Vietnam's 2025 Law on Personal Data Protection: The Legal Turning Point for the Digital Era

Alitium
Level 5, L'Mak Signature Building
147 Hai Ba Trung, District 3
Ho Chi Minh City
Vietnam

P: +84 (28) 3535 6460
E: vietnam@alitium.com

Contact
Phuong Vo
Managing Partner
phuong.vo@alitium.com

Phung Nguyen
Accounting & Tax Partner
phuong.nguyen@alitium.com

Matthew Lourey
Chairman & Advisor
mlourey@alitium.com

[28 July 2025]

Vietnam's 2025 Law on Personal Data Protection

In the context of rapid globalization and digital transformation, personal data has emerged as a highly valuable digital asset; not only for individuals but also for businesses, organizations, and state authorities. Prior to Vietnam's Law on Personal Data Protection 2025 being passed on 26 June 2025, the protection of personal data in Vietnam was governed through provisions dispersed across various legal instruments, specifically:

- Civil Code 2015: Section 2 – Personal Rights, Article 38 on the Right to privacy, personal secrets, and family secrets stipulates that the collection, storage, use, and disclosure of information relating to private life, personal secrets, and family secrets must be consented to by the data subject, unless otherwise provided by law.

- Law on Cybersecurity 2018: Chapter III – Prevention and actions against cybersecurity violations, Article 17 on Prevention and response to cyber espionage; protection of state-secret information, business secrets, family secrets and privacy in cyberspace, provides that information system administrators are responsible for protecting personal data and for removing data associated with violations upon request.

- Notably, the enactment of Decree No. 13/2023/ND-CP dated 17 April 2023 of the Government on personal data protection (hereinafter referred to as Decree 13), a subordinate legal instrument effective from 1 July 2023, has established the first legal framework for the protection of personal data in Vietnam to date.

Although Decree 13 established Vietnam's first dedicated legal framework for personal data protection, it remains somewhat limited in scope and did not comprehensively address the complex and evolving nature of data processing activities, particularly in relation to enforcement mechanisms for violations and cross-border data processing activities. In light of these limitations, the promulgation of the Law on Personal Data Protection 2025 (hereinafter referred to as the PDP Law), which was passed on 26 June 2025 and which takes effect on 1 January 2026, constitutes a critical and timely legislative response. The PDP Law intendeds to provide stronger safeguards for the privacy and personal data of Vietnamese citizens, while also supporting the sustainable development of the digital economy.

Alitium

Below we have highlighted the key developments and provisions introduced by the PDP Laws, along with practical recommendations for businesses in preparing for compliance.

1. Expansion of regulatory scope and subjects of application

The PDP Law introduces a substantial expansion in both its regulatory scope and the entities to which it applies. While Decree 13 primarily focused on organizations and individuals physically present in Vietnam engaged in the collection, storage, use, and processing of personal data within Vietnamese territory, the PDP Law expressly extends its reach to foreign entities without a physical presence in Vietnam, provided they process personal data relating to Vietnamese citizens or persons of Vietnamese origin whose nationality has not yet been determined.

This development signals a clear shift toward extraterritorial application, requiring compliance from multinational companies and corporations that either conduct business activities targeting the Vietnamese market or collect Vietnamese citizens' data. By doing so, the PDP Law strengthens the legal basis for cross-border data governance and enhances protections for Vietnamese individuals using foreign-based digital platforms, for instance, Facebook, Instagram, Google, and others.

2. Defining de-identification of personal data

For the first time in Vietnamese legislation, the PDP Law introduces the concept of "de-identification". This refers to the process of removing or modifying identifying elements within personal data to ensure that the individual cannot be identified or linked to the data. Accordingly, once data has been de-identified, it is no longer regarded as personal data. This means that once personal data is properly anonymized and can no longer be traced back to an individual, it is no longer subject to data protection rules.

