LNT & PARTNERS

LEGAL UPDATE

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.

Key Highlights of the New Draft Decree on Personal Data Protection

Ho My Ky Tan – *Associate*

Tran Minh Thao – *Associate*

Further to our legal update titled "New Personal Data Protection Law – What you need to prepare for future compliance", which outlined key takeaways of the new Personal Data Protection Law (**PDP Law**), we would like to introduce this legal update on key highlights of the recently released draft decree on detailed guidance of several provisions of the PDP Law (**Draft Decree**). The Draft Decree is open for public comments until 26 September 2025 to ensure its timely enactment before the PDP Law's effective date of 1 January 2026.

Data Definitions

The Draft Decree defines "basic personal data" as personal data that reflects common personal background and identity, which is frequently used in transactions and social relationships, and does not fall within the list of sensitive personal data. This is a more generalised definition than the exhaustive list provided in Decree 13/2023/ND-CP (**Decree 13**).

"Sensitive personal data" is defined as personal data that (i) is associated with an individual's privacy; (ii) if infringed upon, will directly affect legitimate rights and interests of agencies, organisations, and individuals; and (iii) requires restricted access, specific processing procedures, and strict security measures.

The Draft Decree's list of sensitive personal data includes several new categories that were not explicitly mentioned in Decree 13, such as electronic identity information, account login names and passwords, bank card information, financial/credit/insurance information, telecommunication subscriber activity and history data, data tracking behaviour and usage of telecommunications/social networks/online media/other online services, etc.

Timelines for Handling Data Subject Requests

The PDP Law stipulates that data controllers and data controller-processors must handle data subject requests in a "timely" manner (a notable shift from the rigid 72-hour deadline in Decree 13),

and delegates the Government the responsibility of providing detailed guidance. The Draft Decree provides the much-needed details for this requirement by setting clear, tiered timelines as follows:

Data Subject Request	Response Deadline	Fulfillment Deadline	Maximum Extension
Withdraw consent, restrict processing, or object to processing	2 working days	7 working days	10 working days
View, edit, provide, or delete personal data	2 working days	10 working days (15 working days if coordination with data processors or third parties is needed)	10 working days

Stricter Requirements for Consent Collection

Under the Draft Decree, data controllers and data controller-processors are mandated to obtain consent in a manner that ensures clear and accurate evidence of the method, time, content, and authentication of the data subject. Acceptable methods of consent include: (i) in writing; (ii) by voice; (iii) via phone messages; (iv) via emails, on websites, platforms, or applications with technical mechanisms for obtaining consent; and (v) other suitable methods that can be verified and authenticated.

The Draft Decree explicitly prohibits the use of default consent settings or any unclear instructions that could mislead a data subject, and requires that any default settings used must comply with data protection principles and uphold data subject rights.

To underscore the protection of the rights of data subjects, who are often the weaker party in the relationship with data controllers or data controller-processors, the Draft Decree also sets out that: (i) in the event of a dispute, the burden of proof regarding the data subject's consent lies with the data controller or data controller-processor; and (ii) an organisation or individual can be authorised to act on behalf of the data subject (in accordance with civil law) to carry out procedures related to the processing of their personal data, provided that the data subject is fully informed and has given consent.

Transfer of Personal Data

Following the provisions of the PDP Law, the transfer of personal data as outlined in the Draft Decree must comply with stringent principles. For instance:

(a) Data transfer in cases of (i) obtaining consent from the data subject, (ii) business reorganisation, and (iii) transfer of personal data by the data controller or data controller-processor to the data processor or third party requires a written agreement. This agreement must specify the purposes, data subjects, types of data being transferred, processing period, legal basis, and the responsibilities of each party for protecting personal data and upholding data subject rights.

(b) When sharing personal data between departments within an agency or organisation for processing in line with established purposes, agencies and organisations must establish policies to govern data sharing and usage, ensure regulatory compliance, and prevent unauthorised disclosure to third parties.

(c) The transfer of sensitive personal data must be safeguarded by security measures (e.g., physical security measures for storage and transmission devices, encryption, anonymisation, etc.).

(d) Personal data must be anonymised before being traded on a data exchange platform.

