DILINH LEGAL

DECREE 356/2025/ND-CP ON PERSONAL DATA PROTECTION

Michael K. Lee and Trang Nguyen

February 2026 https://dilinh.com/

On December 31, 2025, the Government of Vietnam issued Decree No. 356/2025/ND-CP ("**Decree 356**"), guiding the implementation of the Law on Personal Data Protection 2025 ("**PDPL**").

Effective immediately as of January 1, 2026, Decree 356 replaces the previous Decree No. 13/2023/ND-CP. This new regulation establishes a rigorous, comprehensive framework for personal data protection in Vietnam, introducing stricter governance standards, expanded data definitions, and enhanced enforcement mechanisms.

This alert provides an overview of the key aspects of Decree 356 that are most relevant to businesses.

Subjects of application

Under Decree 356, the personal data protection framework applies to Vietnamese agencies, organizations, and individuals, as well as to foreign agencies, organizations, and individuals operating in Vietnam. In addition, Decree 356 applies to foreign agencies, organizations, and individuals that directly participate in or are otherwise involved in the processing of personal data of Vietnamese citizens, and to persons of Vietnamese origin whose nationality has not yet been determined who are residing in Vietnam and have been issued a citizen identification certificate.

Similar to the PDPL, Decree 356 confirms Vietnam's broad and extraterritorial approach to personal data protection, meaning that overseas entities may still be subject to Vietnamese data protection obligations where their activities relate to individuals in Vietnam.

Types of data covered by Decree 356

Under the PDPL, personal data is defined as information associated with or capable of identifying a specific individual, and is classified into two main categories: (a) basic personal data and (b) sensitive personal data. The PDPL sets out the conceptual distinction between these two categories and expressly authorizes the Government to provide detailed guidance on their contents.

Decree 356 implements this mandate by providing more detailed and operational lists of both basic and sensitive personal data:

(a) "**Basic Personal Data**" consists of: (i) family name, middle name, and first name as stated in the birth certificate, and other names (if any) of a person; (ii) date of birth; date of death or disappearance; (iii) gender; (iv) place of birth, place of birth registration, place of permanent, temporary or current residence, hometown, contact address; (v) nationality; (vi) personal image; (vii) phone number; personal identification number, passport number, driver's license number, license plate number; (viii) marital status, (ix) information of familial ties (parents, children, spouses); (x) digital account; and (xi) *other information associated with a specific person or helping identify a particular person that is not sensitive personal data.*

(b) "**Sensitive Personal Data**" means personal data associated with an individual's privacy that, "*when being infringed upon, shall cause a direct effect on the legitimate rights and interests of agencies, organizations, and individuals,*" including: (i) data that reveals racial, ethnic origin; (ii) political, religious and belief views; (iii) information on private life, personal secrets, family secrets; (iv) health condition; (v) genetic and biometric data; (vi) sex life or sexual orientation; (vii) crime records; an individual's location; electronic identification account's usernames and passwords; images of identity documents; (viii) bank accounts' usernames and passwords, bank card information and transaction history, financial and credit information, and information on activities and financial, credit, securities and insurance transactions history at relevant licensed organizations; (ix) data monitoring behavior or use of telecommunications, social media, online communication services, and other cyberspace services; and (x) other personal data required by law to be kept confidential or subject to strict security measures.

Compared to the PDPL, Decree 356 does not alter the classification framework. Still, it significantly enhances legal certainty by clarifying the scope of each category, thereby enabling organizations to more accurately assess compliance obligations, particularly where stricter requirements apply to sensitive personal data.

Internal data protection officer and data protection department

The PDPL imposes a general obligation on organizations processing personal data to implement appropriate organizational and personnel measures to protect personal data, including assigning data protection responsibilities within the organization. However, the PDPL does not provide detailed regulations on such matters.

