PANORAMIC

DATA PROTECTION & PRIVACY

Vietnam

LEXOLOGY

Data Protection & Privacy

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Generated on: July 13, 2026

Contents

Data Protection & Privacy

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 legislative framework for the protection of personal data is principally governed by Law No. 91/2025/QH15 on Personal Data Protection (PDPL), adopted by the National Assembly on 26 June 2025 and effective from 1 January 2026. The PDPL is Vietnam's first dedicated law-level instrument comprehensively regulating the protection and processing of personal data. It establishes a legal framework applicable to both domestic and foreign entities, including provisions with extraterritorial effect.

To implement the PDPL, the government subsequently issued Decree No. 356/2025/ND-CP dated 31 December 2025 (Decree 356), effective from 1 January 2026, providing detailed guidance on certain articles of the law. Together, the PDPL and Decree 356 form the core legal framework for personal data protection in Vietnam.

While the PDPL was developed in light of Vietnam's domestic regulatory context, several of its key principles are broadly inspired by the EU's General Data Protection Regulation (GDPR). This is reflected in concepts such as lawful bases for processing, data subject rights, purpose limitation, and data minimisation, among others.

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 - 1 June 2026

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 annual inspections of cross-border data transfer activities of enterprises and individuals, as well as ad hoc inspections upon detection of violations of personal data protection regulations or leaks or loss of personal data.

The MPS is also tasked generally to receive notifications on 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 - 1 June 2026

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

- compliance with the law of Vietnam, international treaties to which Vietnam is a signatory, and international agreements on personal data protection based on equality, mutual benefit, and respect for independence, sovereignty, and territorial integrity;
- 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; and
- exchanging experience on law-making and practices on personal data protection.

Law stated - 1 June 2026

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?

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.

Detailed provisions on administrative sanctions are expected to be set out in a forthcoming decree on administrative penalties in the field of cybersecurity and personal data protection, which is being drafted by the MPS.

Law stated - 1 June 2026

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 the 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 - 1 June 2026

SCOPE

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?

Vietnam's Personal Data Protection Law (PDPL) covers essentially all processing or use of PI, including collection, analysis, aggregation, encryption, decryption, modification, deletion, destruction, de-identification, provision, publication, transfer, and any other activity affecting personal data. Processing must be conducted for specific, clear, and lawful purposes.

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 an 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 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.

Data controller responsibilities include, among others:

- specifying responsibilities, rights, and obligations of each party in agreements or contracts related to personal data processing;
- determining the purpose and means of processing in documentation and agreements with data subjects (including obtaining the data subject's consent);
- implementing appropriate management and technical measures to protect personal data;
- notifying relevant entities of data protection violations;
- selecting appropriate data processors;
- ensuring data subject rights;

- bearing responsibility to data subjects for damage caused by data processing; and
- cooperating with the Ministry of Public Security and competent authorities in data protection enforcement.

Data processor responsibilities are more circumscribed and include:

- receiving personal data only after an agreement or contract on data processing has been established with the controller or controller-processor;
- processing data strictly in accordance with the agreement or contract with the controller or controller-processor;
- fully implementing personal data protection measures;
- bearing responsibility to the controller or controller-processor (not directly to the data subject) for damages caused by processing; and
- cooperating with the Ministry of Public Security and competent authorities.

Data controller-processor responsibilities are the broadest: this hybrid entity must fulfil all duties of both the controller and the processor.

Law stated - 1 June 2026

Exempt sectors and institutions

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

The PDPL applies broadly to all sectors and types of organisations, both public and private. The PDPL provides 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 data protection framework.

Law stated - 1 June 2026

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 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 (2018 Cybersecurity Law);

- Law No. 116/2025/QH15 on Cybersecurity, passed by the National Assembly on 10 December 2025; effective from 1 July 2026 to replace the 2018 Cybersecurity Law (2025 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 - 1 June 2026

Other laws

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

The PDPL includes provisions addressing the processing of personal data in specific areas such as recruitment, management, and use of labour; health records; finance, banking, and credit information activities; advertising; and the use of social media, big data, AI, blockchain, virtual space, and cloud computing. Other sector-specific legislation supplements these provisions and governs data protection in these particular areas, such as regulations on banking, e-commerce and consumer protection.

