined by a list to be issued by the government later.

Law stated - 3 December 2025

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The Personal Data Protection Decree (PDPD) stipulates that data subjects must be notified of the processing before their personal data is processed. The PDPD further regulates: (1) conditions to obtain the consent, which include information that the data subject must be provided with before collecting the consent; and (2) the data processing notification, which includes information that the data subject must be provided with before the personal data

processing is conducted. In brief, to satisfy the two requirements, the data subject must be provided with:

- purposes of processing;
- type of personal data used in relation to the processing purposes;
- methods of processing personal data;
- information on other organisations and individuals related to the processing purposes above;
- consequences and undesirable damages that are likely to occur;
- start time and end time of data processing;
- rights and obligations of the data subject; and
- indication if any of the data to be processed falls under the category of sensitive personal data.

In addition, if there is a cross-border personal data transfer, the data subject needs to be notified about such transfer as well.

The requirements above, however, are more relaxed under the Personal Data Protection Law (PDPL).

Law stated - 3 December 2025

Exemptions from transparency obligations

When is notice not required?

Under the PDPD, personal data controllers and controller-processors are generally required to notify data subjects before processing their personal data. However, this obligation does not apply in the following cases:

- the data subject is already aware of and has voluntarily given consent to all required information prior to the collection of their personal data; or
- the personal data is processed by competent state authorities for the performance of their duties as provided by law.

Although the PDPD exempts consent in certain circumstances, it does not explicitly address whether notification obligations are also waived in those cases. Nonetheless, it is commonly interpreted that notification may also be exempted.

Law stated - 3 December 2025

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

While the PDPD and the PDPL do not expressly impose specific standards, they do set out general principles related to data quality, currency and accuracy:

- The PDPD requires that personal data be updated and supplemented as appropriate for the intended processing purposes. Data subjects also have a duty to provide complete and accurate personal data when consenting to its processing.
- Similarly, the PDPL emphasises the principle that personal data must be accurate and subject to correction, updating or supplementation when necessary. It also requires data subjects to provide their personal data in a complete and accurate manner in accordance with legal provisions, contracts, or when giving consent to data processing.

Law stated - 3 December 2025

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

The PDPD and PDPL do not explicitly limit the types or amount of personal data that may be collected. However, both incorporate the principle of data minimisation. Specifically, the PDPD requires that personal data be collected in a manner that is appropriate and limited to the scope and purpose of processing, while the PDPL mandates that personal data be collected and processed strictly within a specific and clearly defined scope and purpose, in compliance with legal regulations.

Law stated - 3 December 2025

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

The PDPD and PDPL impose a storage limitation principle and regulate cases of data deletion. For examples, the PDPD requires that personal data be retained only for a period consistent with the processing purpose, while the PDPL states that data must be stored only for the period necessary for processing purposes, unless otherwise provided by law.

Law stated - 3 December 2025

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

The PDPD and the PDPL both acknowledge the purpose limitation principle. Specifically, the PDPD requires that personal data must be processed for specific purposes that have been declared to the data subjects. The PDPL further clarifies that personal data may only be collected and processed for clear, specific, and lawful purposes.

In particular, the PDPD obliges personal data controllers and controller-processors to provide mandatory information to data subjects to obtain valid consent (unless consent-exemption cases are applied). Accordingly, it is understood that any subsequent changes to agreed content (eg, purposes) must also be notified and subject to additional consent (unless consent-exemption cases are applied). This approach is upheld under the PDPL as well.

Law stated - 3 December 2025

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

Neither the PDPD nor PDPL explicitly restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling.

Law stated - 3 December 2025

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

One of the principles the Personal Data Protection Decree (PDPD) set out for personal data protection is that personal data is subject to protection and security measures during processing, including protection against acts in violation of personal data protection regulations and the prevention of loss, destruction or damage caused by incidents or use of technical measures. The PDPD also emphasises that personal data protection be adopted from the beginning of and throughout the processing of personal data.

All entities involved in processing personal data are required to implement both managerial and technical measures. However, the PDPD does not detail standard for such measures, which allow flexibility for enterprises. Moreover, these entities must formulate and enforce internal personal data protection policies, conduct cybersecurity inspection as required, etc. The processing of sensitive personal data additionally requires the establishment of an internal data protection department, the appointment of a data protection officer, and the notification of their details to the regulator; and informing data subjects when their sensitive personal data is being processed, unless an exemption applies.

Similarly, the Personal Data Protection Law (PDPL) requires the coordinated and effective implementation of institutional, technical and human-based measures appropriate for the protection of personal data. However, it does not provide specific guidance on what those measures should entail.

