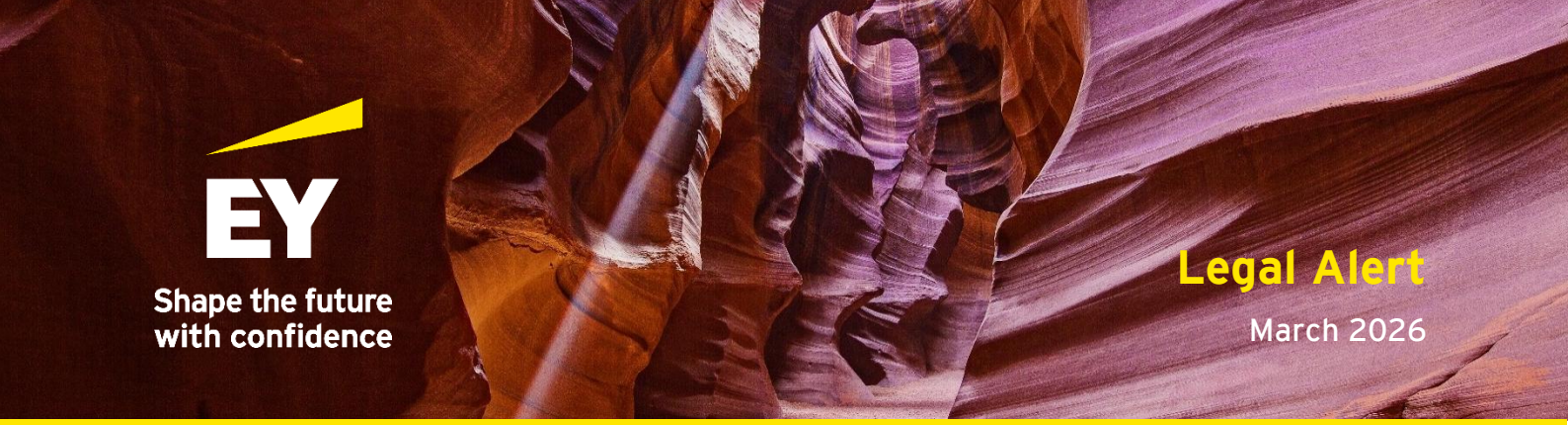


Visit other Alerts here.

Decree No. 356/2025/ND-CP providing detailed guidance for implementation of Personal Data Protection Law

This Alert highlights key compliance requirements set forth in the Decree No. 356/2025/ND-CP dated 31 December 2025 detailing several provisions and measures for implementation of the Personal Data Protection Law (Decree 356), through a comparative review with the Decree No. 13/2023/ND-CP dated 17 April 2023 (Decree 13) and an analysis of the implementing regulations of the Personal Data Protection Law (PDPL).

The PDPL officially took effect on 1 January 2026. The Government issued Decree 356 to provide detailed regulations on personal data protection requirements, as well as the forms and procedures for implementing the PDPL, marking a significant step toward shaping Vietnam's comprehensive data protection regime. Decree 356 replaced Decree 13 and also took effect on 1 January 2026.

Key highlights in Decree 356 include:

- Adjust the categories of basic personal data and sensitive personal data
- Tighten consent requirements
- Clarify the mechanisms and timelines for implementation of data subjects' rights
- Specify the cases and conditions for transfer of personal data
- Provide guidance on competency requirements and responsibilities of data protection officers and data protection departments
- Revise the mechanisms and templates for personal data processing impact assessment and cross-border transfer impact assessment
- Supplement requirements to notify data subjects in addition to notification of violations of personal data protection regulations
- Provide detailed guidance on inspections of personal data protection activities and cases of exemption
- Next course of action

1. List of basic personal data and sensitive personal data

In comparison with Decree 13, Decree 356 has adjusted the classification of personal data.

