



PERSONAL DATA PROTECTION LAW

| Overview

- The new Personal Data Protection Law (PDPL) of Vietnam has been enacted on 26 June 2025 as Law No. 91/2025/QH15. The law retains the core principles and intent of the earlier Personal Data Protection Decree (Decree 13), while introducing more detailed and prescriptive requirements.
- What's particularly notable is that, unlike the technology-neutral approach of the GDPR and other international frameworks, the PDPL introduces sector-specific provisions – likely aimed at facilitating compliance in data-intensive industries. This approach makes sense in the context of Vietnam, where data privacy remains a relatively new concept and many industries have expressed concerns about the challenges of applying Decree 13 to their specific operational practices.
- Key elements, such as the classification of basic and sensitive personal data and the procedures for conducting data protection impact assessments, will be further clarified in an upcoming government decree, which may significantly amend current provisions of Decree 13.
- A key development is the introduction of exemptions for SMEs, reflecting a more pragmatic shift from Decree 13's broad, uniform application. The data breach notification requirement has also been narrowed to cases involving serious harm, aligning more closely with the GDPR. Importantly, the law exempts entities already subject to the Personal Data Processing Impact Assessment and Cross-Border Data Transfer Impact Assessment under the PDPL from duplicative obligations under the Law on Data – another regulation overseen by the Ministry of Public Security. This exemption demonstrates the government's responsiveness to business feedback and its effort to reduce administrative burdens.
- Despite these flexibilities, the PDPL adopts a stricter overall posture. Consent remains the primary lawful basis for processing and is emphasized across sector-specific and high-risk activities. Processing under other lawful bases must be subject to monitoring mechanisms. Processing based on 'legitimate interest' is not permitted under the current framework. The sale of personal data is still strictly prohibited, with penalties of up to 10 times the revenue derived from such activity. Other violations may result in fines of up to 5% of revenue for cross-border data transfer breaches, or up to VND 3 billion for general non-compliance.

Governing Scope (PDPL vs. Decree 13)

Domestic application: PDPL clarifies it applies to:

- Vietnamese entities and individuals, regardless of where they operate.
- Foreign entities and individuals physically present or based in Vietnam.

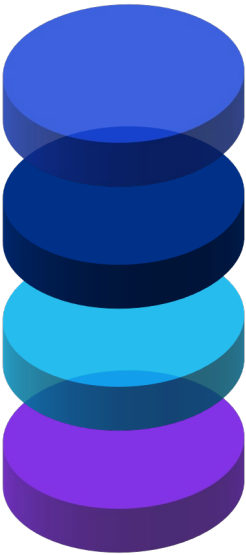
Extraterritorial application: It also narrows extraterritorial scope to data processing involving:

- Vietnamese citizens, or
- Residents in Vietnam with official identification.

Matters awaiting further regulatory guidance from the government

01	Categories of basic personal data	10	Notification content for data breaches
02	Categories of sensitive personal data	11	Personal data protection in finance, banking, and credit information activities
03	Data subjects' rights and responsibilities	12	Personal data protection in activities Involving frontiers technologies
04	Fine calculation based on revenue from violations	13	Notification on biometric data processing causing harm to data subjects
05	Consent format	14	Qualifications and duties for personal data protection departments/personnel
06	Compliance requirements for personal data transfers	15	Standards for data protection and processing services
07	Compliance in cross-border transfer of personal data	16	Inspection procedures for data protection activities
08	Personal data processing impact assessment	17	Compliance support for SMEs, start-ups & micro-businesses
09	Updates of personal data processing and transfer impact assessment records		

Law Application



Territorial Scope

PDPL applies to personal data activities **within** Vietnam.

Earlier Laws

Pre-PDPL laws remain valid if consistent with PDPL principles.

New Laws

Post-PDPL laws must state any deviations from the PDPL.

Impact Assessment Exemption

- ✓ Entities that have already conducted impact assessments in compliance with the PDPL are **not required** to repeat these assessments under the Data Law.
- ✓ Assessments submitted under Decree 13 remain **valid** but must be updated in line with the PDPL.

| **Personal Data Protection Principles**

Removed (but implicitly included in obligations throughout the Law)

Individuality
Data subjects shall be made aware of any operation relating to the processing of their personal data.