3. New obligations for personal data processing organizations and enterprises

The PDP Law introduces stricter obligations for organizations and enterprises involved in personal data processing, aiming to enhance accountability and ensure a higher standard of data security and confidentiality. Specifically:

i. Designation of personnel or department for personal data protection

Organizations and enterprises are required to appoint an internal personnel or department with the appropriate professional qualifications and expertise to oversee compliance with personal data protection obligations. Alternatively, they may engage an external individual or organization with relevant expertise to provide data protection services in lieu of establishing an internal function.

The specific qualifications, standards, and requirements applicable to internal personnel, dedicated departments, or external service providers responsible for personal data protection shall be further detailed in regulations issued by the Government.

ii. Assessment of cross-border personal data transfer impact

Compared to Decree 13, the PDP Law provides a more detailed legal framework governing the cross-border transfer of personal data, specifying three distinct circumstances in which such transfers may occur:

- Personal data stored in Vietnam is transferred to a system located outside of Vietnam;
- Organizations, authorities or individuals in Vietnam transfer personal data to recipients who are individuals or organizations located abroad;
- Organizations, authorities or individuals – either in Vietnam or abroad – use foreign platforms to process personal data collected within Vietnamese territory.

When an organization or individual conducts cross-border personal data transfer, they are required to prepare dossiers on the assessment of cross-border personal data transfer impact and submit them to the data protection authority under the Ministry of Public Security. This submission must be made within 60 days of the date the personal data is first transferred abroad. The

specific contents of the dossier, as well as the procedures for preparation and submission, shall be further detailed in implementing regulations issued by the Government.

However, not all cross-border data transfers are subject to the requirement of preparing the assessment of cross-border personal data transfer impact dossiers. The PDP Law explicitly provides for certain exceptions, including the following circumstances:

- Where the transfer of personal data is carried out by a competent authority;
- When an organization or authority stores its employees' personal data using cloud computing services;
- Where the data subject (the owner of the personal data) transfers their own personal data outside of Vietnam;
- Other circumstances to be specifically defined by the Government in future implementing regulations.

4. Sector-specific regulations on personal data processing

A highlight of the PDP Law is its introduction of activity/sector-specific regulations governing personal data processing in contexts such as recruitment and employment management, sectors of healthcare and insurance, finance, advertising and social media. This marks a significant step forward in both the comprehensiveness and practical relevance of the legal framework, going beyond what was previously provided under Decree 13.

These sector-specific provisions not only broaden the regulatory scope of personal data protection law but also impose clear compliance obligations on organizations and individuals operating within these industries, or engaging in personal data processing activities for purposes related to these sectors:

i. Recruitment and employment management

- Employers (organizations, authorities, or individuals) may only collect personal data that is necessary for recruitment purposes, and must do so in accordance with the relevant legal provisions.
- In cases where a job applicant is not hired, any personal data collected must be deleted or destroyed, unless there is an agreement with the applicant to retain the data for future opportunities.
- Personal data of employees may only be retained for a period that is appropriate under relevant laws or in accordance with a lawful agreement between the parties. Upon termination of the labor contract, the data must also be deleted or destroyed, unless otherwise required by law or agreed upon separately by both parties for continued retention.

ii. Healthcare and insurance sectors

- The collection and processing of personal data in these sectors may only occur with the explicit consent of the data subject. Healthcare organizations are not permitted to disclose personal data to any third parties (healthcare service providers, health insurers, or life insurance companies) without the data subject's prior written consent.
- In cases involving reinsurance or retrocession arrangements, the executed contract must clearly state whether the customer's personal data will be shared with external partners, and if so, must specify the method and conditions under which such data transfers will take place.

iii. Finance, banking, and credit activities

- Organizations and individuals operating in the fields of finance, banking, and credit information must comply with all applicable regulations concerning the protection of sensitive personal data.
- The use of an individual's credit information for credit scoring or rating is only permitted with the data subject's prior and explicit consent.

- In the event of a personal data breach (disclosure or data loss), the data subject must be promptly notified.

- Appropriate security measures must be implemented to prevent unauthorized access, use, or disclosure of personal data, and to ensure data security throughout the entire process of collection and processing.

iv. Advertising services

- Organizations and individuals providing advertising services (advertisers) may only use personal data that has been lawfully transferred by a personal data controlling party, personal data processing and controlling party, or data collected directly through their own business activities.