Data groups	Key updates
Basic personal data	▪ Removing from this basic personal data group: data reflecting activities, activity history in cyberspace; personal tax identification number, social insurance number, health insurance card number
Sensitive personal data	▪ Expanded scope: supplementation of behavior tracking data, usage data of telecommunications services, social networks, online media services, and other services in cyberspace ▪ Broader definition of health information: general definition as "health status", not limited to medical records ▪ Additional and more detailed items: usernames and passwords of electronic identification accounts; images on identity card/citizen cards; bank account information, banking card information, financial transaction history

2. Consent of data subjects

Decree 356 has tightened the requirements for data subjects' consent compared to Decree 13:

- Clear and verifiable consent: consent must be retained, ensuring the ability to verify the timing and content of consent
- Prohibition of default or misleading settings: consent must not be pre-set by default, or no unclear instructions may be created that could confuse data subjects

Beyond the traditional forms recognized under Decree 13, Decree 356 has broadened acceptable forms of valid consent in line with practical reality, such as consent obtained via telephone calls, email, websites, platforms, or applications with technical settings of consent.

3. Implementation of data subject rights

Based on the personal data subject rights provided under the PDPL, Decree 356 sets out specific mechanisms and timelines for the implementation of each group of rights. Accordingly, data controllers and data controllers cum processors must establish clear procedures, processes, and templates to ensure that data subjects can exercise their rights within the prescribed time limits:

Requirements	Response timeframe	Implementation timeframe	Timeframe if coordination with processors/third parties is needed	Extension
Withdrawal of consent/restriction/objection to processing	Two working days	15 days	20 days	One time, maximum 15 days
View/correction or request correction/data provision		10 days	15 days	One time, maximum 10 days

Requirements	Response timeframe	Implementation timeframe	Timeframe if coordination with processors/third parties is needed	Extension
Deletion		20 days	30 days	One time, maximum 20 days
Implementation of measures, solutions for personal data protection		15 days	Not applicable	One time, maximum 15 days

4. Transfer of personal data

In comparison with Decree 13 which previously set out only general provisions on data transfer that were scattered across various articles, Decree 356 has articulated specific conditions and requirements applicable to each case of data transfer:

Case of data transfer	Key conditions and requirements
Transfer based on consent or in cases of restructuring, reorganization, or transfers from data controllers to processors/third parties	▪ To have an agreement with the receiving party clearly specifying purpose, data subjects, data types, processing duration, deletion, legal basis, and responsibilities of parties
Transfer of sensitive personal data	▪ To apply physical security measures ▪ To encrypt, anonymize, or apply other security measures during the transfer
Transfer involving fees	▪ To obtain accurate and clear consent for each transfer ▪ To have an agreement before the data is transferred
Internal transfer within the same organization	▪ To establish control process for sharing and using data and prevent unauthorized disclosure
Data marketplace transactions	▪ Data must be de-identified before the transaction

5. Data protection officer (DPO) or data protection department (DPD)

Decree 356 clarifies that enterprises may adopt a combined approach by appointing an internal DPO/establishing an internal DPD and engaging external organizations or individuals to provide personal data protection services.

Compared to Decree 13 which only set out general obligations regarding the appointment of a DPO and the establishment of a DPD, Decree 356 takes an additional step by establishing specific competency standards and responsibilities for DPOs, DPDs, individuals and organizations providing personal data protection services as follows:

Subject	Competency requirements	Responsibilities
Internal DPO	▪ College degree or higher ▪ At least **two years** of experience relating to: legal affairs, information technology, cybersecurity, data security, risk management, compliance control, **human resources management, organizational personnel** ▪ Trained in personal data protection	▪ Conducting periodic compliance assessments ▪ Developing and implementing policies, procedures, and technical measures ▪ Implementing data subjects' rights ▪ Responding to violations and preparing impact assessment dossiers ▪ Participating in training
Internal DPD	Personnel in the DPD must meet the same competency standards as internal DPO	Same as internal DPO
Individuals providing personal data protection services	▪ College degree or higher ▪ At least **three years** of experience in one of the following areas: legal affairs, **personal data processing**, cybersecurity, data security, risk management, compliance control ▪ **In-depth** training in data protection ▪ Same as internal DPO	▪ Performing the scope of services as agreed ▪ Not taking advantage of the provision of services to engage in any unlawful acts ▪ Deleting, destroying personal data after the contract has been fulfilled and in accordance with the laws
Organizations providing personal data protection services	▪ Operating in the fields of technology, legal services, or consulting in technology or legal matters ▪ Having at least three personnel who meet the competency standards required for individuals providing personal data protection services ▪ Previously having provided products or services related to information security, cybersecurity, information technology, standards assessment, personal data protection consulting ▪ Must prepare capability documentation demonstrating competence in personal data protection	Same as individuals providing personal data protection services