Compliance & Accountability
Data handlers shall be responsible for complying with the principles of data processing

Retained and Updated

Lawfulness
Processed in accordance with the **Constitution and relevant laws**

Purpose Limitation
Processed only for **specific and explicit purposes**

Data Minimization
Collect and process personal data appropriate to the scope and purpose of processing

Data Quality
Ensure accuracy, edited, updated and supplemented when necessary

Storage Limitation
Stored for a period appropriate to the purpose of personal data processing

Security & Confidentiality
Implementing appropriate **institutional, technical, and human** measures

New

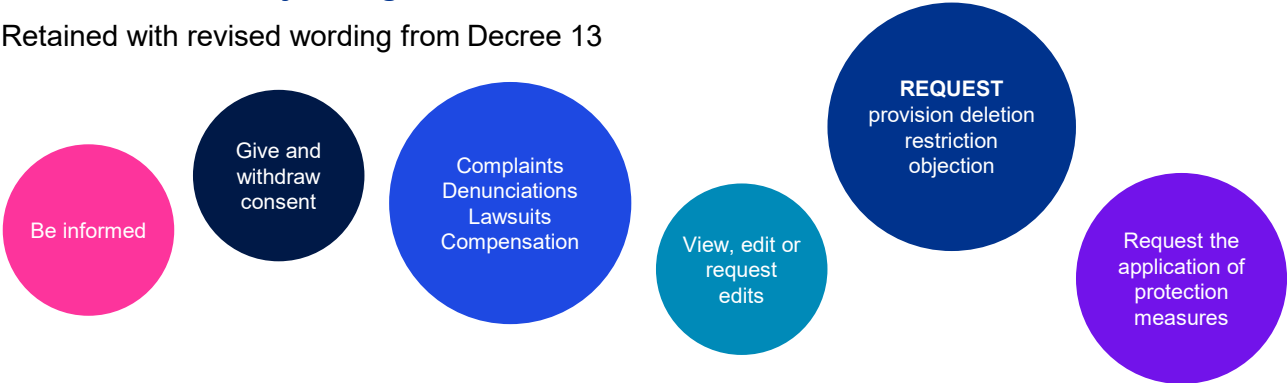
Violation Prevention and Handling
Proactive measures and stringent enforcement against all violations

National Interest and Balancing Rights
Concerning national and ethnic interests, socio-economic development, national defense, security, and foreign affairs

Harmony between personal data protection and the protection of **legitimate rights and interests of others**

| **Personal Data Subject Rights**

Retained with revised wording from Decree 13



| **Principles when implementing Personal Data Subject Rights**

Retained with revised wording from Decree 13

COMPLY with the law and **contractual obligations**
FOR protection of that personal data subject legitimate rights and interests

NOT

Hinder or impede the **legal rights and obligations** of controller, controller cum processor, processor
Infringe the **lawful rights and interests** of the State, agencies, organizations, or other individuals




Consent Exemptions



Mandatory Monitor Mechanisms



Special Handlings

Public recordings 	No consent required in case: (i) protect national security, social order, lawful rights and interests of entities and individuals (ii) public activities (conferences, seminars, competitions, performances)
Location data 	Location tracking using RFID or similar technologies requires consent from the data subject or a legal mandate. Mobile platforms must inform users about the use of location data, implement safeguards to prevent unauthorized third-party access, and offer
Biometric data 	Apply physical security measures, restrict access, monitoring system and notify PD subject in case of damage.

Impact Assessment Dossiers

Processing impact Assessment

- Mandatory for Controller and Controller-cum-Processor
- Processor conducts on contractual basis

Cross-border Transfer impact Assessment

Applied when:

- (i) Data **stored in Vietnam** transfer to data **storage outside** of Vietnam
- (ii) Entities or individuals **in Vietnam transfer** data **to foreign** entities or individuals
- (iii) Data **collected in Vietnam** is **processed on platforms located outside** of Vietnam

UPDATE

- ✓ **Immediately**, for: (i) restructuring; (ii) change in PD protection service providers; or (iii) change in PD processing services
- ✓ **Biannual**, for other cases

| New Sectoral Requirements

Employment

(Article 25)

Healthcare & Insurance

(Article 26)

Banking & Finance

(Article 27)

Advertisement

(Article 28)

Social Media & OTT

(Article 29)

Frontier Technologies

(Article 30)

I. Employment (Article 25)

01. Recruitment

- Consent is **mandatory**
- **ONLY** request information serving recruitment purpose and other *agreed purposes*
- Delete or destroy data if the applicant is **NOT** recruited, *unless otherwise agreed*.

