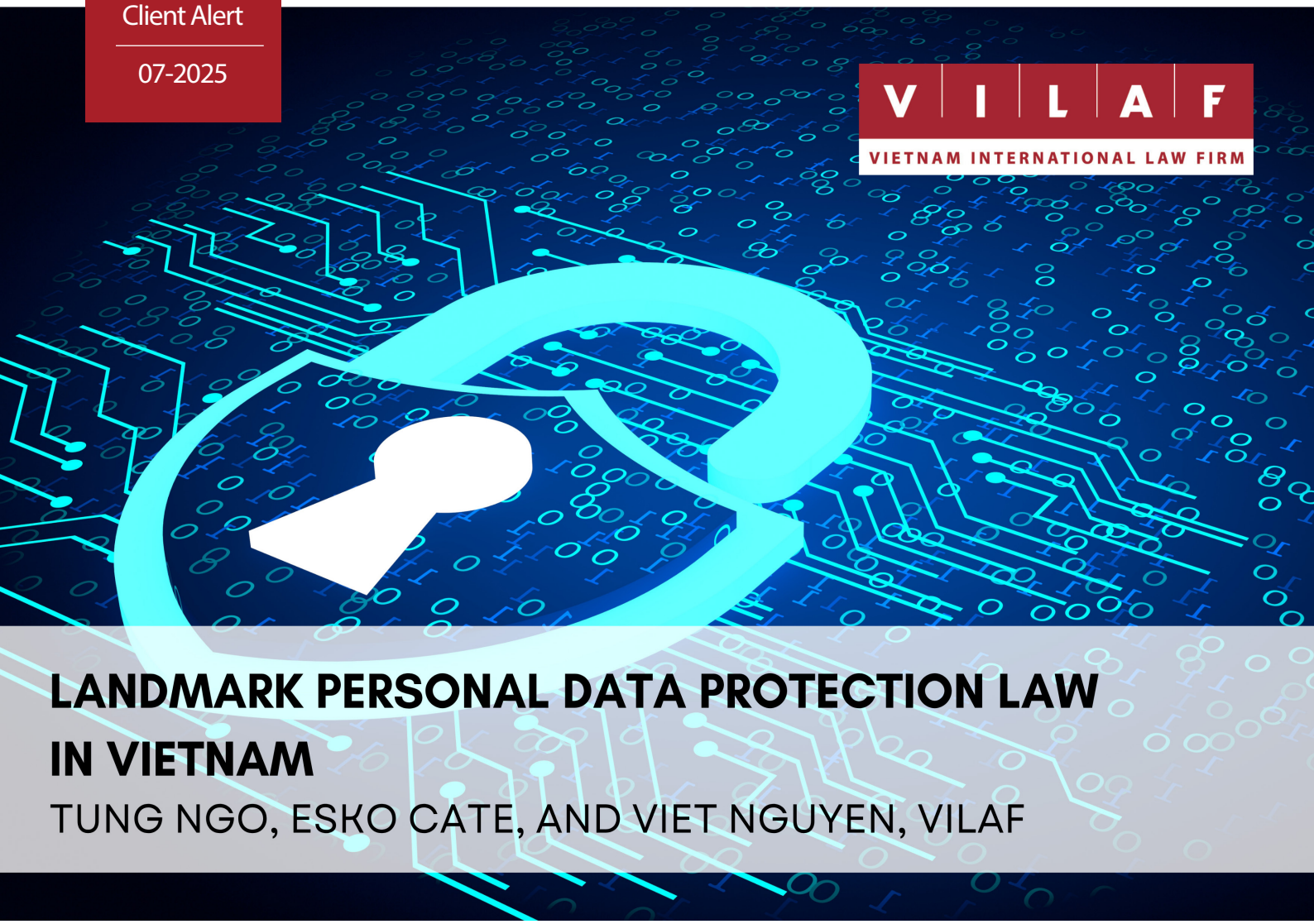
Client Alert

07-2025

VILAF

VIETNAM INTERNATIONAL LAW FIRM



LANDMARK PERSONAL DATA PROTECTION LAW IN VIETNAM

TUNG NGO, ESKO CATE, AND VIET NGUYEN, VILAF

Vietnam's National Assembly has recently passed the Law on Personal Data Protection ("**LPDP**") with overwhelming support. This landmark legislation, comprising 39 articles, will take effect on January 1, 2026, and will supplement and supersede the existing Decree No. 13/2023/ND-CP on personal data protection ("**Decree 13**").

COMPREHENSIVE SCOPE

The LPDP introduces a framework that is more detailed than that of Decree 13 to govern the collection, processing, storage, transfer, disclosure, and deletion of personal data. It substantially clarifies and defines the roles and responsibilities of data controllers, processors, third parties, and enforcement authorities, as well as implementing much needed exceptions.

The LPDP applies to:

i. Vietnamese individuals and entities;
ii. foreign individuals and entities operating in Vietnam; and
iii. foreign entities processing personal data of Vietnamese citizens or individuals of Vietnamese origin residing in Vietnam with valid identification.

The LPDP also simplifies and updates the definition of personal data, with further classification and guidance to be issued by the Government.

INTRODUCTION OF SPECIFIC PENALTIES

The LPDP introduces significant enforcement mechanisms, including both administrative fines and criminal liability, depending on the severity of the violation. Entities must also compensate affected individuals for any damage resulting from their violations of the LPDP.

For entities, the maximum fines for administrative violations include up to ten times the revenue from the sale of personal data, 5% of the previous year's revenue for cross-border data transfer violations, and up to 3 billion VND for other violations. For individuals, the maximum fines are half of those applicable to organizations. The Government will issue guidance on how revenue from violations is calculated.

