30 YEARS | FRASERS LAW COMPANY

Vietnam's Long-awaited Personal Data Protection Law

What is changing and how does it affect your business?

Legal Update | July 2025

Vietnam's Long-awaited Personal Data Protection Law: What is changing and how does it affect your business?

On 26 June 2025, the National Assembly of Vietnam officially enacted the Personal Data Protection Law (***PDPL***), which will come into force on 1 January 2026. Compared to Decree No. 13/2023/ND-CP of the Government dated 17 April 2023 on personal data protection (***Decree 13***), the PDPL provides clearer regulations to enhance the data privacy landscape in Vietnam while still ensuring the free flow of data. We highlight the key provisions introduced by the PDPL in our Legal Update.

1. Scope of application

Compared to Decree 13, the PDPL provides greater clarity in relation to its applicability to foreign organisations, agencies and individuals. Accordingly, for foreign organisations, agencies, and individuals not based in Vietnam, the PDPL applies only when such entities directly process or are involved in the processing of personal data of Vietnamese citizens or persons of Vietnamese origin with undetermined nationality reside in Vietnam and have been issued identification cards.

2. Administrative fines

The PDPL introduces significant administrative fines for violations of personal data protection regulations, specifically:

- For the trading of personal data, the maximum fine is either 10 times the revenue gained from the violation or VND3 billion (approximately US$113,208), whichever is higher.
- For breaches involving cross-border transfers of personal data, the maximum fine is either 5% of the violator's revenue from the previous year or VND3 billion (approximately US$113,208), whichever is higher.
- For other violations, the maximum fine is VND3 billion (approximately US$113,208).

The above fines apply to legal entities. In cases where the same violations are committed by an individual, the maximum administrative fine is equivalent to half of the amount applicable to legal entities.

3. Transfer of personal data

The PDPL sets out specific circumstances under which the transfer of personal data is permitted, including:

- having the consent of the data subject;
- sharing personal data among departments within the same agency or organisation to process personal data in accordance with the intended purposes;
- transferring due to restructuring of agencies and organisations (e.g., separation, merger, or reorganisation);
- transferring to personal data processors or third parties by personal data controllers or personal data controllers and processors, for processing in accordance with the law;
- transferring upon request from relevant authorities; and
- transferring without the data subject's consent in certain cases as prescribed by laws (e.g., to serve the operations of relevant authorities, implement

agreements between the data subject and relevant agencies, organisations, or individuals).

4. Application dossiers for data processing impact assessment and cross-border data transfer impact assessment

The PDPL does not specify the detailed dossiers and procedures for personal data processing impact assessment (***DPIA***) and cross-border personal data transfer impact assessment (***DTIA***) but delegates these responsibilities to the Government for regulation. Alternatively, the PDPL provides general principles as follows:

- With respect to DTIA, entities performing the following activities are required to prepare and submit the DTIA to the specialised personal data protection authority within sixty (60) days from the date of the first transfer:
  - Transferring personal data stored in Vietnam to data storage systems located outside Vietnam;
  - Vietnamese agencies, organisations, or individuals transferring personal data to foreign entities or individuals; and
  - Vietnamese or foreign agencies, organisations, or individuals using platforms located outside Vietnam to process personal data collected within Vietnam.

  However, there are certain exceptions where the DTIA requirements do not apply:
  - Cross-border data transfers conducted by relevant authorities;
  - Agencies or organisations storing employee personal data on cloud computing services;
  - Data subjects personally transferring their personal data across borders;
  - Other cases as prescribed by the Government.
- With respect to DPIA, the provisions under the PDPL are largely similar to those set out in Decree 13. Accordingly, personal data controllers, personal data controllers and processors, and personal data processors are required to prepare and submit a DPIA to the specialised personal data protection authority within sixty (60) days from the date of the commencement of personal data processing. Under the PDPL, the governmental authorities are exempt from DPIA requirements.

