LEXCOMM
Solicitors & Barristers

Legal Update
July 2025

Legal Update on Law on Personal Data Protection

On 26 June 2025, the National Assembly officially passed Law No. 91/2025/QH15 on Personal Data Protection (**PDPL**), which will officially replace Decree No. 13/2023/ND-CP on Personal Data Protection (**Decree 13**). Building upon the foundations established by Decree 13, the PDPL introduces a consolidated and comprehensive legal framework for personal data protection in Vietnam and has extraterritorial effect, applying not only to domestic entities but also to foreign organisations that directly process or are involved in processing personal data of individuals residing in Vietnam. The PDPL consists of 39 articles divided into five chapters and will come into force on 01 January 2026.

In this legal update, we will outline the key contents of the PDPL, highlighting critical compliance obligations that all entities engaging in personal data processing in Vietnam should stay alert on.

1. Scope of the application

(1) The PDPL applies to all entities that process personal data or are involved in the processing of personal data within the territory of Vietnam, regardless of their nationality. This extra-territorial scope of application is recognised under the PDPL, which explicitly stipulates that the provision thereof applies to:

(a) Vietnamese agencies, organisations, and individuals;

(b) foreign authorities, entities, and individuals operating in Vietnam; and

(c) foreign agencies, organisations, and individuals that directly process or are involved in the processing of personal data of Vietnamese citizens or stateless persons of Vietnamese origin residing in Vietnam.

(2) The PDPL is designed to safeguard the personal data of all Vietnamese residents, including both Vietnamese citizens and stateless persons of Vietnamese origin residing in Vietnam. Accordingly, its protection mechanisms apply to any processing activities

involving their personal data, regardless of whether the processing is conducted within or outside of Vietnam.

2. Data Controller, Data Processor, Data Controlling and Processing Entity, Third Party and their responsibilities

Identify the data processing roles

(1) Similar to Decree 13, the PDPL also provides a number of concepts in personal data protection, including the roles of "Data Controller", "Data Processor", "Data Controlling and Processing Entity" and "Third Party", outlined as follows:

(a) The Data Controller is the entity determining the purpose and methods of processing personal data;

(b) The Data Processor is the entity handling personal data on behalf of the Data Controller through a contract or agreement;

(c) The Data Controlling and Processing Entity is the entity that simultaneously determines the purpose, methods, and directly processes data; and

(d) Third Parties are external entities authorised to process data, distinct from the Data Controller, Data Processor, and Data Controlling and Processing Entity.

(2) Concerning Third Parties, the PDPL does not explicitly specify which entities qualify as Third Parties. However, following the Ministry of Public Security's perspective, entities participating in data processing without directly handling the data (e.g., providing a platform for cloud storage) may be considered Third Parties.

Responsibilities of each party under the PDPL

(3) The Third Party under the PDPL is not assigned a comprehensive list of obligations. Its responsibilities are limited and primarily relate to cooperate with authorised entities and complying with lawful instructions during data processing. Such obligations may be further specified in forthcoming implementing regulations of the PDPL.

(4) All three other entities, the Data Controller, Data Processor, and Data Controlling and Processing Entity, share several core obligations under the PDPL when participating in personal data processing. These include implementing data protection measures, preventing unlawful data collection, and cooperating with the competent authorities in handling violations of personal data protection law.

(5) Apart from the aforementioned responsibility, the Data Controller have specific obligations as follows:

(a) Clearly define roles, rights, and obligations of all parties involved in personal data processing in relevant contracts or agreements;

(b) Determine the purposes and means of personal data processing and ensure such purposes and means are stated in their documentation with data subjects in accordance with the PDPL's requirements;

(c) Implement and maintain technical and managerial measures appropriate to the level of risk to protect personal data, and regularly review and update such measures as needed;

(d) Report personal data breaches to the competent authority;

(e) Select appropriate Data Processors with sufficient technical and organisational capacity to perform personal data processing activities securely and lawfully;

(f) Protect the rights of data subjects, including responding to their lawful requests and ensuring transparency of processing;

(g) Assume liability for any damages caused by their processing of personal data;

(h) Prevent any unauthorised or unlawful collection of personal data through their systems, devices, or services;

(i) Cooperate with the Ministry of Public Security (**MPS**) and other relevant authorities by providing necessary information and support in investigations or legal enforcement proceedings.

(6) Aside from the responsibility mentioned above, the Data Processor must also carry out the following tasks:

(a) Only receive and process personal data pursuant to a written contract or agreement with the Data Controller or the Data Controlling and Processing Entity.;

(b) Process personal data strictly within the scope of the agreed-upon terms and purposes;

(c) Implement and maintain adequate technical and organisational measures to protect personal data in compliance with the PDPL;

(d) Be liable to the Data Controller or Controlling and Processing Entity for any damage caused in the course of its processing;

(e) Assist competent authorities such as the MPS in enforcing data protection laws;

(f) Fulfil all additional responsibilities under the PDPL and other applicable regulations.

(7) The Data Controlling and Processing Entity must comply with all responsibilities imposed on both the Data Controller and the Data Processor above.

3. Requirements on PDPIA and PDTIA Dossiers

Who needs to submit the PDPIA and PDTIA Dossiers?

(1) The PDPIA dossier must be established, maintained, and submitted by the Data Controller, the Data Controlling and Processing Entity, or alternatively by a Data Processor (if such processor is under contract with the Data Controller and on behalf of the either Data Controller or the Data Controlling and Processing Entity), following the initiation of personal data processing (which encompasses activities such as collecting,

recording, analyzing, storing, disclosing, accessing, copying, transmitting, etc., of personal data).