Law stated - 1 June 2026

PI formats

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

Under the PDPL, 'personal data' is defined as digital data or information in other forms that identifies or assists in the identification of a specific individual. The law divides personal data into two categories:

- basic personal data, covering common identifiers such as name, date of birth, gender, address, national ID numbers, phone numbers, marital status, family relationships, and digital account information; and
- sensitive personal data, which includes racial/ethnic origin, political and religious views, private life information, health data, biometrics, genetics, sexual life/orientation, criminal records, location data, login credentials, bank account and financial transaction data, online behavioural tracking data, and any other data required by law to be kept confidential.

De-identified data is explicitly excluded from the definition of personal data. Location data and biometric data receive additional heightened protections, including specific consent requirements and a dedicated 72-hour breach notification regime.

Law stated - 1 June 2026

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?

The PDPL has extraterritorial effect. Its scope is not limited to personal data controllers and processors physically established or operating in Vietnam, but also applies to foreign agencies, organisations, and individuals that are directly involved in or related to the processing of personal data of Vietnamese citizens and people of Vietnamese origin (who have not yet determined their nationality, are residing in Vietnam, and hold a Vietnamese ID card). Therefore, even if a data controller, data processor or data controller-processor has no physical presence or business operations in Vietnam, it will still be subject to the requirements of the PDPL if it processes personal data of these categories of data subjects.

Law stated - 1 June 2026

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 Law (PDPL), the processing of personal data without consent is permissible in the following circumstances:

- to protect the life, health, honour, dignity, and legitimate rights and benefits of the personal data subject or others in urgent cases; or to protect one's own or others' legitimate rights or benefits, or benefits of the state or agencies/organisations in a necessary manner against infringement of such rights or benefits;
- to address emergencies or threats to national security that have yet to escalate to the level of a declared emergency; to prevent and combat riots, terrorism, crimes, and law violations;
- to serve the operations of state agencies and state management according to the law;
- to carry out the agreement between the personal data subject and relevant agencies, organisations and individuals as prescribed by law;
- to carry out audio and/or video recording and process personal data obtained from audio or video recording activities in public places for the implementation of tasks concerning national defence, national security protection, assurance of social order and safety, and protection of the legitimate rights and interests of agencies, organisations and individuals; or where audio, images, and identification data collected at public events do not harm a personal data subject's honour, dignity, or reputation; or

- in other cases according to the law.

However, even when consent (and the associated notice) is not required, organisations must still establish monitoring mechanisms including setting up processing rules and defining responsibilities, implementing appropriate data protection measures, conducting regular compliance assessments, and maintaining a mechanism to receive and handle complaints from relevant parties.

Law stated - 1 June 2026

Legitimate processing – types of PI

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

The law imposes heightened requirements for processing sensitive personal data. When seeking consent to process sensitive data, controllers must explicitly inform data subjects that the data in question is classified as sensitive. Organisations processing sensitive data must establish access-restriction rules, dedicated processing procedures, and additional security measures. The transfer of sensitive data requires physical security measures for storage and transmission devices, as well as encryption and anonymisation.

Beyond the general sensitive data regime, biometric data and location data receive further specialised protections: biometric data collectors must implement physical device security, restrict access, and maintain monitoring systems consistent with international standards, while location tracking via RFID or other technologies is prohibited absent consent or a competent authority's request. Breaches involving location or biometric data trigger a dedicated notification obligation to affected data subjects within 72 hours.

Additionally, sector-specific rules apply to sensitive data in finance and banking (requiring annual compliance assessments, full processing logs, and 72-hour breach notification for sensitive financial data) and in health and insurance (restricting disclosure of health data to third-party insurers or healthcare providers without the data subject's written request).