SIMILARITIES & DIFFERENCES

One of the most significant changes in the LPDP is the inclusion of exceptions to the previously absolute rights of data subject. Under the LPDP, several exceptions to the requirements to obtain consent for data processing are added and several others are clarified. The LPDP applies a more balanced approach, requiring that individuals do not obstruct or hinder the lawful rights and obligations of personal data controllers and/or processors when exercising their rights, nor infringe upon the legitimate rights and interests of organizations or other individuals. These clarifications help prevent the weaponization of data privacy rights against data controllers and/or processors and create a data processing environment that is more conducive to doing business.

That said, the LPDP retains key compliance obligations from Decree 13, particularly regarding data processing, cross-border data transfers, and appointment of data protection department and personnel:

1. **Impact Assessments ("DPIA")**

   Under the LPDP, both Data Processing Impact Assessments ("DPIAs") and Outbound Transfer Impact Assessments ("OTIAs") remain mandatory. Data controllers and processors must prepare and retain DPIA reports within 60 days of commencing any personal data processing, while entities transferring personal data abroad must submit OTIA reports within 60 days of the first transfer. Both assessments must be updated every six months or immediately upon certain changes in business operations. The Government may evaluate the reports and request supplementation. However, the LPDP does outline some limited exemptions to the OTIA requirement, including transfers by authorized state agencies, use of cloud services for employee data, and self-transfers by data subjects.

2. **Appointment of data protection department and personnel**

   Entities are responsible for appointing qualified personnel or departments to oversee personal data protection. However, under the LPDP, it is clear that entities may hire external individuals or entities to provide these services. Details of the qualifications and roles of the data protection department and personnel will be further specified by the Government.

Additionally, in comparison to previous drafts, the LPDP no longer details administrative procedures, processes, or documentation requirements. Instead, it delegates authority to the Government, which is expected to issue detailed compliance regulations through future decrees and circulars. Businesses should prepare for additional guidance and operational requirements in the near term.

ACTIVITY-SPECIFIC RULES

The LPDP introduces detailed data protection obligations tailored to processing related to specific activities, including employment, healthcare and insurance, finance, advertising, and social media. These provisions go beyond the scope of Decree 13 and impose targeted compliance requirements on organizations operating in these domains or processing personal data related to these purposes. The key areas are as follows:

1. Employment & Recruitment

   For recruitment, organizations and individuals are permitted to collect only personal data that is necessary for recruitment purposes and must use such data in accordance with applicable laws. If a candidate is not hired, the collected data must be deleted or destroyed, unless otherwise agreed with the data subject. The LPDP states that employers must manage employee personal data in compliance with applicable laws, specifically the Labor Code, retain it only for the lawful or agreed duration, and delete it upon contract termination unless otherwise agreed or required by law.

2. Health and insurance

   Personal data may only be collected and processed with the explicit consent of the data subject. Healthcare organizations are prohibited from disclosing personal data to third parties without written consent. In the insurance sector, reinsurance contracts must clearly specify whether and how personal data will be transferred to external partners.

3. Finance

   Financial, banking, and credit information organizations must comply with regulations on sensitive data protection, obtain consent before using personal credit information for scoring, and notify data subjects in case of data breaches. Additionally, they must implement measures to prevent unauthorized access and ensure data security during collection, processing, and provision of credit information.

4. Advertisement

   Advertising service providers can only use personal data transferred by data controllers, data controllers / processors, or collected through their own business activities. They must obtain customer consent for data processing, provide clear mechanisms for individuals to opt out of receiving advertising communications, and comply with applicable laws on spam prevention. Notably, the LPDP prohibits the outsourcing of advertising services that involve the use of personal data. Providers are also responsible for demonstrating compliance with all data protection obligations. Additionally, for behavioral or targeted advertising, additional safeguards apply.

5. Social media

   Social media and online communication service providers must clearly inform users about the personal data collected. Providers must not collect unauthorized data or require images or videos of identification documents for account verification. The LPDP extends restrictions beyond personal data and explicitly prohibits providers from eavesdropping on calls and messages without consent. They must also publish privacy policies, offer mechanisms for users to access, edit, and delete data, and protect Vietnamese citizens' data during cross-border transfers.

PREPARING FOR THE NEW LAW ON PERSONAL DATA PROTECTION

The LPDP comes into effect on January 1st, 2026. Especially in light of the substantial penalties for non-compliance set out in the LPDP, businesses should begin taking proactive steps as soon as possible. These include:

1. Preparing or reviewing and updating internal data protection policies, procedures, and contracts to align with new legal requirements.

2. Conducting data mapping and risk assessments to identify personal data flows inside your organization and to evaluate potential vulnerabilities.

3. Training employees on their responsibilities under the LPDP, including data subject rights and handling procedures.

4. Staying informed about upcoming Government decrees/circulars that will provide additional, detailed guidance on compliance obligations.

We are actively monitoring the release of implementation guidelines and will keep you updated as new information becomes available.

In the meantime, VILAF is ready to support your transition and help you navigate the LPDP with tailored services.

For further details, please contact Mr. Ngo Thanh Tung at tung@vilaf.com.vn.

FOR MORE INFORMATION PLEASE CONTACT:

VILAF
VIETNAM INTERNATIONAL LAW FIRM

Tung Ngo
HCMC Managing Partner
tung@vilaf.com.vn

Esko Cate
Senior Associate
esko.cate@vilaf.com.vn

Viet Nguyen
Associate
hoangviet.nguyen@vilaf.com.vn