(2) Meanwhile, the PDTIA must be established, maintained, and submitted in the following circumstances:

(a) When personal data stored in Vietnam is transferred to a data storage system located outside of Vietnam;

(b) When entities based in Vietnam transfer personal data to entities located abroad; and

(c) When foreign entities use offshore platforms to process personal data that has been collected within Vietnam.

However, the requirement to conduct a PDTIA does not apply in the following cases:

(a) Cross-border transfers of personal data by competent state authorities;

(b) Storage of employee personal data by organisations or agencies on cloud computing services;

(c) Personal data transferred across borders by the data subject themselves; and

(d) Other exemptions as prescribed by the Government.

(3) On another note, household businesses and micro-enterprises (except those engaged in personal data processing services, directly processing sensitive personal data, or handling data of a large number of data subjects) are exempt from the requirement to submit the Dossiers. Small enterprises and start-ups (with the same exceptions) may choose not to submit the Dossiers for a period of five years from the effective date of the PDPL.

(4) Additionally, any Dossiers submitted in accordance with Decree 13 and accepted by the authority prior to the effective date of the PDPL will remain valid and do not need to be resubmitted. However, any updates to those Dossiers which are made after the PDPL takes effect must comply with the requirements of the PDPL.

Procedure for the submission of the Dossiers

(5) The PDPL does not provide detailed provisions regarding the contents, conditions, or procedures for the preparation and submission of the Dossiers. These matters will be addressed explicitly in implementing regulations to be issued by the Government, which are expected to be promulgated before the effective date of the PDPL (01 January 2026).

4. Personal Data Protection Officer

(1) Unlike Decree 13, which only required the appointment of a Data Protection Officer (**DPO**) in limited circumstances, the PDPL expands this obligation significantly. Under the PDPL, all entities that process personal data, whether sensitive or basic, are required to designate a DPO. The DPO plays a central role in supervising data processing activities, ensuring compliance with applicable legal requirements, and serving as a point of contact for both the competent authorities and data subjects.

(2) The PDPL provides flexibility in how entities may appoint their DPO. Specifically, organisations may either assign the role to the qualified internal personnel or engage third-party service providers that specialise in data protection services. However, any individual or entity appointed must satisfy criteria, which are expected to be clarified in forthcoming implementing regulations issued by the Government.

5. Personal Data Protection in Certain Activities

(1) **Data Protection for Vulnerable Individuals**: Organisations must implement safeguards when handling personal data of vulnerable individuals (e.g., children or persons with limited capacity), obtain dual consent for children aged 7 and above, and cease processing upon consent withdrawal or authority request.

(2) **Data Protection in Employment**: Employers may only collect necessary data during recruitment and must delete it if not retained. During employment, employee data must be managed lawfully and securely, with transparent use of monitoring technologies.

(3) **Data Protection in Health and Insurance**: Entities handling health and insurance-related data must obtain explicit consent and comply with all regulations for sensitive data. Such data may not be shared with third parties unless clearly authorised.

(4) **Data Protection in Banking and Finance**: Entities must protect sensitive information, notify individuals of breaches, and avoid profiling without consent. Only essential data from lawful sources may be collected.

(5) **Data Protection in Advertising and Marketing**: Advertisers are limited to using personal data with consent and must clearly inform individuals of methods, frequency, and opt-out options. Subcontracting full advertising services involving personal data is prohibited.

(6) **Data Protection for Social Media and Online Platforms**: Social media and online platforms must disclose data collection practices, offer privacy controls, and obtain consent for cookies, location tracking, and surveillance.

(7) **Data Protection in AI, Blockchain and Cloud Computing**: Organisations using emerging technologies like AI, blockchain, and cloud computing must ensure purpose limitation, integrate appropriate safeguards, and assess risk.

(8) **Data Protection in Emerging Technologies and Special Data Categories**: Biometric and location data processing requires informed consent, access restrictions, and user opt-outs. Public recordings are permitted without consent only in narrow cases (e.g. national security) and must be disclosed, limited in use, and subject to deletion policies.

6. Conclusion

The PDPL represents a pivotal advancement in Vietnam's data protection regime, building upon the foundation of Decree 13 while introducing more comprehensive and sector-specific obligations. The law imposes comprehensive compliance obligations on both domestic and foreign entities, especially those acting as Data Controllers, Data Processors, or Data Controlling

and Processing Entities. Entities must pay close attention to consent requirements, impact assessments, and breach notification protocols, while anticipating further clarity from forthcoming implementing regulations.

To ensure readiness ahead of the PDPL's effective date on 01 January 2026, organisations should proactively assess their data processing activities, update internal governance frameworks, and implement robust compliance measures aligned with the new regime.

Key contacts

If you have any questions or would like to know how this might affect your business, please contact the key contacts.

Nguyen Viet Ha
Partner
Head of Technology, Media and telecoms
Hanoi, Vietnam
+84 24 3971 0888
ha.nguyen@lexcommvn.com

Hoang Le Quan
Senior Associate
Hanoi, Vietnam
+84 24 3971 0888
quan.hoang@lexcommvn.com

Tran Quang Long
Junior Associate
Hanoi, Vietnam
+84 24 3971 0888
long.tran@lexcommvn.com

Legal notice

The contents of this publication, current at the date of publication set out above, are for reference purposes only. They do not constitute legal advice and should not be relied upon by any party for any purpose.