Law stated - 1 June 2026

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 Law (PDPL) stipulates that for consent to be valid, data subjects must be informed of certain information prior to giving their consent. In particular, the data subject must be provided with:

- the type of personal data to be processed;
- the purposes of processing;

- the identity of the personal data controller or personal data controller-processor;
- rights and obligations of the data subject; and
- an indication if any of the data to be processed falls under the category of sensitive personal data.

Law stated - 1 June 2026

Exemptions from transparency obligations

When is notice not required?

The PDPL is silent on this matter. However, given that Vietnam's privacy notice obligations are largely embedded within the consent mechanism, it can be inferred that a privacy notice may not be required in circumstances where consent is not needed. That said, the collection and use of personal data without consent and/or a privacy notice remain subject to overarching requirements, including compliance with lawful bases and the principle of data minimisation.

Law stated - 1 June 2026

Data accuracy

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

While the PDPL does not expressly impose specific standards, it does set out general principles related to data quality, currency and accuracy. In particular, 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 - 1 June 2026

Data minimisation and purpose limitation

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

The PDPL does not explicitly limit the types or amount of personal data that may be collected. However, it incorporates the principle of data minimisation. Specifically, 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 - 1 June 2026

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 PDPL imposes a storage limitation principle and regulates cases of data deletion. The PDPL states that data must be stored only for the period necessary for processing purposes, unless otherwise provided by law.

Law stated - 1 June 2026

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 Law (PDPL) sets out for personal data protection is the requirement of the coordinated and effective implementation of institutional, technical and human-based measures appropriate for the protection of personal data.

In addition, the PDPL stipulates that a personal data controller is obligated to implement appropriate managerial and technical measures to protect personal data in accordance with the law, and to review and update such measures when necessary. Meanwhile, a personal data processor is required to fully implement personal data protection measures in compliance with the PDPL and other relevant laws.

Decree No. 356/2026/ND-CP (Decree 356) also provides further clarification on these protection measures in certain specific sectors and scenarios, such as personal data protection in big data processing, AI and the metaverse, blockchain technology, and others.

Law stated - 1 June 2026

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 PDPL, the Cybersecurity Law, and other sector-specific regulations, such as banking and finance regulations. The requirements and triggering conditions will vary depending on the specific legislation applied to the case.

Under the PDPL, if a breach of personal data protection regulations is detected that may harm national defence, national security, social order and safety, or infringe on the life, health, honour, dignity, and property of data subjects, the data controller, controller-processor, or third party must notify the data protection authority within 72 hours from the detection of such breach. Data processors, in contrast, are required to promptly inform the data controller or controller-processor upon discovering such a breach. 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 - 1 June 2026

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?

The Personal Data Protection Law (PDPL) and Decree No. 356/2026/ND-CP (Decree 356) impose comprehensive internal control and accountability obligations. Controllers, controller-processors, and processors must all prepare and maintain a data processing impact assessment (DPIA) dossier, and file it with the specialised authority within 60 days of first processing and update it every six months. The DPIA dossier contains processing agreements, policies, procedures, data flow diagrams, security measures, and compliance assessment results, which must always be available for inspection.

Organisations must also designate qualified data protection personnel or a data protection unit by a formal written document, whose functions include developing compliance policies, periodically assessing the organisation's compliance status through evaluation reports, proposing risk-control measures, and implementing technical security standards and emergency response plans.

Controllers must implement appropriate management and technical measures (institutional, technical, and human) and review/update them as necessary. Data processing service providers must additionally build a risk governance framework and conduct annual compliance and trustworthiness assessments.

The specialised data protection authority under the Ministry of Public Security may conduct regular or surprise inspections covering compliance status, DPIA activities, and processing service operations, with administrative penalties for non-compliance.

Law stated - 1 June 2026

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?

The PDPL requires all organisations to appoint data protection personnel, also commonly referred to as Data Protection Officers (DPOs), regardless of the type of personal data they

handle. The detailed requirements and responsibilities of the DPO are further provided by Decree 356.

