LNT & PARTNERS

LEGAL ALERT

Our monthly publication is dedicated to provide a roundup of key regulatory updates that impact investment and business activities in Vietnam. Visit our Resource Center for the latest legal updates and firm news.

Decree 356/2025/ND-CP – New framework replacing Decree 13/2023/ND-CP with refined Personal Data Categories and heightened Processing Obligations

Phan Thi Ngoc Diep – *Senior Associate*

Trinh Minh Vu – *Trainee Associate*

The Government has promulgated Decree No. 356/2025/ND-CP ("**Decree 356**"), replacing Decree No. 13/2023/ND-CP ("**Decree 13**") and clarifying requirements under the Personal Data Protection Law ("**PDP Law**"). Effective from 1 January 2026, Decree 356 introduces changes that businesses should carefully consider.

This Legal Alert highlights the most notable updates.

Key matters

1. Personal Data Classification

Decree 356 introduces certain changes to the lists of basic personal data and sensitive personal data, with different levels of impact (*Art. 3-4*).

- For **basic personal data**, certain identifiers that were previously included in Decree 13 - such as personal tax codes, social insurance numbers and health insurance card numbers - have now been removed. That said, given that the catch-all and exclusion clause remains in place (providing that any information associated with or capable of identifying a specific individual, and not classified as sensitive data, will be treated as basic personal data), it is likely that these removed identifiers will continue to fall within the category of basic personal data (*Art. 3.11*).

  In addition, family relationship data has been broadened to also encompass information relating to spouses, whereas previously it was limited to parents and children only (*Art. 3.9*).

- For **sensitive personal data**, Decree 356 broadens and clarifies the scope by introducing certain new categories - such as digital identity account credentials, images of identity

documents, and behavioural or usage-tracking data on digital platforms - while also providing more detailed treatment of financial and banking data.

In addition, data relating to individuals' activities and history in cyberspace, which was previously classified as basic personal data, has now been reclassified as sensitive personal data (*Art. 4.1*).

Decree 356 further requires businesses that process sensitive personal data to establish access-control protocols, internal handling procedures and appropriate security safeguards (*Art. 4.2*).

2. Key Personal Data Protection Requirements

a. **Stricter Consent standards.** Under Decree 356, consent must be obtained in a verifiable format. Acceptable forms include: written documents, recorded voice calls, text message confirmations, emails, technical consent settings on websites, platforms or applications, or other verifiable formats (*Art. 6.1*). The decree expressly prohibits default opt-in mechanisms and any misleading design practices that obscure the distinction between granting and refusing consent (*Art. 6.3*). Furthermore, data controllers and controller–processors are obligated to maintain records of data subjects' consent and bear the burden of proof in case of a dispute *Art. 6.2*).

b. **Clearer qualification requirements for Data protection officer (DPO).** The appointment of DPO(s) must still be formally made in writing (*Art. 13.1*). To qualify as a DPO, the appointed individual must now (i) hold at least a college-level qualification, (ii) possess a minimum of two years of post- graduation professional experience in one of the following relevant fields: legal, information technology, cybersecurity, data security, risk management, compliance control, human resource management or organizational structure, and (iii) have undergone internal training covering both legal knowledge and professional skills related to personal data protection (*Art. 13.2*).

c. **Timeframes for handling data subject requests vary according to the type of requests.** Data controllers and data controller–processors must establish clear procedures to facilitate the exercise of data subject rights, and to ensure that data subjects are duly informed of such procedures. Requests from data subject (such as withdrawal of consent, erasure of personal data or other rights-related requests) must be acknowledged within 02 working days of receipt and completed within statutory timeframes ranging from *10, 15, 20 or 30 days* depending on the nature of the request and whether the involvement of a data processor or third party is required to fulfil the request. A single extension of the applicable deadline (for an additional 10, 15 or 20 days, as relevant to the nature of the request) is permitted, provided that the extension is properly justified and the data subject is notified accordingly (*Art. 5*).

d. **Stricter rules for Personal data transfer, requiring formal agreements and added safeguards for sensitive information.** Decree 356 establishes a more comprehensive regulatory framework governing the transfer of personal data. In specified circumstances, data controllers and data controller–processors are required to enter into a personal data transfer agreement that sets out key elements, including the purpose of the transfer, categories of personal data involved, applicable legal basis, duration of processing and responsibilities for data protection. For transfers involving sensitive personal data, the decree imposes heightened safeguards. These include the implementation of physical security measures for storage and transmission devices together with technical protections such as encryption, anonymization and other appropriate security measures throughout the transfer process. (*Art. 7*).

e. **New Sector-specific requirements.** Decree 356 imposes enhanced personal data protection obligations on certain sectors, notably finance and banking, big data processing, AI systems, virtual environments, blockchain and cloud services (*Arts. 8–12*).

3. Critical updates to DPIA submission

a. **Two-way review mechanism with defined timelines.** For the first time, Decree 365 formally introduces a two-way review mechanism, under which a data controller or data processor submitting a Data Protection Impact Assessments (DPIAs) for data processing activities or cross-border data transfers will receive an official outcome on its submission, whether approval or rejection. This mechanism purportedly aims to enhance transparency and accountability in the review process and to formalize the review practices that were applied in practice during the effectiveness of notwithstanding the fact that Decree 13 was silent on this procedure. Under this two-way review mechanism, Decree 356 also introduces a clear timeline for the evaluation of each DPIA submission (*Arts. 18–19*):

- 15 day-evaluation period: The agency responsible for protecting personal data must evaluate and issue a decision - either satisfactory or unsatisfactory – within 15 days of receiving a complete application.

