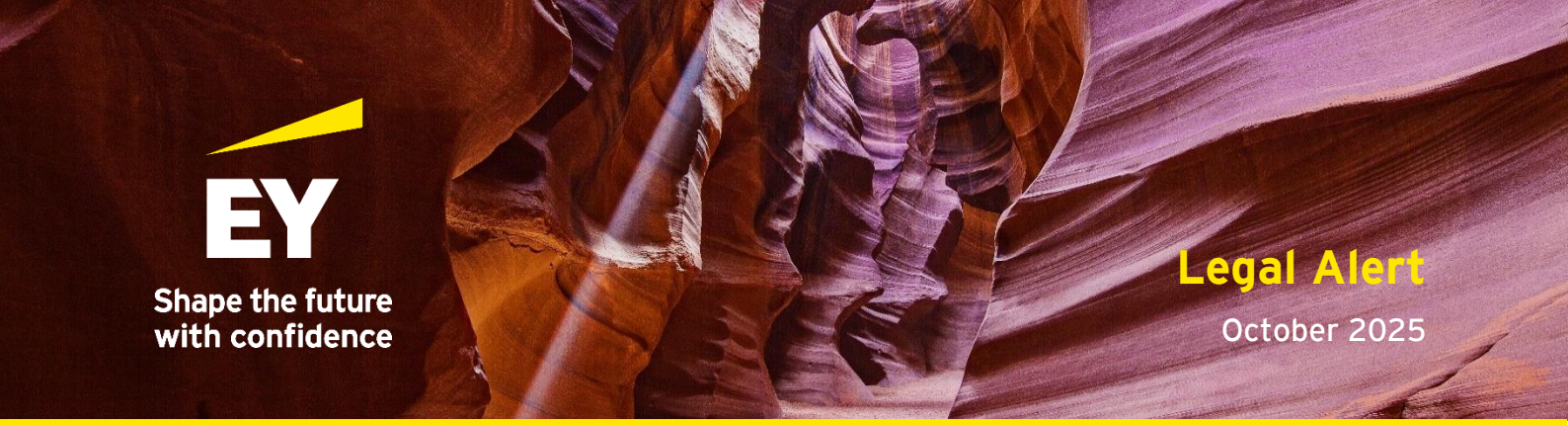


Visit other Alerts here.

Draft Decree detailing several provisions of the Personal Data Protection Law

This Alert highlights key compliance requirements set forth in the Draft Decree detailing several provisions of the Personal Data Protection Law

Following the issuance of the 2025 Law on Personal Data Protection (PDPL) dated 26 June 2025, the Ministry of Public Security released the Draft Decree detailing several provisions of the PDPL (Draft Decree) for public consultation. This Draft Decree is intended to clarify personal data protection requirements and conditions, as well as procedures and enforcement mechanism under the new PDPL, marking a significant step toward shaping Vietnam's comprehensive data protection regime.

Key highlights in the Draft Decree include:

- Definition and categorization of basic personal data and sensitive personal data
- Implementation of rights of data subjects
- Transfer of personal data
- Data protection officer or data protection department
- Data processing impact assessment and cross-border transfer impact assessment
- Notification of violations of personal data protection regulations
- Personal data processing services
- Sector-specific personal data protection
- Inspection of personal data protection
- Exemption

It is anticipated that the Decree will be issued and effective from 1 January 2026. We therefore highlight certain actions that companies should consider as soon as practical.

1. **Definition and categorization of basic personal data and sensitive personal data**

- Basic personal data: Contrary to the listing approach in Decree 13/2023/ND-CP (Decree 13), the Draft Decree defines basic personal data by exclusion, encompassing personal data that does not fall within the sensitive category.

- Sensitive personal data: Draft Decree provides further guidance, specifying that sensitive personal data requires restricted access, strict processing procedures, and heightened security measures. In addition to the categories listed under Decree 13, the Draft Decree explicitly includes:

  (i) Ideological view

  (ii) Individual digital identities

  (iii) Account usernames and passwords; banking card information, bank account transaction history; financial, credit, and other information related to customers' financial, securities, and insurance transactions at credit institutions, foreign bank branches, payment intermediary service providers, securities or insurance organizations, and other authorized entities

  (iv) Data on the activity and history of telecommunications subscribers

  (v) Data tracking behavior or usage of telecommunications services, social networks, online media services, and other services in cyberspace

  (vi) Other personal data designated by organizations or individuals as requiring strict protection measures

  With the addition of (vi), the Draft Decree effectively extends the concept of sensitive personal data beyond the law's enumerated categories, giving organizations both flexibility and responsibility to safeguard critical personal data.