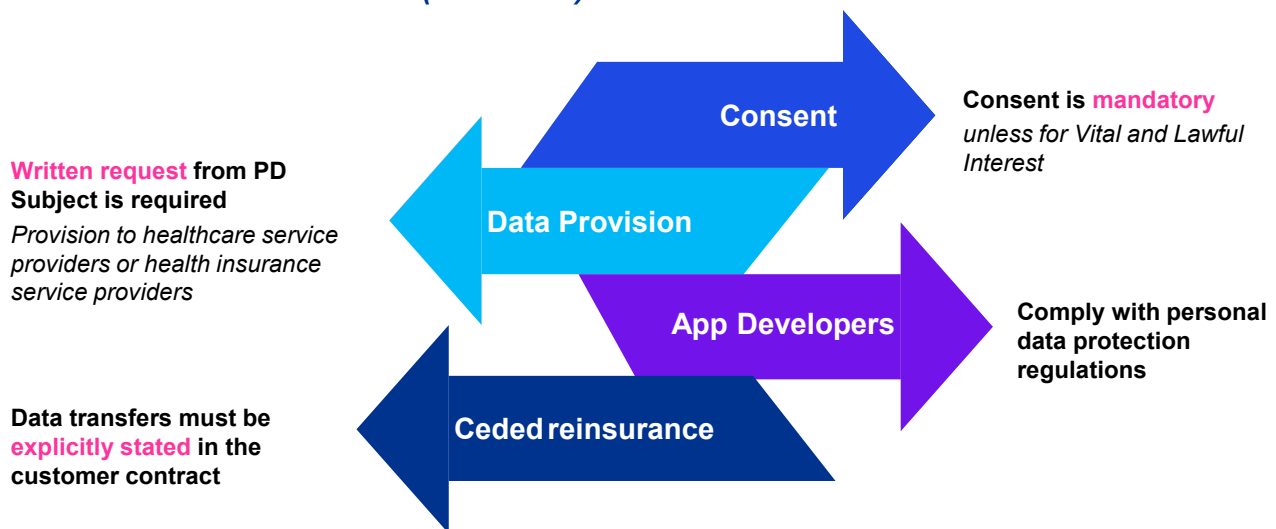
02. Employment

- PDPL, Labor Law, Occupation Law, Data Law and other relevant laws
- Store for a regulatory terms or *agreed terms*
- Delete or destroy data upon termination, *unless otherwise agreed* or specified by laws

03. Technology Application

- Process for employee protection and **informed basis**
- **PROHIBIT** processing data collected from illegal technologies.
- Cloud storage of employee data does **NOT** necessitate a cross-border transfer impact assessment – Art 20.6(b)

II. Healthcare & Insurance (Article 26)



III. Banking & Finance (Article 27)

Banking & Finance Organizations

- ✓ Consent is **mandatory** for **credit scoring**
- ✓ **Notify** PD Subject in case information loss of bank account, finance, credit, credit information
- ✓ Implement regulations on **sensitive personal data**, **security standards** in banking and finance regulations
- ✓ **ONLY** collect data for credit information from sources in accordance with relevant laws

Credit Information Organizations

- ✓ Apply measures **preventing** unauthorized access, use, alter personal data
- ✓ Measures for **restore loss data** is available
- ✓ Secure process during credit scoring

IV. Advertisement (Article 28)

Advertising Activities

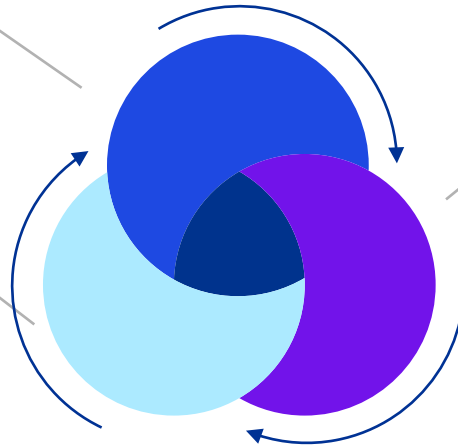
(in general)

Comply with anti-spam and advertising laws

Personalized advertising

(incl. behavioral, targeted and personalized advertising)