Law stated - 3 December 2025

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Vietnamese laws impose mandatory data breach notification requirements under several legal instruments, including the PDPD and PDPL and other sector-specific regulations, such as the Cybersecurity Law, e-commerce regulations, etc. The requirements and triggering conditions will vary depending on the specific legislation applied to the case.

Under the PDPD, if a breach of personal data protection regulations occurs, the personal data controller or controller-processor must notify the data protection authority within 72 hours of the time the incident occurs. Data processors, in contrast, are required to promptly inform the data controller upon discovering such a breach. This notification obligation is preserved under the PDPL, although the timeline is revised to 72 hours from the time of detection. Under the PDPL, while notification is mandatory in high-risk cases, voluntary reporting is encouraged to demonstrate accountability and mitigate risks.

There are also requirements to notify affected data subjects if the data breach is relevant to biometric data or personal data processed by financial institutions, or if the data breach causes or is likely to cause significant loss to the legitimate rights and interests of affected data subjects.

Law stated - 3 December 2025

INTERNAL CONTROLS

Accountability
Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

While the Personal Data Protection Decree (PDPD) explicitly affirms the accountability principle, it does not prescribe specific internal control measures. This provides companies with the flexibility to adopt and implement controls that align with their operational capacity and needs.

Law stated - 3 December 2025

Data protection officer
Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

Under the PDPD, appointing a Data Protection Officer (DPO) is only mandatory for organisations that process sensitive personal data. However, the PDPD does not define the specific responsibilities or required qualifications for the role.

In contrast, the Personal Data Protection Law (PDPL) requires all organisations to appoint a DPO, regardless of the type of personal data they handle. The detailed requirements and responsibilities of the DPO will be further provided by the government.

Law stated - 3 December 2025

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Under both the PDPD and the PDPL, personal data controllers, controller-processors and processors are required to maintain internal records relating to their personal data processing activities under the form of personal data processing impact assessment and cross-border personal data transfer impact assessment (if any).

Law stated - 3 December 2025

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Under the PDPD, personal data controllers, controller-processors, and processors processing personal data in Vietnam are all required to carry out a personal data processing impact assessment (DPIA). The parties must use the mandatory forms issued by the regulator to conduct the assessment, which cover, among other contents:

- contact information of the personal data controller, controller-processor, or processor;
- contact information of the individual or organisation designated to protect personal data of the personal data controller, controller-processor, or processor;
- the purposes of processing;
- the categories of personal data to be processed;
- information on any receiving parties, including those located outside of Vietnam;
- any instances of cross-border data transfers;
- the duration of processing and any expected timeframe for deletion or destruction of the data (if applicable);
- a description of the data protection measures in place; and
- an assessment of the potential impact of processing activities, including possible consequences or harms, and the measures to mitigate or eliminate them.

In addition, where personal data of Vietnamese citizens is transferred outside of Vietnam, a cross-border personal data transfer impact assessment ("TIA") must also be conducted. This requirement applies to all entities that are taking the role of transferors/data exporters, including personal data controllers, controller-processors, processors, or other third parties acting as data senders. The TIA must include:

- contact information for both the sender and recipients;
- details of the organisation or individual under the sender responsible involved in sending and receiving a Vietnamese citizen's personal data;
- description and explanation about objectives of the processing of a Vietnamese citizen's personal data after the personal data is transferred abroad;
- description and clarification of type of personal data to be transferred abroad;
- description and explanation about the observance of regulations on protection of personal data, detailed measures for protecting personal data;
- assessment of impact of personal data processing, undesirable consequences and damage that may occur, and measures for reducing or removing such consequences and damage;
- the data subject's consent, given with full awareness of the mechanism for feedback and complaints in the event of incidents or arising requests; and
- a formal document outlining the respective obligations and responsibilities of the sender and recipient in relation to the cross-border data processing.

Under the PDPL, the DPIA and TIA requirements are maintained. The specific components of both the DPIA and TIA dossiers are expected to be clarified in upcoming guiding documents.

Law stated - 3 December 2025

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

There is no specific obligation in relation to how personal data processing systems must be designed under current personal data protection laws.

Law stated - 3 December 2025

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There is no general requirement for data controllers, processors or controller-processors to register their data processing activities with the supervisory authority.

Law stated - 3 December 2025

Other transparency duties

Are there any other public transparency duties?

There is currently no general requirement under Vietnamese law to make public statements about the nature of the processing activities. The transparency obligations under the Personal Data Protection Decree and Personal Data Protection Law are limited to notifying the data subjects directly, not the public.

