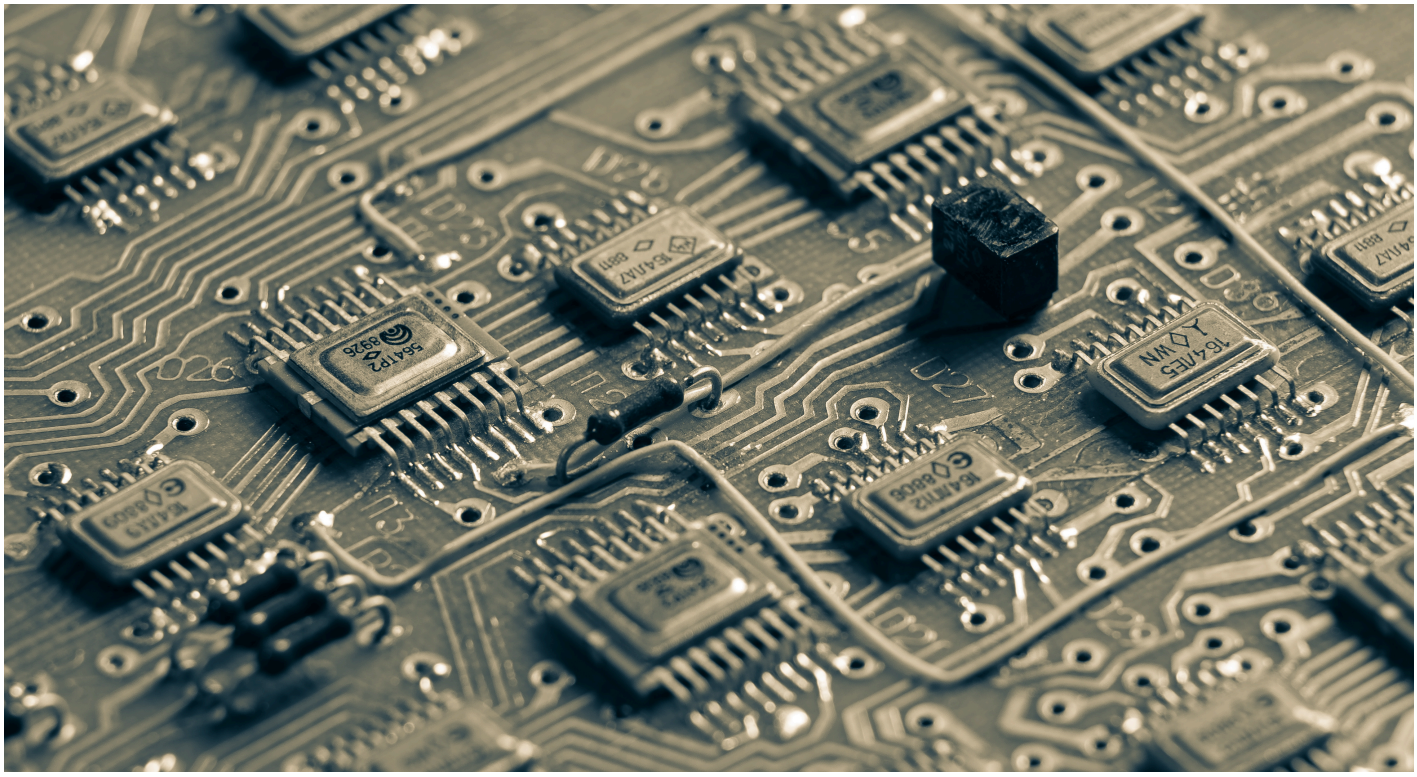
DILINH LEGAL

Law on Personal Data Protection No. 91/2025/QH15

By Michael Lee, Trang Nguyen, and Le Pham

August 2025 https://dilinh.com/



On June 26, 2025, Vietnam's National Assembly passed the Law on Personal Data Protection No. 91/2025/QH15, effective January 1, 2026 ("**PDPL**"). The PDPL will replace Decree No. 13/2023/ND-CP on Personal Data Protection (PDPD). The PDPL establishes a more comprehensive and detailed framework for data protection, building on and expanding the provisions of PDPD. It introduces new concepts, exemptions, and obligations, while retaining key compliance requirements such as data processing principles, cross-border data transfer regulations, and the need for Data Processing Impact Assessments (DPIAs) and Outbound Transfer Impact Assessments (OTIAs).