Qualifications of DPO and Data Protection Service Provider

<table>
<tr><th>Qualification</th><th>Data Protection Officer (DPO)</th><th>Individual data protection service provider</th></tr>
<tr><td>Level of education</td><td colspan="2">Bachelor’s degree or higher</td></tr>
<tr><td>Work experience</td><td>3 years of experience (since graduation) in legal affairs, personal data processing, cybersecurity, data security, risk management, or compliance</td><td>5 years of experience (since graduation) in legal affairs, personal data processing, cybersecurity, data security, risk management, or compliance</td></tr>
<tr><td rowspan="2">Training</td><td>• Certification in basic personal data protection from a qualified training provider in Vietnam.</td><td>• Certification in specialised personal data protection from a qualified training provider in Vietnam.</td></tr>
<tr><td colspan="2">• Pass the personal data protection certification program by the data protection authority.</td></tr>
<tr><td>Other requirements</td><td colspan="2">• No prior convictions in the fields of data, information technology, or telecommunications.
• Understanding of personal data protection laws and data processing activities of agencies and organisations.</td></tr>
</table>

Other key points regarding the data protection officer/department and data protection service provider are set out in the Draft Decree as below:

(a) Organisations may establish a data protection department (optional), and all DPOs in such department must meet the qualifications set out above. The appointment of the data protection officer/department must be in writing, specifying roles, responsibilities, and authority related to personal data protection. Organisations must execute confidentiality agreements with their DPOs, which may include liability exemption provisions.

(b) Organisations may engage qualified individuals or organisations as data protection service providers and must make information about them publicly available to data subjects and other relevant parties.

(c) A qualified organisational data protection service provider is an organisation (i) offering technology, legal, or technical/legal advisory services, (ii) with at least 3 individuals qualified for providing data protection services, and (iii) having relevant experience in data security, cybersecurity, IT, standards assessment, or personal data protection consulting. The organisational data protection service provider is required to maintain a detailed capability profile for clients, showing its business scope, service experience, policies, staff qualifications, and other supporting documents.

DTIA and DPIA

Compared to the PDP Law, the Draft Decree provides new exemptions for the preparation and submission of DTIAs, such as journalism and media activities, cross-border personnel management, cross-border data transfers for contract execution, logistics, payments, or visa applications, etc. The Draft Decree also stipulates that the competent authority may conduct inspections of cross-border data transfer no more than once a year, unless a violation of personal data protection regulations is detected, or a data leak or loss incident occurs for personal data of Vietnamese citizens.

While immediate updates within 60 days are required for specific material changes as set out in the PDP Law, DTIAs and DPIAs must also be updated every six months in the event of new purposes for processing or transferring personal data, or a change in the data controller, data controller-processor, data processor, or a third party involved.

Non-applications of the Exemptions for SMEs

The PDP Law provides for general provisions regarding the non-application of the exemptions for SMEs, but the specific thresholds were left to be determined. The Draft Decree now provides these quantitative thresholds, namely (i) the processing of personal data of 100,000 or more data subjects, for small enterprises and start-ups; and (ii) the processing of personal data of 500,000 data subjects, for micro-enterprises and business households.

Personal Data Processing Services

In response to the growing need for regulated and standardised data processing, the Draft Decree introduces personal data processing services as a new conditional business sector, with the following types of services included:

(a) Services for providing and operating automated systems and software to process personal data on behalf of the data controller or data controller-processor;

(b) Services for credit scoring, ranking, and assessing;

(c) Services for collecting and processing personal data online from websites, applications, and social networks;

(d) Services for collecting and processing personal data via websites, applications, software, and social networks for surveys and market research;

(e) Services for collecting and processing personal data through websites, applications, and healthcare software for health monitoring and medical services;

(f) Services for collecting and processing personal data via educational applications and software with monitoring features such as attendance, recording, behavior scoring, and emotion recognition;

(g) Services for analysing and mining personal data, including using analytical tools to search for information, trends, and patterns from personal data; applying data mining methods to extract value from personal data, predict user behavior, or optimize services;

(h) Services for encrypting personal data during transmission and storage;

(i) Services for automatically processing personal data based on big data technology, artificial intelligence, blockchain, and virtual reality; and

(j) Platform services providing personal location data.

Under the Draft Decree, organisations offering these services will have to apply for a Certificate of eligibility to conduct personal data processing services from the competent data protection authority, of which the proposed validity period is 5 years.

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

Dr. Van Tuan Nguyen

Banking & Finance, Compliance & ABAC, Foreign Investment, Litigation & ADR, Intellectual Property

VanTuan.Nguyen@LNTpartners.com

Ms. Duyen Duong

Real Estate, Corporate Governance, Insolvency & Restructuring, Corporate/M&A

AnhDuyen.Duong@LNTpartners.com

Ms. Nhi Luong

Litigation & ADR, Employment

VanNhi.Luong@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 3921 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.