Law stated - 3 December 2025

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The Personal Data Protection Decree (PDPD) and Personal Data Protection Law (PDPL) allow the sharing of personal data with outsourced service providers (processors), provided there is a valid legal basis, such as the data subject's consent or a lawful exemption, and a contract is established between the controller and the processor. However, the laws do not specify the detailed content or mandatory clauses of such contracts between the parties. The controller, of note, remains responsible to the data subject for damages caused by the processing of personal data.

Law stated - 3 December 2025

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Under Vietnam's personal data protection laws, the sharing of personal data with third parties that are not processors or service providers must have a valid legal basis, typically the data subject's consent unless an exemption applies. Personal data trading is strictly prohibited, unless otherwise provided by law.

With respect to marketing and advertising activities, the PDPD requires marketing and advertising service providers to only use personal data of consented targeted audiences collected through their business activities to provide marketing and advertising services. The PDPL makes it clearer that advertising service providers can use targeted audiences' personal data transferred by the personal data controller and/or the personal data controller-processor as agreed upon or collected through their business activities to conduct the advertising services.

These requirements apply specifically to marketing and advertising service providers acting on behalf of other parties. They do not apply to organisations that promote their own products or services.

Law stated - 3 December 2025

Cross-border transfer
Is the transfer of PI outside the jurisdiction restricted?

Cross-border transfers of personal data are generally allowed, provided that the data subjects have given their consent and the transferor prepares a cross-border transfer impact assessment within 60 days of the commencement of data processing, and fulfils other obligations.

Restrictions may apply if the data is classified under certain special categories, such as state secrets, or is considered 'core data' under the Data Law.

Law stated - 3 December 2025

Further transfer
If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Yes, the requirement applies equally.

Law stated - 3 December 2025

Localisation
Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

Under the personal data protection framework, there is no data localisation requirement.

However, pursuant to the Cybersecurity Law and its guidance under Decree No. 53/2022/ND-CP, domestic companies providing telecommunications services, internet services, and value-added services in cyberspace in Vietnam that carry out activities of collecting, exploiting/using, or analysing and processing certain types of data (regulated data) in Vietnam must store such data in Vietnam for a specified period to be stipulated by the government. The regulated data is as follows:

- data on personal information of service users in Vietnam;
- data created by service users in Vietnam: account names, service use time, information on credit cards, email addresses, IP addresses of the last login or logout session, and registered phone numbers in association with accounts or data; and
- data on relationships of service users in Vietnam: friends and groups such users have connected or interacted with.

This data localisation requirement also applies to foreign companies if the following conditions are all met:

- the company is engaged in any of the following 10 services:

- telecommunications;
- data storage and sharing in cyberspace;
- supply of national or international domains to service users in Vietnam;
- e-commerce;
- online payment;
- intermediary payment;
- transport connection via cyberspace;
- social networking and social media;
- online electronic games; and
- providing, managing or operating other information in cyberspace in the form of messages, phone calls, video calls, email or online chats ('regulated services');

- the MPS notifies the foreign company that its services have been used for committing violations under Vietnamese laws;
- the foreign company fails to comply with the authority's request or works against measures implemented by the MPS; and
- the MPS sends the foreign company a request to store the regulated data and/or establish a branch or representative office in Vietnam.

Law stated - 3 December 2025

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Under the Personal Data Protection Decree (PDPD), data subjects are entitled to access their personal data held by personal data controllers for the purpose of reviewing, correcting and requesting corrections, unless otherwise stipulated by law. While the PDPD does not detail the procedure for exercising this right, it does require that any request for correction of personal data must be addressed as soon as possible or in accordance with relevant sector-specific laws. If the correction cannot be made, the data subject must be notified within 72 hours of the time the request is received. This right may be limited in cases where the processing of personal data is lawfully conducted without the data subject's consent.

Similarly, the Personal Data Protection Law (PDPL) upholds the data subject's right to access their personal data for viewing, modification, and requesting modifications. However, it has yet to provide detailed guidance on how this right should be exercised. In exercising their rights, data subjects must comply with the principle that such actions must aim to protect their own legitimate rights and interests, and must not obstruct or interfere with the lawful rights and obligations of personal data controllers, controller-processors and processors. They must also refrain from infringing upon the lawful rights and interests of the state,

agencies, organisations or individuals. As with the PDPD, this right may also be restricted where personal data is processed without the data subject's consent in accordance with the law.

Law stated - 3 December 2025

Other rights

Do individuals have other substantive rights?