Specifically, a DPO will:

- advise on the development of policies, procedures, regulations, and forms to ensure compliance with personal data protection laws;
- participate in the exercise of the rights of the data subjects;
- participate in periodic activities assessing compliance with personal data protection laws and propose measures to enhance compliance effectiveness and to prevent and control risks;
- prepare dossiers for cross-border personal data transfer impact assessment and personal data processing impact assessment; receive and report breaches of personal data protection; and fulfil other requirements of competent authorities in accordance with regulations;
- participate in programs and training courses on personal data protection;
- participate in the implementation of technical confidentiality measures for personal data, standards and regulations on personal data protection, and emergency response plans for personal data protection incidents.

A DPO appointed by an agency or organisation must satisfy the following competency requirements:

- hold at least a college degree or higher qualification;
- have at least two years of working experience (calculated from the date of graduation) in one of the following fields: legal affairs, information technology, cybersecurity, data security, risk management, compliance control, human resources management, or personnel and organisational administration;
- have received training or professional development in legal knowledge and professional skills relating to personal data protection.

The law also permits organisations to engage external service providers to perform DPO functions instead of appointing internal personnel; such service providers are subject to more stringent qualification requirements.

Law stated - 1 June 2026

Record-keeping

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

The PDPL requires multiple categories of internal records. Controllers, controller-processors, and processors must prepare and maintain DPIA dossiers from the moment they begin processing personal data, containing impact assessment reports, copies of processing agreements/contracts, and all relevant policies, procedures, regulations, and forms. For cross-border transfers, a data transferor (data exporter) must prepare a separate transfer impact assessment (TIA) dossier. These dossiers must always be available for inspection

and are submitted to the specialised authority within 60 days, then updated periodically every six months or immediately upon specified changes.

Controllers and controller-processors must also store records of data subject consent in a verifiable format, and bear the burden of proving consent in disputes. In the finance and banking sector, organisations must specifically record logs of all personal data processing activities.

For breach incidents involving location or biometric data, organisations must record, store, and update violation records for a minimum of five years from the date the incident is remedied. Organisations must also maintain documentation of their data protection unit or personnel designation, including formal written assignments of functions and duties.

Law stated - 1 June 2026

Risk assessment

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

Under the PDPL, 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:

- information and contact details of the personal data controller, controller-processor, processor, and third parties;
- contact information of the data protection department (DPD) and data protection officer (DPO), personal data protection service providers (if any) of the personal data controller, controller-processor, processor, and third parties;
- description and explanation of the purposes of processing, categories of personal data to be processed, detailed personal data processing activities, and personal data flow diagrams;
- description and explanation of the obtaining of consent from the personal data subjects; policies on storage, deletion, and destruction of personal data;
- plans for ensuring personal data safety, personal data protection measures, system design diagrams, and the applied personal data protection standards; and
- an assessment of the potential impact of processing activities, including undesirable consequences or harms that may occur, 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, except where an applicable exemption applies. 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:

-

information and contact details for both the sender and recipients, the processor, and other parties related to the cross-border transfer of personal data;

- contact information of the DPD and DPO, personal data protection service providers (if any) of the sender and recipients;
- description and explanation about objectives of the cross-border transfer of personal data, categories of personal data to be transferred abroad, details of the cross-border transfer and processing activities, and personal data processing flow diagrams;
- description and explanation of the obtaining of consent from the personal data subjects, policies on storage, deletion, and destruction of personal data;
- plans to ensure the security of personal data after the cross-border transfer, personal data protection measures and applicable personal data protection standards;
- system diagram and description of the functions of the system used for storing and processing personal data after receipt of the cross-border transferred personal data;
- procedures governing the onward transfer or disclosure of personal data by the recipient to third parties;
- results of the self-assessment on compliance with personal data protection regulations conducted by the agency, organisation, or individual engaging in cross-border personal data transfer activities;
- assessment of the level of personal data protection implemented by the recipient, the level of impact and risks arising from the cross-border transfer and processing of personal data, undesirable consequences and damage that may occur, and the measures to mitigate or eliminate them.

Law stated - 1 June 2026

Design of PI processing systems

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

The PDPL and Decree 356 impose significant system design obligations for systems using big data, AI, blockchain, metaverse, and cloud computing. These systems must integrate appropriate data security measures, use suitable authentication and identification methods, and implement access controls, and AI processing must be classified by risk level.