2. **Implementation of rights of data subjects**

- **Right to consent**

  - Clear and verifiable consent: Data controllers and data controllers cum processors obtaining consent from data subject must clearly and accurately document the method, time, content, and verification of the data subject.

  - Acceptable consent methods: Consent must be verifiable and may include email, electronic platforms, websites, or apps with technical consent mechanisms.

  - Prohibition of default or misleading settings: Data controllers and data controllers cum processors cannot use default consents, or unclear instructions that could confuse data subjects. Default settings must respect data protection principles and data subject rights.

- **Rights to withdraw consent, restrict, object to the processing, view, correct or request correction, be provided with and delete personal data**

  Data controllers and data controllers cum processors must establish clear processes, procedures and forms to enable data subjects to exercise their rights to withdraw consent, restrict, object to the processing, view, correct or request correction, be provided with their data and delete, with specific timelines as follows:

  - Response timeline: within two working days

- Execution timeline:
  (i) Requests to withdraw consent, restrict, or object to processing: must be completed within seven working days
  (ii) Requests to view, correct or request correction, be provided with their data and delete data: must be completed within 10 to 15 working days, depending on whether data processors or third parties are involved
- Extension: Processing may be extended by up to 10 additional working days based on request complexity, with the data subject informed of the reason for the delay

3. Transfer of personal data

- Transfer of personal data with consent, or transfer to continue processing personal data in the event of reorganization or restructuring cases for units, enterprises and organizations, or transfer from data controller or data controller cum processor to data processor or a third party to process: requires a written agreement detailing purpose, data subjects, data types, processing duration, deletion, legal basis, and responsibilities.
- Transfer of sensitive personal data: requires encryption, anonymization, and physical security measures.
- Transfers involving fees/services: requires clear consent, purpose limitation, defined roles, and pre-transfer agreements.
- Internal transfer within the same organization: must formulate policies and prevent unauthorized disclosure.
- Trading of data: Data must be de-identified before marketplace transactions.

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

Under PDPL, companies are required to (i) appoint an internal DPO or establish internal DPD; and/or (ii) hire external organizations and individuals to provide personal data protection services.

The Draft Decree further provides guidance on designation of DPO/DPD:

- Qualifications for internal DPO: (i) University degree, (ii) at least three years of experience in legal affairs, personal data processing, cybersecurity, data security, risk management, compliance management, (iii) completion certificate of a basic training course on personal data protection issued by a competent training organization in Vietnam, (iv) meeting the required level in the professional personal data protection assessment program by the A05, (v) knowledge of data protection laws and processing activities of the organization and (vi) not having relevant criminal records in the fields of data, information technology, and telecommunications
- Qualifications for internal DPD: Personnel within DPD must satisfy the aforesaid qualifications for internal DPO.
- Qualifications for external individuals providing personal data protection services: similar to internal DPO, with the only difference being the requirement of at least five years of relevant experience
- Qualifications for external organizations providing personal data protection services: (i) must operate in technology, legal, or consulting sectors, (ii) must have at least three qualified personnel meeting the standards of external individuals providing personal data protection services, and (iii) must have prior experience providing services or products related to security, cybersecurity, information technology, or personal data protection standard

assessment, personal data protection consulting. Service providers must prepare a capability dossier demonstrating their expertise.

Internal DPO and DPD are responsible for developing and implementing policies, processes, and technical measures to ensure compliance with personal data protection laws; facilitate data subject rights; assess risks, and respond to data breaches or cross-border data transfers. They must also participate in training, conduct impact assessments, and advise on decisions related to personal data protection within the organization. Whereas responsibilities of external organizations and individuals providing personal data protection services are limited to delivering services strictly within the agreed scope.

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

The Draft Decree adds a new notable CTIA exemption of "cross-border transfer of personal data for cross-border personnel management in accordance with labor rules, internal labor regulations, and collective labor agreements as prescribed by law". This indicates that multinational companies managing employee data across jurisdictions will have reduced compliance burdens.

On the other hand, DPIA and CTIA dossier requirements are significantly more stringent than the prior framework under Decree 13. CTIA and DPIA dossiers must include data flow diagram; plan to ensure the security of personal data (post-transfer for CTIA), applied personal data protection measures and standards; system diagram and description of storage and processing systems (post-transfer for CTIA); procedures for onward transfer and sharing from recipients to third parties (for CTIA); compliance self-assessment and documentation ensuring data subject rights; as well as assessment of the recipient's level of data protection (for CTIA).