- Prior to processing personal data, advertisers must obtain the data subject's consent and provide a clear mechanism for the data subject to refuse or request cessation of advertising communications.

- The use of personal data for advertising purposes must comply with legal provisions on anti-spam regulations (via email, text messages, or phone calls).

- It is strictly prohibited for advertisers to lease out or delegate the advertising service to third parties if such services involve the use of customers' data.

- Advertisers are responsible for demonstrating full compliance with all regulations on personal data protection.

v. Social media platforms and online communication services

- Organizations and individuals providing social media platforms and online communication services (service providers) must ensure transparency regarding the specific categories of personal data intended to be collected. The collection of any data beyond the scope expressly consented to by the user is strictly prohibited.

- Service providers are prohibited from requiring users to furnish images or videos containing all or part of personal identification documents solely for account verification.

- Any act of unauthorized interception of calls or access to message content without the explicit consent of the user is strictly prohibited.

- Privacy policies must be clearly disclosed, and users must be allowed to access, modify, and delete their personal data. In cases where data is transferred abroad, service providers must implement appropriate safeguards to protect the personal data of Vietnamese citizens.

vi. Other specialized sectors (artificial intelligence, cloud computing, biometric data, audio and video recording activities in public places and public activities)

These provisions aim to safeguard privacy in the context of emerging technologies. In particular, service providers are prohibited from unlawfully collecting or processing data in a manner that harms data subjects.

5. Penalty framework for data protection violations

The PDP Law addresses a key shortcoming of Decree 13 by clearly stipulating administrative sanctions relating to personal data protection. Penalties are more clearly defined, particularly for organizations, as follows:

- Unlawful trading of personal data: A fine of up to 10 times the revenue gained from violating conduct.

- Violation of cross-border transfer of personal data: A maximum fine of up to 5% of the preceding fiscal year's revenue.

- Other violations (excluding the two categories above): A maximum fine of VND 3 billion.

For individuals committing similar violations, the maximum fine is capped at 50% of that imposed on organizations.

Further guidance on determining revenue as a basis for calculating penalties is to be provided by the Government.

6. Impacts and recommendations for enterprises

To ensure compliance and mitigate legal risks ahead of the PDP Law coming into effect on 1 January 2026, enterprises should proactively take the following actions:

- **Conducting a comprehensive review:** Assess all current practices for collecting, storing, processing, and sharing personal data to identify any gaps with the new legal requirements.
- **Developing and updating internal policies:** Establish or revise internal personal data protection policies, response protocols for data subject requests, and integrate data protection clauses into contracts with clients, partners, and vendors.
- **Designating and training personnel:** Appoint a dedicated individual or department, or engage an external service provider, and provide training to all relevant personnel to strengthen awareness and ensure effective compliance with data protection obligations.
- **Conducting an assessment on personal data impact:** Evaluate potential risks in new or existing data processing activities and maintain or submit assessment documentation as required by law.
- **Ensuring cross-border data transfer compliance** (for enterprises involved in transferring personal data abroad): Prepare and submit the required dossiers on the assessment of cross-border personal data transfer impact in accordance with the new regulations.
- **Enhancing information technology (IT) and data security infrastructure:** Upgrade IT systems and implement technical security measures to safeguard personal data across all processing stages.

The promulgation of the PDP Law represents a major milestone in strengthening Vietnam's legal framework for privacy and data security. To ensure compliance and minimize potential legal risks, organizations, authorities, and individuals must proactively review the new requirements and take timely steps to align their operations with the law's provisions.

Article written by Mr Dao Hieu Tran, Legal Associate at Alitium

For any further questions you may have, please reach out to us at vietnam@alitium.com

****

This article is intended to provide an overview of recent updates to tax regulations. While it aims to present useful insights, it is important to note that the content shared here should not be considered as formal legal or financial advice. For specific guidance on tax obligations or legal matters related to your business, we strongly recommend consulting with a qualified professional, such as a tax advisor or legal expert or directly reach out to us.