6. Data processing impact assessment (DPIA) and cross-border transfer impact assessment (CTIA)

Decree 356 introduces a notable CTIA exemption of "cross-border transfer of personal data for cross-border personnel management in accordance with labor rules, policies and collective labor agreements as prescribed by law". This provision helps reduce compliance burdens for multinational companies that manage employee data across multiple countries.

On the other hand, for CTIA and DPIA dossier, Decree 356 imposes more stringent requirements compared to Decree 13:

Category	Decree 13	Decree 356
Assessment mechanism	Ex-post review mechanism	Ex-ante mechanism, requiring dossiers to be reviewed and approved by the Department of Cybersecurity and High-Tech Crime Prevention and Control (A05), the Ministry of Public Security.
Dossier components	▪ DPIA and CTIA reports ▪ Contract on personal data processing	Adding internal policies, procedures, regulations, and templates on personal data protection in addition to all documents required under Decree 13
Impact assessment report	▪ Form No. 06, Decree 13; Forms No. D24-DLCN-01 or D24-DLCN-02 or D24-DLCN-03, D25-DLCN-04, Decision 4660/QD-BCA-A05 ▪ No requirement to delineate roles or provide a data-flow diagram.	▪ Forms No. 09 and No. 10, Decree 356 ▪ Clear delineation between activities performed in the role of data controller and activities performed in the role of data processor or third party, identify corresponding categories of data subjects and quantities ▪ Include a detailed data processing flow diagram for each role; plan for ensuring data security
Dossier processing duration	▪ Not applicable	▪ **15 days:** for A05 to evaluate and determine whether the dossier meets or does not meet the requirements ▪ **30 days:** for the enterprise to supplement and complete the dossier if it is incomplete or non-compliant. If the enterprise fails to do so, administrative sanctions may be imposed.
Update	▪ Update when changes arise, but no specific cases or deadlines for updates are provided	▪ **Periodic update every six months when:** (i) new purposes for transferring or processing data arise; or (ii) there are changes to the data controller, data controller cum processor, data processor, or third party. ▪ **Immediate update within 10 days when:** the entity is reorganized, ceasing its operation, dissolved, or declared bankrupt; there are changes to the personal data protection service provider; or changes to business lines and services involving personal data processing which were registered in DPIA, CTIA dossiers.

In addition, Decree 356 further elaborates the PDPL and amends Decree No. 165/2025/ND-CP dated 30 June 2025 guiding the implementation of Law on Data 2024 (Decree 165) regarding impact assessment obligation. Accordingly, where the cross-border transfer or processing of core data or important data involves personal data, the data administrator is only required to prepare DPIA and CTIA dossiers in accordance with the PDPL and Decree 356, and is not

required to conduct risk assessments or impact assessments under the Law on Data 2024 and Decree 165.

7. Notification of violations of personal data protection regulations

For location and biometric data, in addition to the obligation to notify A05 in the event of a breach, Decree 356 introduces new requirements to (i) notify the data subject within 72 hours from the time the breach is discovered or (ii) publicly disclose the breach and notify data subjects as soon as feasible.

Notably, breach records must be retained for at least five years after remediation.

8. Inspection of personal data protection activities

Inspections of personal data protection activities may be conducted regularly or on an ad-hoc basis, as follows:

Criteria	Content
Basis	▪ Suspicion of violations of personal data protection laws ▪ Instructions from competent state authorities ▪ Implementation of state management duties
Subject	Organizations, individuals who: ▪ Process personal data ▪ Provide data processing services ▪ Conduct DPIA, CTIA ▪ Involved in cases or incidents relating to violations of personal data protection regulations
Content	▪ Personal data protection compliance ▪ DPIA and CTIA activities ▪ Provision of personal data processing services
Data marketplace transactions	▪ A05 will notify the inspection subject 15 working days in advance ▪ Conduct an immediate inspection without prior notice

9. Exemptions

The exemptions under Decree 356 broaden the scope, subjects, and duration of exemptions compared to Decree 13. However, the introduction of additional conditions—specifically, the requirement not to process sensitive personal data or that the cumulative number of data subjects processed must be below 100,000 may, in practice, narrow the number of entities eligible for exemptions.