Decree 356 adds specific design mandates: big data systems require multi-factor authentication (minimum), encryption/anonymisation during transfers, continuous monitoring tools, and periodic security assessments; AI systems must meet cybersecurity standards emphasising algorithm reliability, system stability, and attack prevention, with built-in monitoring mechanisms and early-warning capabilities; blockchain systems must not store personal data directly on-chain (only de-identified data or hash values) and must use secure encryption/hashing algorithms; cloud systems must encrypt personal data at rest and in transit with strict access controls; biometric systems require physical device security and intrusion-detection tracking; and blockchain developers must comply with data protection rules from the research and development stage onward – reflecting a 'by design' principle.

Law stated - 1 June 2026

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?

The Vietnamese framework does not require a general registration of all controllers or processors with the supervisory authority; instead, it imposes a data processing impact assessment (DPIA) filing obligation. All controllers, controller-processors, and processors must submit a DPIA dossier to the specialised data protection authority (under the Ministry of Public Security) within 60 days of first processing personal data, which the authority evaluates within 15 days. Exemptions apply to competent state authorities (fully exempt), household businesses and micro-enterprises (fully exempt), and small enterprises/startups (may defer for 5 years). However, these exemptions do not apply if the entity provides commercial data processing services, directly processes sensitive data, or processes data of over 100,000 data subjects.

Separately, organisations that commercially provide data processing services must obtain a Certificate of Eligibility from the authority, requiring submission of a formal application, business registration, data protection unit documentation, a project proposal (covering risk governance, standards, personnel, and compliance plans), and qualified personnel credentials; the authority evaluates within 10 days and issues the certificate within 30 days of receiving a compliant dossier.

As to penalties, failure to complete DPIA dossiers may result in administrative sanctions, and general data protection violations carry maximum fines of 3 billion dong for organisations (half for individuals), with cross-border transfer violations subject to fines of up to 5 per cent of the prior year's revenue, plus potential criminal prosecution and civil damages.

Law stated - 1 June 2026

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 Law are limited to notifying the data subjects directly, not the public.

Law stated - 1 June 2026

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 Law (PDPL) allows 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. In addition, Decree No. 356/2025/ND-CP specifies the mandatory content of data transfer agreements between the parties. The controller, of note, remains responsible to the data subject for damages caused by the processing of personal data.

Law stated - 1 June 2026

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 advertising activities, the PDPL requires advertising service providers to only use targeted audiences' personal data transferred by the personal data controller and/or the controller-processor as agreed upon or collected through their business activities to conduct the advertising services.

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

Law stated - 1 June 2026

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

Yes, cross-border transfers of personal data are restricted. The PDPL provides that any entity transferring personal data outside Vietnam (whether by moving data stored in Vietnam to overseas servers, transferring data to foreign organisations/individuals, or using overseas platforms to process data collected in Vietnam) must prepare and file a cross-border data transfer impact assessment (TIA) dossier with the specialised data protection authority within 60 days of first transferring data. The authority may order a cessation of cross-border transfers if it discovers that transferred data is being used in activities harmful to national defence or national security.

Exemptions from the TIA requirement apply to:

- transfers by competent state authorities;
- organisations storing employee data on cloud services;

- data subjects transferring their own data; and
- other cases specified by the government – with the decree further exempting press/media activities, data already publicly disclosed, emergency situations protecting life/health/property, cross-border HR management under labour agreements, and transfers for purposes such as logistics, payments, hotels, visas, and scholarships.

The maximum administrative fine for organisations violating cross-border transfer rules is 5 per cent of the prior year's revenue (or up to 3 billion dong if no revenue or if the revenue-based amount is lower).