Below are its key provisions, simplified for clarity:

Scope of Application

The PDPL applies to domestic entities, organizations, and individuals, as well as foreign entities in Vietnam or those directly engaged or involved in processing personal data of *Vietnamese citizens or individuals of Vietnamese origin* without a determined nationality residing in Vietnam, provided they have an identity card. PDPL has narrowed its scope of application concerning foreign actors. Under PDPD, "foreign agencies, organizations, and individuals directly participating in or related to personal data processing activities in Vietnam," irrespective of the nationality of the person's data, were subject to it.

Definition of Personal Data

Personal data now includes any information—digital or otherwise—that identifies an individual, expanding beyond PDPD's focus on electronic formats. It explicitly excludes anonymized data, encouraging its use to reduce compliance risks.

Categories of Personal Data

The PDPL classifies personal data into:

Basic: Common identity and background information frequently used in transactions and social interactions, defined by a government list.

Sensitive: personal data associated with individuals' privacy rights that, if breached, harms rights, also defined by a government list.

Prohibited Acts

Beyond PDPD's bans (e.g., misusing data, threatening national security), the PDPL prohibits:

1. Using others' data or allowing others to use their data for illegal acts.

2. Buying/selling personal data, except where legally permitted.

3. Appropriating, intentionally disclosing, or causing loss of personal data.

Significant Penalties for Violations

Buying/selling data: Fines up to 10 times transaction revenue or VND 3 billion, whichever is greater.

Cross-border data transfer violations: Fines up to 5% of preceding-year revenue or VND 3 billion, whichever is greater.

Other violations: Up to VND 3 billion.

These penalty caps apply to organizations (50% for individuals).

Processing Without Consent

Personal data can be processed without consent for:

1. To safeguard life, health, dignity, lawful rights, or legitimate interests of the data subjects, others, or the State against infringement.

2. To respond to emergencies or threats to national security, and to prevent riots, terrorism, crime, or legal violations.

3. Fulfilling state duties.

4. Fulfilling contractual obligations.

5. Other cases as provided by sector-specific legal provisions

Organizations must establish data processing policies, apply appropriate data protection measures, conduct risk assessments, perform audits, and handle complaints.

Data Breach Reporting

Data controllers, data controller-cum-processors, and third parties must notify the Ministry of Public Security within 72 hours of *detecting* breaches that affect security or the rights of individuals. Processors must also inform controllers/controller-cum-processors promptly.

Data Protection Officer/Department

Companies must appoint internal data protection staff/departments or hire external services, offering more flexibility than PDPD.

Cross-Border Data Transfers

Overseas data transfer impact assessments (OTIAs) require updates every six months for any changes or immediately for major changes (e.g., restructuring, bankruptcy, changes in data protection service providers, or new services). Exemptions include state agencies, cloud-stored employee data, and individuals transferring their data.

Data Processing Impact Assessment (DPIA)

DPIAs are required once per organization's term, updated every six months upon any changes or immediately for significant changes (e.g., restructuring, bankruptcy, changes in data protection service providers, and new business lines/services involving personal data processing).

Transition Rules

Small enterprises and startups are exempt from DPIAs, OTIAs, and appointing data protection staff for five years, unless they are processing sensitive data, providing data services, or handling large datasets. Household businesses and micro-enterprises have similar exemptions.

Sector-Specific Rules

Children/Vulnerable Persons: Legal representatives manage data rights. For children aged seven and above, both the child's consent and the representative's consent are required for the collection and use of private data.

Employment: Recruiters must limit data use to hiring purposes, delete data of applicants not hired, and comply with applicable labor laws.

Health/Insurance: Consent is required for data use, except in specific cases; health apps and reinsurance must follow strict rules.

Finance/Banking: Consent is needed for credit scoring; breaches must be reported.

Advertising: Providers need consent, must offer opt-outs, and cannot fully outsource data services.

Social Media: Platforms must disclose data use, avoid unauthorized collection, provide privacy controls like "Do Not Track", and refrain from eavesdropping, wiretapping, recording phone calls, or reading text messages without the data subject's consent, unless otherwise permitted by law.

Big Data/AI/Blockchain: Processing must be secure, lawful, and include risk-based protection.

Location/Biometric Data: Consent is required for tracking, and biometric data must be protected with strict security measures.

Public Recordings: Audio/video recordings in public spaces can be used without consent for security or public events purposes, but must be deleted after use and respect the rights of individuals.

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