- 30-day completion window: If an application is incomplete or fails to comply with regulatory requirements, applicants are granted 30 days to provide the missing information or correct deficiencies. Failure to complete the required documentation within this timeframe may result in administrative penalties.

b. **Introduction of new forms and workflow requirements.** Decree 356 replaces the earlier forms issued under Decree 13 with new, more comprehensive templates for documenting data processing activities.

- Role-based workflow requirement: The new forms mandate that businesses outline workflows for personal data processing based on specific roles and responsibilities.

- Process flow and system modelling: Businesses must now provide detailed models of their data processing flows and systems, going beyond simple descriptive information. This requires a deeper and more technical understanding of how personal data is handled within the organization.

- Practical implications: These requirements reflect practices already being applied in reality but now carry formal regulatory weight. They demand that organizations move from surface-level reporting to substantive documentation or their data governance structures.

c. **Specific threshold for non-applicability of DPIA formulation exemptions.** Generally, small enterprises and household businesses are permitted to defer the formulation of DPIAs without being deemed in breach of the law for a period of up to 5 years from 01 January 2026. However, this exemption does not apply where such entities process personal data of data subjects on a "large-scale" (*Art. 38 of PDP Law*). In this regard, Decree 356 **provides** further clarity by stipulating that the exemption ceases to apply from the point at which personal data of 100,000 or more data subjects is processed (*Art. 41*).

4. Resolving overlapping DPIA requirements for data classified as both core/important data and personal data.

Decree 356 clarifies that where core data or important data also constitutes

personal data, the safeguarding and processing of such data shall be subject to the PDP Law and its guiding Decree 356 (rather than the Data Law and its guiding Decree 165/2025/ND-CP). Notably, businesses processing core/important data that is also personal data are not required to conduct the separate risk assessments prescribed under the Data Law; instead, the DPIA conducted in accordance with the PDP Law will be deemed sufficient. By removing this duplicative obligation, the regulation is expected to streamline the compliance process and reduce administrative burdens for data controllers and processors (*Art 42.3*).

Unresolved Matter

One of the major outstanding concerns under the PDP Law - the calculation method for illegal gains for sanctioning purposes - remains unprescribed.

What Businesses Should Do

Where data processing activities are complex or undergo significant changes—such as the reclassifications of certain categories of sensitive personal data, the introduction of new data processing obligations, or the adoption of new statutory forms—businesses should consider undertaking a comprehensive compliance review and seek professional legal advice to ensure the new requirements are properly implemented and support the development of a robust, future-proof data protection strategy.

As Decree 356 has only recently come into effect, the Ministry of Public Security is still finalizing internal procedures to support compliance. Businesses should therefore monitor forthcoming guidance closely and prepare to align their documentation with the new forms and requirements.

CONTACT US

For more information about any of these legal briefs, please contact our Partners:

Mr. Hong Bui

Corporate/M&A, Foreign Investment, Compliance & ABAC, Employment, Litigation & ADR

Hong.Bui@LNTpartners.com

Mr. Binh Tran

Corporate Governance, Employment, Foreign Investment, Litigation & ADR, Real Estate, Corporate/M&A, Tax

Binh.Tran@LNTpartners.com

Ms. Quyen Hoang

Corporate/M&A, Compliance & ABAC, Employment, Insolvency & Restructuring

Quyen.Hoang@LNTpartners.com

Dr. Net Le

Banking & Finance, Real Estate, Litigation & ADR, Corporate/M&A, Tax

Net.Le@LNTpartners.com

Dr. Tuan Nguyen

Antitrust/Competition, Corporate/M&A, Employment, Compliance & ABAC, Foreign Investment

Tuan.Nguyen@LNTpartners.com

Mr. Thuy Nguyen

Corporate/M&A, Foreign Investment, Employment, Tax

Thuy.Nguyen@LNTpartners.com

Ms. Minh Vu

Tax, Foreign Investment, Banking & Finance, Corporate Governance, Corporate/M&A, Projects

Minh.Vu@LNTpartners.com

Mr. Phu Nguyen

Litigation & ADR

Phu.Nguyen@LNTpartners.com

Ms. Nhi Luong

Litigation & ADR, Employment

VanNhi.Luong@LNTpartners.com

Ms. Diep Nguyen

Litigation & ADR, Banking & Finance, Employment, Tax, Intellectual Property, Compliance & ABAC

Diep.Nguyen@LNTpartners.com

Mr. Hai Ngo

Banking & Finance, Corporate Governance, Litigation & ADR, Real Estate

Hai.Ngo@LNTpartners.com

For further information, please contact us:

Ho Chi Minh City (HQ)

Level 21, Bitexco Financial Tower
2 Hai Trieu St., Sai Gon Ward

+84 28 3821 2357

Hanoi

Level 12, Pacific Place Building
83B Ly Thuong Kiet St., Cua Nam Ward

+84 24 3824 8522

About us

LNT & PARTNERS ("LNT") is a full-service independent Vietnam law firm, which focuses on advisory and transactional work in the areas of corporate and M&A, competition, pharmaceutical, real estate, infrastructure and finance as well as complex and high-profile litigation and arbitration matters. The firm is among Vietnam's most prominent, representing a wide range of multinational and domestic clients, including Fortune Global 500 companies as well as well-known Vietnamese listed companies.

For more information about any of these legal briefs, please contact the individual authors or your usual LNT contact.