Law stated - 1 June 2026

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 - 1 June 2026

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 2018 Cybersecurity Law and its guidance under Decree No. 53/2022/ND-CP, domestic companies providing services on telecommunications networks and the internet, 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 No. 116/2025/QH15 on Cybersecurity, which takes effect on 1 July 2026 and replaces the 2018 Cybersecurity Law, retains the data localisation requirements under the 2018 Cybersecurity Law for domestic and foreign enterprises providing services on telecommunications networks and the internet, and value-added services in cyberspace in Vietnam that engage in the collection, exploitation, analysis, or processing of personal data. However, the detailed implementation requirements remain subject to the issuance of the official guiding decree.

Law stated - 1 June 2026

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.

The Personal Data Protection Law (PDPL) upholds the data subject's right to access their personal data for viewing, modification, and requesting modifications. Decree No. 356/2025/ND-CP further stipulates that the personal data controller and controller-processor shall develop clear procedures and forms for the exercise of the rights of the data subjects and ensure that data subjects are informed of the procedures for exercising such rights. Upon receiving a data subject request to view, modify, and request modification, the personal data controller and controller-processor must respond within two working days, fully provide information on the relevant procedures, and fulfil the request within 10 days (or 15 days where processor or third-party involvement is required). A

one-time extension of up to 10 additional days is permitted where necessary, provided that the data subject is notified and the extension can be justified as necessary and reasonable.

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. This right may also be restricted where personal data is processed without the data subject's consent in accordance with the law.

Law stated - 1 June 2026

Other rights

Do individuals have other substantive rights?

The PDPL recognises the rights of data subjects to: be informed; give or withhold consent; withdraw consent; access/view data, correct and request corrections; request data provision, data deletion, and restriction of data processing; object to data processing; file complaints, denunciations, and lawsuits; claim damages; and request competent authorities or agencies, organisations, or individuals relevant to personal data processing to adopt solutions and measures to protect their personal data according to the law.

Law stated - 1 June 2026

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 the PDPL, individuals are entitled to claim compensation as prescribed by law when there are violations against regulations on the protection of their personal data. Although the PDPL does not explicitly clarify 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 - 1 June 2026

Enforcement

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

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

Law stated - 1 June 2026

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

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

Small enterprises and startups have a five-year grace period from the effective date of the Personal Data Protection Law (PDPL) 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 - 1 June 2026

SPECIFIC DATA PROCESSING

Cookies and similar technology

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

Under the Personal Data Protection Law (PDPL), providers of social networking and online communication services are required to offer users the option to refuse the collection and sharing of cookies.

With respect to cookies used in other circumstances, data collected through such tools may be considered personal data if it identifies or can help identify a specific individual. In such cases, the use of cookies is subject to the general data processing requirements set forth under the PDPL.

Law stated - 1 June 2026

Electronic communications marketing

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

Vietnam has detailed rules governing electronic marketing. In addition to the PDPL (which requires consent for using personal data in advertising and mandates that customers be informed of the content, method, form, and frequency of product promotion, with a mechanism to refuse advertising communications), Decree 91/2020 on Anti-Spam Text Messages, Email and Calls (Decree 91) imposes specific requirements:

- advertisers must obtain prior consent before sending advertising texts, emails, or making advertising calls;
- a Do Not Call List is maintained by the authority, and advertisers are prohibited from contacting numbers on this list;
-

there is also a limitation on the number of advertising messages sent within a day and the time period for sending such messages;

- all advertising texts and emails must be labelled with 'QC' or 'AD';
- advertising emails must include advertiser information (name, phone, email, address, website);
- all channels must include a clear opt-out mechanism, and advertisers must immediately cease communications upon receiving an opt-out request;
- advertisers must use a registered name identifier (brand name) issued by the authority for text and call advertising; and
- violations carry administrative fines ranging from 5 million dong to 170 million dong depending on the offence.

Law stated - 1 June 2026

Targeted advertising

Are there any rules on targeted online advertising?

The PDPL contains specific rules on targeted online advertising. It provides that organisations and individuals using personal data for behavioural advertising, targeted advertising, or personalised advertising may only collect personal data through tracking of websites, portals, or applications with the data subject's consent, and they must establish a mechanism allowing data subjects to refuse data sharing, determine data retention periods, and delete/destroy data when no longer necessary.