DPIA and DTIA shall be conducted once for the entire duration of operations of agencies, organisations, or enterprises and shall be updated every six (6) months to reflect any changes or immediately in the following circumstances:

- When the agency or organisation is reorganised, dissolved, or declared bankrupt in accordance with the law;
- When there is a change in information about the organisation or individual providing personal data protection services;
- When arising a new business line or service line or suspending the business of services and products related to personal data registered in DPIA and DTIA.

It should be noted that DPIA and DTIA submitted to the authority in accordance with Decree 13 shall remain valid. Entities are not required to re-submit them in accordance with the PDPL. Another noteworthy provision is that entities that have

conducted DPIA and DTIA in accordance with the PDPL are not required to conduct personal data processing risk assessment or cross-border personal data transfer impact assessment under relevant data laws.

5. Detailed regulations for personal data protection in specific activities

The PDPL introduces new data protection requirements applicable to various activities, such as employee recruitment and management; insurance business; finance and banking; marketing; social media; big data processing, artificial intelligence (***AI***), blockchain, metaverse, cloud computing.

Notably, the provisions on employee recruitment and management explicitly require employers to request only personal data necessary for recruitment purposes. If a candidate is not hired, the employer must delete or destroy their personal data, unless otherwise agreed upon with the candidate. A similar approach applies to employees, whereby upon termination of the employment contract, the employer is required to delete or destroy the employee's personal data, unless otherwise agreed upon or required by law.

In relation to finance and banking, the PDPL establishes specific responsibilities for organisations and individuals operating in these fields, such as they are prohibited from using a data subject's credit information for credit scoring, credit rating, credit assessment, or evaluating creditworthiness without the consent of the data subject, they shall collect only the personal data necessary to carry out credit information activities from sources in accordance with the law, and they must promptly notify the data subject in the event of any breach or loss of information related to bank accounts, financial data, or credit information.

For the advertising sector, the PDPL introduces stricter regulations, notably prohibiting organisations and individuals providing advertising services from outsourcing or contracting other parties to carry out the entire advertising service where the use of personal data is involved.

In addition, to protect human rights in an increasingly digital landscape, the use of big data, AI, blockchain, metaverse, and cloud computing must incorporate appropriate personal data security measures. Suitable authentication methods, identification processes, and access controls must be employed when processing personal data. Furthermore, the processing of personal data using AI must follow risk-based classification to implement corresponding data protection measures.

The introduction of the above sector-specific personal data protection regulations aims to strengthen the protection of personal data, given that these sectors are particularly sensitive and any violations in these areas could have serious negative impacts on the rights and interests of data subjects.

6. Personal data protection workforce

The personal data protection workforce includes, among others, (i) dedicated data protection departments and personnel within agencies and organisations, and (ii) organisations and individuals providing personal data protection services.

Agencies and organisations are responsible for appointing qualified data protection departments and personnel or hiring organisations and individuals to provide personal data protection services (collectively referred to as ***the DPO and DPD Requirements***). The specific qualifications and standards required for these entities and individuals will be further detailed by the Government.

7. Transitional provisions

Small businesses and startups may opt out of the DPIA, DPO and DPD Requirements for five (5) years from the effective date of the PDPL. Microenterprises and household businesses are fully exempt from these requirements. However, these exemptions do not apply to entities that provide personal data processing services, directly process sensitive personal data, or handle personal data of a large number of data subjects.

There is no explicit provision in the PDPL in relation to the status of Decree 13 once the PDPL takes effect. However, it is expected that a new decree will be issued to provide detailed guidance on the implementation of the PDPL, which will replace Decree 13.

Authors

Duong Thi Mai Huong
Partner
huong.duong@frasersvn.com

Nguyen Pham Minh Thao
Legal Assistant
thao.nguyen@frasersvn.com

Ho Chi Minh City

19th Floor, Deutsches Haus
33 Le Duan Boulevard
Saigon Ward
Ho Chi Minh City, Vietnam
T: +84 28 3824 2733

Hanoi

15th Floor, Pacific Place
83B Ly Thuong Kiet Street
Cua Nam Ward
Hanoi, Vietnam
T: +84 24 3946 1203

Website www.frasersvn.com
Email legalenquiries@frasersvn.com