Decree 356 supplements the PDPL by introducing new provisions for the appointment of personal data protection officers or the establishment of personal data protection departmentswithin the organization. Such appointment or establishment must be through a formal decision defining the functions, duties, and authority of such officers or departments. Additionally, such officers and personnels within the departments must meet all of the following requirements: (i) graduated college or above; (ii) have at least two (02) years of relevant work experience (after graduation) in either inhouse legal counsel, information technology, cybersecurity, data security, risk management, compliance, human resource management, or personnel management fields; and (iii) has received training and professional development in legal knowledge and specialized skills related to personal data protection. These provisions transform the PDPL's general governance requirement into a clearly enforceable internal compliance obligation.

Decree 356 also provides limited transitional and exemption mechanisms. Within five (05) years from January 01 2026, small enterprises, start-ups, household businesses, and micro-enterprises are not required to appoint a personal data protection officer or establish a data protection department, unless they either (i) provide personal data processing services, (ii) directly process sensitive personal data, or (iii) process personal data relating to 100,000 or more data subjects, based on the cumulative volume of personal data processed.

For classification purposes, a micro-enterprise is an enterprise employing no more than ten (10) employees participating in social insurance on an annual average basis and meets one of the following revenue criteria:

- For enterprises operating in the agriculture, forestry, fishery, industry, and construction sectors, the total annual revenue must not exceed VND 3 billion, or the total capital must not exceed VND 3 billion.

- For enterprises operating in the trade and services sector, the total annual revenue must not exceed VND 10 billion, or the total capital must not exceed VND 3 billion.

A small enterprise is an enterprise that does not qualify as a micro-enterprise and meets one of the following employee and revenue thresholds:

- For enterprises operating in the agriculture, forestry, fishery, industry, and construction sectors, the number of employees participating in social insurance on an annual average basis must not exceed one hundred (100), and the total annual revenue must not exceed VND 50 billion, or the total capital must not exceed VND 20 billion.

- For enterprises operating in the trade and services sector, the number of employees participating in social insurance on an annual average basis must not exceed fifty (50), and the total annual revenue must not exceed VND 100 billion, or the total capital must not exceed VND 50 billion.

Although Vietnamese law does not provide a statutory definition of a "start-up," it does define an "innovative start-up enterprise." An innovative start-up enterprise is an enterprise that implements innovative business models and demonstrates the capacity for rapid growth and market expansion through the effective exploitation of technology, intellectual property, breakthrough ideas, or new business models.

Individuals and organizations providing personal data protection services

While the PDPL recognizes that personal data protection activities may be outsourced to third-party service providers, it does not comprehensively regulate the qualifications, responsibilities, or operating conditions of such parties.

Decree 356 addresses this gap by providing detailed regulations regarding both individuals and organizations providing personal data protection services, such as provisions on qualification requirements, professional standards, statutory responsibilities, disclosure requirements, and compliance with relevant laws when accessing or processing personal data, maintaining confidentiality, and deleting or destroying personal data upon completion of services.

Data Processing Impact Assessment (DPIA)

Data controllers and combined controller-processors are required to prepare, retain, and submit a Data Processing Impact Assessment (DPIA) dossier to the authority *within sixty (60) days from the first day of personal data processing*. Processors may prepare and maintain a DPIA file in accordance with their contractual arrangements with the controller.

A DPIA dossier is mainly composed of:

- Impact Assessment Report (statutory form).

- A contract or an agreement between parties that outlines the responsibilities related to personal data processing.

- Data Protection Policies & Procedures: Include policies, procedures, forms, and other relevant documents that address data protection measures within the organization.

The details of the Impact Assessment Report include:

- Contact Information: Include the contact details of all parties involved, including the data controllers, data processors, and third parties.

- Data Protection Officer/Department/Service Provider: Include the contact details of the data protection officer/department and service provider (if any) of the data controller, data processor, and third parties.

- Purpose of Data Processing: Provide a clear explanation of the purpose of personal data processing, the types of data processed, data handling activities, and data flow diagrams.

- Consent and Data Management: Describe how consent is obtained from data subjects, along with data retention, deletion, and destruction policies.

- Data Security Measures: Outline security measures, protection protocols, system design diagrams, and data protection standards applied.

- Compliance Evaluation: Provide an assessment of compliance with personal data protection regulations.

- Risk Assessment: Evaluate the impacts and risks of personal data processing, including potential adverse consequences and mitigation strategies.