Social media and online media service providers must clearly disclose what personal data is collected when users install and use their services, must not collect data beyond the agreed scope, must provide users with cookie opt-out options, and must offer a 'do not track' option or only track usage with user consent. They are also prohibited from eavesdropping, wiretapping, or recording calls and reading text messages without consent.

Additionally, the use of personal data for advertising must comply with the anti-spam regulations under Decree 91/2020 and the laws on advertising, and controllers may only transfer personal data to advertising service providers in accordance with the law. Advertising service providers must be able to prove their use of customer personal data for advertising purposes and are prohibited from outsourcing or delegating the entirety of their advertising services involving personal data to third parties.

Law stated - 1 June 2026

Children's data

Are there any specific rules relating to the use of children's PI?

For children, the legal representative shall exercise the rights of the personal data subject on the child's behalf, except in cases where personal data may be processed without consent as permitted by law.

Where the processing of a child's personal data involves the publication or disclosure of information relating to the private life or personal secrets of a child of seven years or older, consent must be obtained from both the child and the child's legal representative.

The processing of a child's personal data must be suspended in the following circumstances:

- the person who provided consent as mentioned above withdraws such consent for the processing of the child's personal data, unless otherwise provided by law; or
- upon request by a competent authority where there are sufficient grounds to determine that the processing of personal data may infringe upon the lawful rights or interests of the child, unless otherwise provided by law.

Law stated - 1 June 2026

Age verification

Are there any specific rules relating to the use of PI for age verification purposes online?

The PDPL and Decree 356 do not contain specific standalone provisions addressing the use of personal data for age verification purposes online or regulating third-party age verification services as a distinct topic. However, several general and sector-specific rules would apply to age verification activities involving personal data. Social media and online media providers are prohibited from requiring users to provide images or videos containing full or partial identity documents as an account authentication factor, which would constrain certain age verification methods that rely on identity document uploads.

Any collection of personal data for age verification would still be subject to the general consent requirements, purpose limitation, and data minimisation principles under the PDPL. Where age verification involves sensitive data – such as identity card images (classified as sensitive under the Decree) or biometric data – the heightened protections for sensitive data processing would apply, including the requirement to inform data subjects that the data is sensitive.

Law stated - 1 June 2026

Sensitive personal information

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

The PDPL imposes heightened requirements for processing sensitive personal data. When seeking consent to process sensitive data, controllers must explicitly inform data subjects that the data in question is classified as sensitive. Organisations processing sensitive data must establish access-restriction rules, dedicated processing procedures, and security measures. The transfer of sensitive data requires physical security measures for storage and transmission devices, encryption, anonymisation, and other security measures during the transfer process. Additionally, biometric data and location data – both classified as sensitive – receive further specialised protections, including dedicated breach notification

requirements within 72 hours to affected data subjects, with mandatory record-keeping for at least five years.

In the finance and banking sector, entities processing sensitive financial data must apply technical data protection standards, conduct annual compliance assessments, log all processing activities, and notify both the specialised authority and affected data subjects within 72 hours of discovering any disclosure or loss of sensitive data.

Law stated - 1 June 2026

Profiling

Are there any rules regarding the use of PI for individual profiling?

The Vietnamese framework regulates individual profiling primarily through Decree 356's provisions on AI, big data, and automated processing. Controllers and controller-processors must notify data subjects about automated personal data processing, explain the operating principles of the algorithm and its impact on their rights and lawful interests, and provide options for data subjects to opt out of such processing. Data inferred by AI that can be used to identify or help identify a specific individual must be subject to personal data protection measures. Organisations must establish monitoring mechanisms for AI systems covering both state authority supervision and accountability to data subjects. Data subjects retain the right to correct, anonymise, or delete their identification profiles, even when platforms store behavioural history.

In the finance and banking sector, credit scoring, credit ranking, credit information assessment, and creditworthiness evaluation specifically require the data subject's consent, and the consent notice must explicitly disclose these profiling purposes.

Big data processing (defined as large-scale, continuous processing from multiple sources with the capability to analyse behaviour, predict trends, or classify users) requires organisations to have a mechanism to notify and explain to data subjects how their data is used in analytics systems.