The PDPD recognises 11 rights of data subjects, including the rights to: be informed; give consent; access data for the purpose of reviewing, correcting and requesting corrections; withdraw consent; delete data; restrict data processing; request data provision; object to data processing; file complaints, denunciations, and lawsuits; claim damages; and self-defence. Generally, all these rights are retained under the PDPL.

Law stated - 3 December 2025

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Under both the PDPD and PDPL, individuals are entitled to claim compensation as prescribed by law when there are violations against regulations on protection of their personal data. Although neither the PDPD nor the PDPL explicitly clarifies whether actual damage is required or if emotional harm alone is sufficient, the Civil Code provides broader guidance. Specifically, the Civil Code recognises that compensation is not limited to financial losses and may include non-material damages, such as mental suffering caused by harm to honour, dignity or reputation.

Law stated - 3 December 2025

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The rights of data subjects under the PDPD and PDPL may be enforced through both the judicial system and the competent supervisory authorities.

Law stated - 3 December 2025

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

Under the Personal Data Protection Decree, micro, small and medium-sized enterprises, as well as startups, may opt out of the requirement to appoint a data protection officer or establish a data protection department for the first two years following their establishment, unless they are directly engaged in the business of personal data processing.

Small enterprises and startups have a five-year grace period from the effective date of the Personal Data Protection Law to comply with regulations on preparing and updating impact assessment dossiers and designating departments and personnel to protect personal data. Business households and micro-enterprises are exempted from these regulations. The exemptions and grace period, however, do not apply in cases where a large amount of personal data is processed, in the provision of data processing services, or in cases where sensitive personal data is directly processed.

Law stated - 3 December 2025

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

Although Vietnamese laws do not expressly regulate the use of cookies or similar tracking technologies, data collected through such tools may be regarded as personal data if it is linked to, or can help identify, a specific individual. In such cases, the use of cookies is subject to the general data processing requirements set out under the Personal Data Protection (PDPD) and Personal Data Protection Law (PDPL).

Law stated - 3 December 2025

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

The PDPD and the PDPL regulate lawful basis for the processing of personal data in advertising or marketing activities only; they do not specifically regulate methods of marketing activities (eg, email, fax, telephone or other electronic channels). Instead, these issues will be separately governed in advertising-related regulations.

To be specific, the PDPD requires marketing and advertising service providers to only use personal data of consented targeted audiences collected through their business activities to provide marketing and advertising services. The PDPL makes it clearer that advertising service providers can use targeted audiences' personal data transferred by the personal data controller and/or the personal data controller-processor as agreed upon or collected through their business activities to conduct the advertising services.

Law stated - 3 December 2025

Targeted advertising

Are there any rules on targeted online advertising?

The PDPD is silent on targeted online advertising. However, in addition to other general requirements for advertising activities, the PDPL stipulates that organisations and individuals using personal data for behaviour-based, targeted or personalised advertising must comply with the following requirements:

- personal data may only be collected through tracking websites, e-portals or applications with the data subject's consent; and
- a mechanism must be in place to allow the data subject to decline the sharing of their data, along with methods to define data retention periods and to delete or destroy the data once it is no longer needed.

Law stated - 3 December 2025

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

The processing of sensitive personal data is generally governed by the same fundamental principles that apply to all personal data under the PDPD and PDPL. However, due to the nature of sensitive data, additional requirements may apply to ensure its enhanced protection.

Law stated - 3 December 2025

Profiling

Are there any rules regarding individual profiling?

Currently, there are no specific requirements or restrictions that apply to profiling in Vietnam.

Law stated - 3 December 2025

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

The PDPD does not specifically address cloud computing services. In contrast, the PDPL expressly requires that personal data in a cloud computing environment be processed only for proper purposes and limited to the necessary scope, while safeguarding the lawful rights and interests of the data subject.

Such processing must comply with the PDPL and other applicable laws, and must also align with Vietnam's ethical standards and cultural traditions. Cloud-based systems and

services must incorporate suitable measures to secure personal data, including proper authentication, identification and access control mechanisms. It is prohibited to use or develop cloud computing systems involving personal data in ways that threaten national defence, security, social order, or safety, or that infringe upon the life, health, honour, dignity or property of others. Additional guidance on this issue will be provided by the government.

Law stated - 3 December 2025

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The adoption of the Personal Data Protection Law (PDPL) was a key development in Vietnam's personal data protection. The PDPL introduces a range of sector-specific provisions addressing emerging topics such as AI, cloud computing, blockchain, etc. The government is now, as at late 2025, actively preparing detailed implementing and sanctioning decrees, with the aim of issuing them within the year to ensure effective enforcement.

Law stated - 3 December 2025