Category	Decree 13	Decree 356
Scope of exemption	Appointment of DPO, DPD	▪ Appointment of DPO, DPD, engagement of external individuals/organizations providing personal data protection services ▪ Obligation to prepare, update, and submit DPIA, CTIA reports

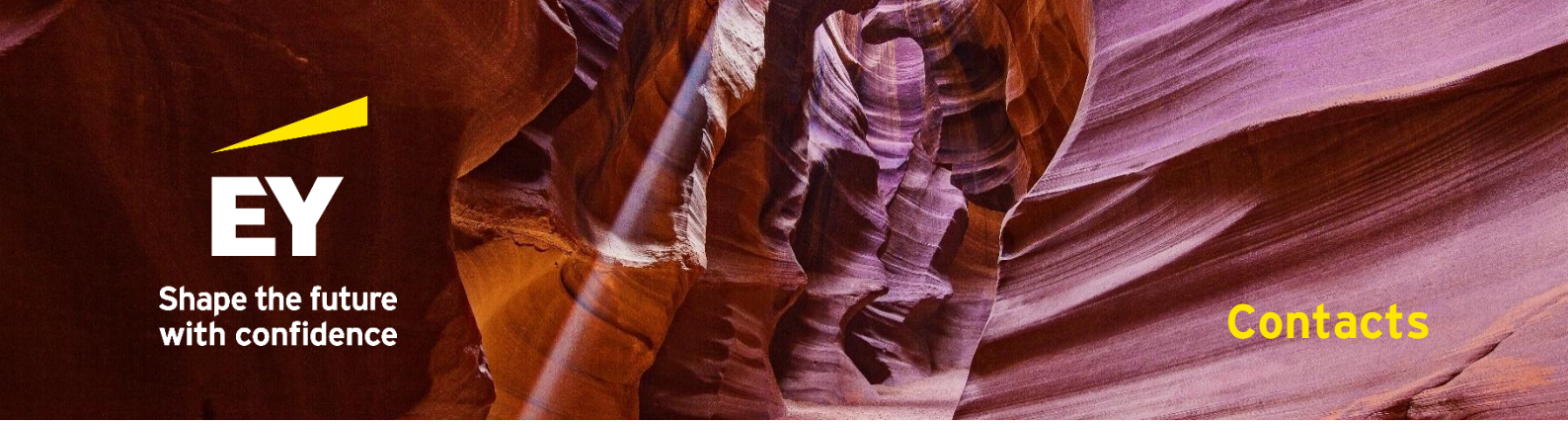
Entities eligible for exemption	▪ Micro, small, and medium-sized enterprises ▪ Start-ups	▪ Household businesses, micro and small enterprises ▪ Start-ups
Duration of exemption	Two years from the date of establishment	▪ Small enterprises, start-ups: Five years from 1 January 2026 ▪ Household businesses, micro-enterprises: fully exempt
Cases not eligible for exemption	Enterprises directly engaging in personal data processing as a business activity	Household businesses, enterprises that: ▪ Provide personal data processing services, ▪ Directly process sensitive personal data ▪ From the time of reaching a cumulative processing volume of 100,000 data subjects or more

Next course of action

In the context of increasingly stringent requirements for compliance with personal data protection regulations and the growing enforcement actions and administrative sanctions imposed by state agencies on violations, enterprises need to quickly develop and implement a comprehensive personal data protection program, closely aligned with the entire data lifecycle and encompassing both internal and external governance, from policy frameworks and technical measures to human factors. A comprehensive personal data protection program recommended for businesses is as follows:

No.	Activity	Content
1	**Gap assessment and develop a compliance roadmap**	▪ Assess gaps in operations, procedures, policies, templates, management and technical measures, human resources governance, data subject and partner management, and administrative procedural compliance in accordance with PDPL, Decree 356, consumer protection regulations, and other relevant laws ▪ Develop an implementation roadmap with appropriate tasks, timelines, resources, and budget.
2	**Enhance and standardize the personal data protection policy framework**	Enhance and standardize the enterprise's personal data protection framework in line with the PDPL, Decree 356, consumer protection regulations, and other relevant laws, including: ▪ Policy on personal data processing and consent templates for each data subject group ▪ Policies, guidelines, and procedures for personal data protection for employees, including: (i) General regulations on personal data processing (ii) Procedure for managing data subject consent forms (iii) Procedure for handling data subject rights requests

		(iv) Procedure for assessing and managing risks of business partners and service providers (v) Policy on retention, deletion, and destruction of personal data (vi) Governance regulations for personnel or departments in charge of personal data protection (vii) Policy for periodic compliance assessment on personal data protection (viii) Incident response policy for personal data breaches ▪ Standard contractual clauses for personal data transfer and processing ▪ Cross-border data transfer agreements
3	**Data flow mapping**	▪ Conduct a comprehensive assessment of systems, applications, databases, and business processes to identify all relevant data sources ▪ Develop a complete personal data flow diagram
4	**Prepare, update, and submit DPIA, CTIA**	▪ Prepare, track, update, and submit DPIA, CTIA using Forms No. 09 and No. 10 of Decree 356
5	**Appoint or hire personal data protection personnel**	▪ Assess whether internal DPO/DPD or external data protection service providers meet professional competency standards ▪ Reflect the structure, responsibilities, and operating mechanisms of these roles in the appointment decision, internal governance policies, and service contracts (if applicable)
6	**Awareness training**	▪ Develop awareness training programs for employees ▪ Conduct periodic training sessions
7	**Periodic assessment**	▪ Conduct periodic personal data protection compliance assessment to recommend measures to enhance compliance effectiveness, and prevent and mitigate risks in personal data processing activities



Ho Chi Minh City Office

Robert King | EY Vietnam, Laos, Cambodia Tax Leader
EY Consulting Vietnam Joint Stock Company
robert.m.king@vn.ey.com

Thinh Xuan Than | Law Leader
EY Law Vietnam Limited Liability Company
thinh.xuan.than@vn.ey.com

Hieu Duy Nguyen | Managing Director
EY Law Vietnam Limited Liability Company
hieu.d.nguyen@vn.ey.com

Robert Tran | EY Vietnam Cybersecurity and Technology Risk Leader
EY Vietnam Cybersecurity Services Company Limited
robert.tran@vn.ey.com

Thach Thi Cam Tran | Senior Manager
EY Law Vietnam Limited Liability Company
thach.cam.tran@vn.ey.com

Hanoi Office

Anh Thuy Pham | Associate Partner
EY Law Vietnam Limited Liability Company
anh.thuy.pham1@vn.ey.com

Linh Hoang Anh Nguyen | Director
EY Law Vietnam Limited Liability Company
linh.hoang.anh.nguyen@vn.ey.com

Japanese Business Services (JBS)

Takahisa Onose | EY Vietnam, Laos, Cambodia JBS Leader
Ernst & Young Vietnam Limited
takahisa.onose@vn.ey.com

Takaaki Nishikawa | Director
Ernst & Young Vietnam Limited
takaaki.nishikawa@vn.ey.com

Yuka Otomi | Associate Director
Ernst & Young Vietnam Limited
yuka.otomi@vn.ey.com

Korean Business Services (KBS)

Binh Thanh Phan | EY Vietnam, Laos, Cambodia KBS Leader
EY Consulting Vietnam Joint Stock Company
binh.thanh.phan@vn.ey.com

Kyung Hoon Han | Director
Ernst & Young Vietnam Limited
kyung.hoon.han@vn.ey.com

Chinese Business Services (CBS)

Truong Duc Le | EY Vietnam, Laos, Cambodia CBS Leader
Ernst & Young Vietnam Limited
truong.duc.le@vn.ey.com

Owen Tsao | Director
Ernst & Young Vietnam Limited
owen.tsao@vn.ey.com

Trinh Kiet Luong | Assistant Director
Ernst & Young Vietnam Limited
trinh.kiet.luong@vn.ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

APAC No. 16020301
ED None

ey.com/en_vn