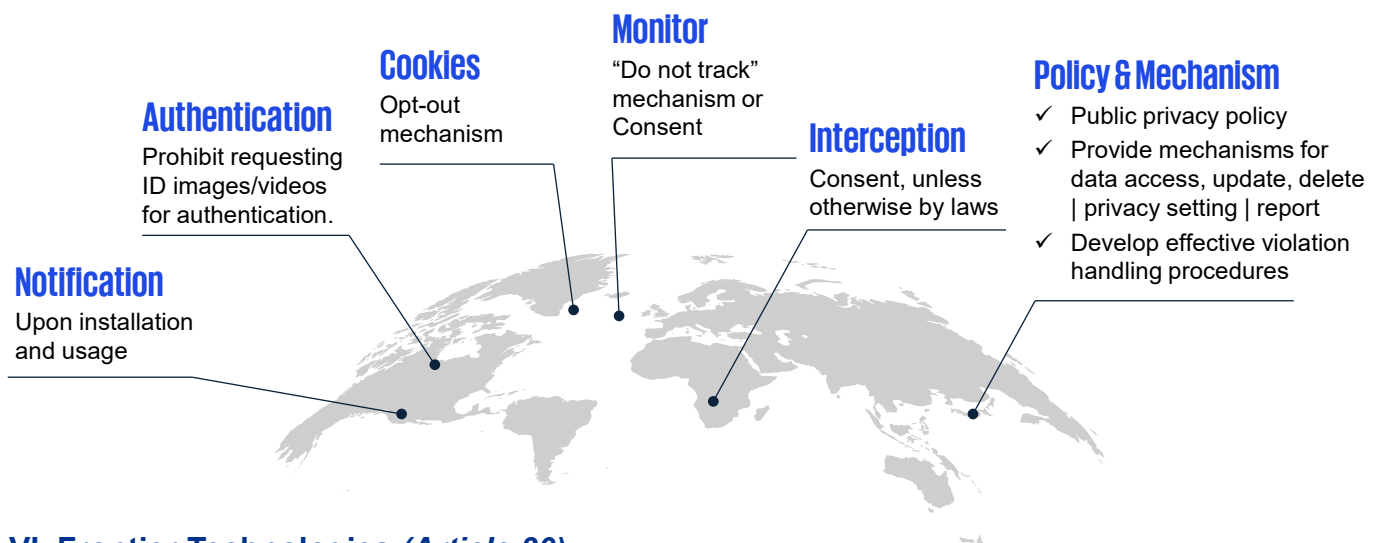
- ✓ Consent is **mandatory** for **web and app monitoring**
- ✓ Opt-out mechanism is required for data sharing
- ✓ Identify **retention period**
- ✓ **Delete or destroy** data when no longer necessary



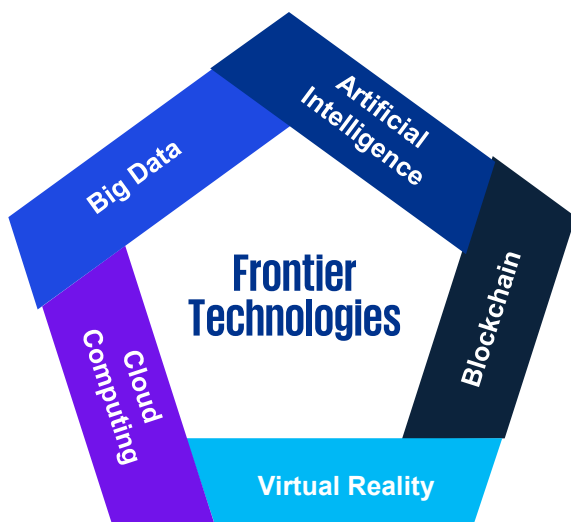
Advertising Services

- ✓ Consent is **mandatory** on **informed-basis** and provide **opt-out mechanism**
- ✓ **ONLY** process data receiving via agreement or collecting in doing business
- ✓ **Subcontract** the entire service is **NOT** allowed
- ✓ Service providers bear **the burden of proof**

V. Social Media & OTT (Article 29)



VI. Frontier Technologies (Article 30)



- ✓ Purpose limitation and necessity, ensure the **lawful rights and interest** of PD subject
- ✓ Comply with applicable laws, and align with **ethical standards and Vietnamese customs**.
- ✓ Built-in data security, authentication and controls
- ✓ **Risk-based protection** in AI
- ✓ **Prohibit** harmful usage against national security, public order, or individual well-being

Contact us

Hanoi

46th Floor, Keangnam Landmark 72,
E6 Pham Hung, Me Tri, Nam Tu Liem

T +84 (24) 3946 1600

Ho Chi Minh City

10th Floor, Sun Wah Tower,
115 Nguyen Hue, Ben Nghe, District 1

T +84 (28) 3821 9266

Da Nang

Unit D3, 5th Floor, Indochina Riverside Towers,
74 Bach Dang, Hai Chau I, Hai Chau

T +84 (236) 351 9051

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 KPMG Limited, KPMG Tax and Advisory Limited, KPMG Law Limited, KPMG Services Company Limited, all Vietnamese one member limited liability companies and member firms of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.



Scan to visit our website: kpmg.com.vn

Email: info@kpmg.com.vn