The circumstances and timeline for updates of DPIA and CTIA are also clarified under the Draft Decree:

- Periodic update every six months: when (i) new purposes of transfer or processing arise; or (ii) there are changes to data controllers, data controllers cum processors, data processors, or third parties.
- Immediate update within 60 days if the entity is reorganized, terminated operation, dissolved, or declared bankrupt; if there are changes to the personal data protection service provider; or if new or changes to business lines/services involving personal data registered in DPIA/CTIA dossiers.

6. Notification of violations of personal data protection regulations

For location and biometric data, in addition to notifying A05, the data controller or data controller-cum-processor must (i) notify affected data subjects within 72 hours of detecting a breach, or (ii) if technical or urgent constraints prevent notifying all affected subjects within 72 hours, issue a public electronic notice and provide personalized notifications as soon as feasible. Records of the breach must be retained for at least five years.

7. Personal data processing services

With the rise of personal data activities, regulators have introduced stricter oversight by classifying personal data processing services as a conditional business sector, requiring organizations to meet personnel qualifications, obtain an eligibility certificate from A05, and comply with ongoing operational obligations.

Personal data processing services include the following:

- Providing and operating automated systems or software to process personal data on behalf of data controller or data controller cum processor

- Scoring, ranking, or assessing the creditworthiness of data subjects
- Collecting and processing personal data online via websites, apps, or social networks
- Collecting and processing personal data via websites, apps, software, or social networks for surveys or market research
- Collecting and processing personal data via websites, apps, software for healthcare, health monitoring or medical services
- Collecting and processing personal data via educational apps, software with monitoring features, such as attendance checking, video recording, behavior scoring, or emotion recognition
- Analyzing and exploiting personal data, including the use of analytical tools to identify information, trends, and patterns from personal data; applying data mining methods to extract value from personal data, predict user behavior, or optimize services
- Encrypting personal data during transmission or storage
- Automatically processing personal data using big data, artificial intelligence, blockchain, or virtual reality technologies
- Platform services providing personal location data

8. Sector-specific personal data protection

The Draft Decree defines big data, artificial intelligence, blockchain, metaverse, and clarifies sector-specific personal data protection obligations under the PDPL.

- **For finance, banking, and credit information**
  - Comply with international and Vietnamese standards for data protection and cybersecurity
  - Conduct annual compliance assessments
  - Maintain logs of all personal data processing
  - When obtaining consent, clearly specify purposes of data processing, data sources and parties involved in collection and sharing, storage duration and procedures for withdrawing consent or deleting data
  - Notify affected data subjects within 72 hours of any breach involving bank, financial, or credit information
- **For big data (large-scale, continuous, and integrated processing of personal data from multiple sources, enabling behavior analysis, trend prediction, or user classification)**
  - Encrypt, anonymize, pseudonymize data, and restrict access
  - Monitor access, conduct regular cybersecurity assessments, and train staff
  - Ensure third-party compliance
  - Inform data subjects about how their data is used
- **For artificial intelligence, metaverse**
  - Inform subjects of automated processing, explain algorithmic impacts, and offer opt-out options

- Implement strong cybersecurity system, establish strategic contingency plans, build personal data protection mechanisms in accordance with the highest international standards and early-warning systems for cybersecurity risks, implement controls to stop artificial intelligence and metaverse from being used to threaten national security or public order, conduct annual compliance assessment, and conduct data protection impact assessment before deploying systems, especially if data subject rights could be significantly affected
- Authorities may require artificial intelligence algorithms to be deleted if they violate data protection regulations.

- **For cloud computing**
  - Contracts with cloud providers must specify compliance with Vietnamese data protection laws, roles and responsibilities, data flow, security measures, notification of changes, data retention, deletion, and data subject rights.
  - Cloud service providers must comply with Vietnamese data protection laws, require subcontractors to comply, and apply appropriate technical and organizational measures based on the processing scale and level.
  - Personal data must be encrypted at rest and in transit, with strict access restrictions.
- **For blockchain**
  - Avoid storing personal data directly on the blockchain; use encryption or hashed values
  - Apply secure encryption and hashing algorithms
  - Conduct annual compliance audits
  - Perform data protection impact assessments before deployment, especially if significant risks to data subjects' rights exist

9. Inspection of personal data protection

Inspections of personal data protection can be regular, periodic, or ad-hoc, triggered by legal violations or for State management purposes. Any entity processing personal data, providing processing services, conducting DPIA, CTIA, or certifying data protection competence may be inspected. Inspections will cover compliance status, DPIA, CTIA activities, and certification processes. A05 will notify subjects 15 working days in advance, and results are kept confidential.