The use of personal data for behavioural advertising, targeted advertising, or personalised advertising (a form of profiling) requires data subject consent for tracking via websites/apps, a mechanism to refuse data sharing, defined retention periods, and deletion when no longer necessary.

AI-based personal data processing must also be classified by risk level to apply proportionate protection measures.

Law stated - 1 June 2026

Automated decision-making

Does the law restrict the use of PI in automated decision making that affects individuals without human intervention?

The PDPL does not prohibit the use of PI for making automated decisions without human intervention that affect individuals, including profiling. However, Decree 356 stipulates that

personal data controller and controller-processor shall be responsible for notifying the data subject of automated personal data processing, explaining the operating principles of the algorithms and their impacts on the legitimate rights and interests of the data subject, and providing options allowing data subjects to opt out of such processing.

While the framework does not impose an outright prohibition on automated decision-making, it effectively requires transparency, explanation of algorithmic logic, an opt-out right, ongoing monitoring, risk classification, and – in the financial sector – specific prior consent, thereby substantially restricting unfettered automated decisions without human accountability.

Law stated - 1 June 2026

Cloud services

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

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.

Decree 356 provides more detailed implementing regulations regarding cloud computing services. In particular, organisations and individuals entering into contracts related to personal data processing with cloud computing service providers shall have the following responsibilities:

- specify in the contract the compliance with the laws of Vietnam on personal data protection, provide information on the personal data protection unit and personnel, and comply with administrative procedures related to personal data protection in accordance with the law;
- identify personal data processing flows, the roles of the concerned parties in cloud computing service provision, and corresponding responsibilities;
- require confidentiality measures and technical and organisational measures, which shall be clearly stipulated in the contract;
- immediately notify the concerned parties of any changes that may affect personal data;
- comply with personal data processing time limits and requirements for deletion and destruction of personal data;
- ensure the exercise of the rights of the personal data subjects;
-

fully implement technical measures to ensure that access to personal data is reasonably delegated.

Cloud computing service providers must:

- comply with the personal data protection regulations of Vietnam, provide information on the personal data protection unit and personnel, and comply with administrative procedures related to personal data protection in accordance with the law;
- require subcontractors to comply with personal data protection regulations and obligations in accordance with the law;
- apply technical and organisational measures at a level appropriate to the scale and extent of their personal data processing;
- conduct periodic assessments of compliance with personal data protection regulations once per year.

Personal data in cloud computing must be encrypted both at rest and in transit, together with strict access authorisation.

Law stated - 1 June 2026

UPDATE AND TRENDS

Key trends and future developments

Are there any emerging trends or hot topics in data protection in your jurisdiction, and are there any proposed changes to the current legislation?

Vietnam's data protection landscape is in a period of rapid transformation. The most significant development was the elevation of the framework from decree-level to a full statutory Law on Personal Data Protection (effective 1 January 2026), accompanied by implementing Decree 356. A critical pending development is the draft decree on sanctioning, which the government is expected to pass in the very near future. Until this decree is issued, there is an enforcement gap as the Ministry of Public Security (MPS) lacks a formal basis to impose specific administrative penalties under the new law.

In parallel, Vietnam is rapidly developing technology-specific legislation, including a Law on Artificial Intelligence with a national governance framework, Decree 142/2026 on AI risk classification, a new Law on Cybersecurity (effective July 2026), and a new Law on Electronic Commerce (effective July 2026). The Data Law (effective July 2025), governing both personal and non-personal data, creates an overlapping regime that organisations must navigate alongside the Personal Data Protection Law (PDPL). The MPS is drafting a new Law on Data Security, which proposes a broader regulatory framework for data security and data governance with implications for, and potentially influence, the direction of the current personal data protection regime. Businesses should, therefore, continue to monitor forthcoming legislative developments closely.

These developments place Vietnam squarely within the broader Asia-Pacific privacy acceleration trend, with the intersection of privacy and AI governance, children's data protection, and increasing enforcement expectations being key themes.

Law stated - 1 June 2026