A DPIA is completed once for the entire duration of the organization's operations, but must be updated in accordance with the law. The licensing authority will review and respond within fifteen (15) days; incomplete dossiers must be corrected within thirty (30) days. Under the statutory requirements, updates must be made periodically every six (06) months when changes to the purpose, data controllers and/or processors, third parties occur, or within ten (10) days in specific scenarios such as organizational restructuring, changes in operational status (termination, dissolution, bankruptcy), changes in data-protection service providers, or changes regarding business lines relevant to personal data processing.

Cross-Border Data Transfer Impact Assessment (CBTIA)

A CBTIA is required whenever Vietnam-originated personal data is transferred abroad or processed using an overseas platform. Businesses must file this assessment *within sixty (60) days from the first transfer*. Similar to DPIA, businesses will only need to complete the CBTIA once during the entire course of operation, but it must be updated whenever there is a relevant change, as explained above. This framework ensures visibility and control over outbound data flows. The licensing authority will review and respond within fifteen (15) days; incomplete dossiers must be corrected within thirty (30) days. Dossier must be updated and supplemented in accordance with regulatory requirements.

A CBTIA dossier is mainly composed of:

- Cross-border data transfer impact assessment report (statutory form).

- Copies of contracts or data transfer agreements defining the responsibilities of the transferring and receiving parties.

- Internal policies, procedures, regulations, forms, and related documents on personal data protection.

Details in the Cross-Border Data Transfer Impact Assessment Report include:

- Contact Information: Details of the data transferring party, data receiving party, data processors, and other relevant parties involved in the cross-border data transfer.

- Data Protection Contacts: Contact details of the data protection department/officer and data protection service providers (if any).

- Purpose and Scope of Transfer: Description and justification of the purpose of cross-border data transfer, categories of personal data transferred, processing activities, and data flow diagrams.

- Consent and Data Management: Explanation of consent mechanisms and policies for data storage, retention, deletion, and destruction.

- Data Security Measures: Safeguards and security measures applied after cross-border transfer, including applicable data protection standards.

- System Architecture and Functions: System diagrams and description of storage and processing systems used by the data receiving party.

- Onward Transfer Procedures: Processes governing the transfer or sharing of personal data by the receiving party to third parties.

- Compliance Assessment: Results of self-assessment on compliance with personal data protection regulations.

- Risk and Impact Assessment: Assessment of the data recipient's level of data protection, potential risks and impacts of cross-border transfer and processing, possible adverse consequences, damages, and mitigation measures.

Notice and handling of incidents

Decree 356 clarifies the obligation to notify personal data breach incidents by specifying notification requirements applicable to different sectors and types of data processing activities. Notwithstanding sector-specific clarifications, as a general rule, organizations must notify the competent authority of a personal data breach within seventy-two (72) hours of detecting the incident.

In addition to notification, organizations are required to promptly implement measures to contain and mitigate the incident, apply remedial actions to prevent recurrence, and maintain records documenting the incident, its causes, and the handling measures taken, in accordance with the PDPL and Decree 356.

The impact of Decree 356 on businesses

Decree 356 clarifies and strengthens the PDPL's data protection obligations. It requires businesses to follow clearer procedures on reporting, record-keeping, and internal governance, including maintaining compliance dossiers, appointing data protection personnel where needed, and complying with specific notification timelines - most notably the 72-hour requirement for reporting data incidents in most cases.

In practice, Decree 356 increases day-to-day compliance obligations for businesses, especially those processing large volumes of personal data or operating across borders.

Please get in touch with Diep Hoang at **diep.hoang@dilinh.com** and Michael Lee at **michael.lee@dilinh.com** for more information.

CONTACT

Dilinh Legal
1F 139 Hai Ba Trung Street,
Xuan Hoa Ward, Ho Chi Minh City,
Vietnam
https://dilinh.com/
contact@dilinh.com

(Dee) Diep Hoang
Partner
M: [+84] 947 406 026
diep.hoang@dilinh.com

Michael K. Lee
Partner
M: [+84] 902 727 935
michael.lee@dilinh.com