10. Exemption

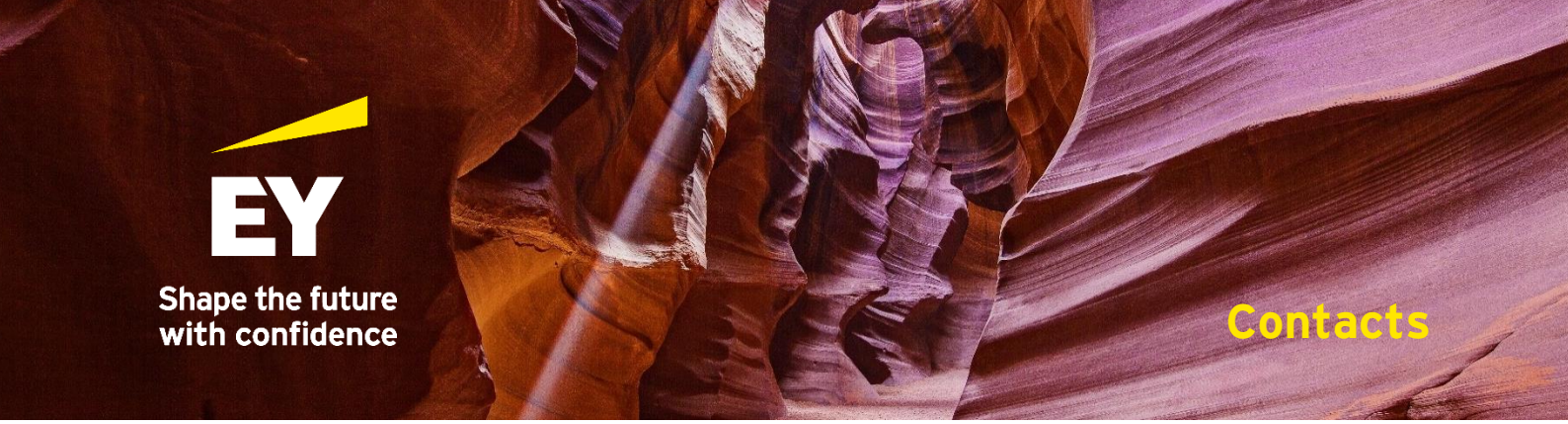
Exemptions from DPIA, update of DPIA and CTIA, appointment of DPO, DPD obligations will not apply to small and startup enterprises, household businesses and micro-enterprises if they:

- Provide personal data processing services
- Directly process sensitive personal data
- Exceed a scale of 100,000 data subjects (for small and startup enterprises) or 500,000 data subjects (for household businesses and micro-enterprises)

Next course of action

The Draft Decree introduces significant changes that expand and clarify obligations for organizations handling personal data, expected to take effect from 1 January 2026 alongside the PDPL. These updates signal heightened regulatory scrutiny and underscore the need for organizations to act promptly to align with Vietnam's strengthened data protection framework. Several interconnected areas of action are recommended to ensure compliance and prepare for inspections by A05.

- **Framework enhancement:** Organizations must review and revise their personal data framework to accommodate the new categorization of basic and sensitive personal data, sector-specific data and the corresponding protection measures. Clear processes for obtaining and managing consent from data subjects must be established, ensuring that consent is documented and verifiable, with specific timelines for responding to data subject requests.
- **Personnel:** With only a few exceptions, organizations must designate a DPD, DPO with the required qualifications. Appointments should be made in writing, clearly stating the legal obligations of such personnel. Additionally, training sessions should be conducted for staff involved in data processing to ensure they understand the new requirements under the PDPL and Draft Decree.
- **Administrative requirements and procedures:** The new stringent DPIA and CTIA requirements demand comprehensive documentation. Organizations should review their current data processing activities and cross-border transfers to identify areas needing immediate attention. They must develop and implement robust DPIA and CTIA frameworks, including detailed data flow diagrams and security plans, while assigning responsibilities to personnel for monitoring and documenting necessary updates.



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 | Director
EY Law Vietnam Limited Liability Company
thinh.xuan.than@vn.ey.com

Robert Tran | Deputy General Director
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

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

Le Hong Nguyen | Manager
EY Law Vietnam Limited Liability Company
le.hong.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. 16141001
ED None

ey.com/en_vn