Data. Protection. Adding Value.

Data Protection Laws - Viet Nam

Legislation

Decree No. 13/2023/ND-CP of the Government**,** which came into effect on 1 July 2023, plays a vital role in Vietnam government's efforts to enhance the protection of personal data ("**PDPD**"). PDPD outlines the rights and responsibilities of individuals and organizations involved in personal data processing activities. Its primary objective is to promote the responsible handling of Personal Data, thereby fostering a safe and privacy-focused atmosphere in Vietnam.

Scope: PDPD outlines regulations for safeguarding personal data of Vietnamese citizens and assigns responsibilities for its protection to relevant agencies, organisations, and individuals. It applies to both Vietnamese and foreign entities within Vietnam's jurisdiction, as well as Vietnamese entities and individuals operating overseas, and foreign entities, without any commercial presence in Vietnam, involved in personal data processing within Vietnam.

Exemptions: PDPD does not apply to personal data of non-Vietnamese citizens

Risk Level: High

Supervisory Authority

Supervisory Authority: The Ministry of Public Security's Department of Cybersecurity and High-Tech Crime Prevention and Control ("**A05**") is the organization responsible for enforcing the Decree and is the Regulatory Authority. It works with the Ministry of Public Security to carry out the State data protection management.

Registration/Approval Requirements: There is no compulsory registration or approval procedures regarding personal data protection under the PDPD. Nonetheless, personal data controllers, processors, or controller cum processor must submit the impact assessment dossier for personal data processing to A05 within 60 days of initiating personal data processing activities. Additionally, if personal data is transferred abroad, the impact assessment dossier for such transfers must also be submitted within the same timeframe.

General PDPD Principles

PDPD outlines fundamental principles regarding personal data protection that must be adhered to as follows:

- Personal data is processed in accordance with the law.
- Data subjects are informed about activities related to the processing of their personal data, unless otherwise provided by law.
- Personal data will only be processed for the purposes registered and declared by the data controller, data processor, data controller cum processor, third party.
- Collected personal data must be appropriate and limited to the scope and purpose to be processed. Personal data may not be bought or sold in any form, unless otherwise prescribed by law.
- Personal data shall be updated and added for the processing purposes.
- Personal data shall be protected and secured throughout the processing. To be specific, the personal data shall be protected from violations against regulations on protection of personal data and prevention of loss, destruction or damage caused by incidents and use of technical measures.
- Personal data shall be stored within a period of time that is appropriate for the processing purposes, unless otherwise provided for by law.
- Data controller and data controller cum processor have to prove their compliance to the above principles.

Enforcement

Enforcement (Fines, Criminal Penalties):

- Violations such as inadequate security measures or failure to minimise personal data may incur fines ranging from VND 2 million (~ USD 90) to VND 70 million (~ USD 3,060).
- Criminal penalties may also be imposed for violations of rules governing confidentiality and safety concerning an individual's email, mail, telephone, or other forms of communications. Penalties may include: a warning, a fine between VND 20 million (~ USD 830) and VND 200 million (~ USD 8,510), and / or non-custodial reform of up to three years or a prison sentence of between one and three years in duration.

Remedies: Forced erasure or destruction of personal data

Personal Data Processing

Legal Basis for Processing: Personal data can be processed based on: (i) explicit consent of data subjects, and (ii) cases of exemption from consent under Article 17 of PDPD, such as emergency circumstances, compliance with legal obligations, and agreement between data controller and data processor.

Sensitive Personal Data: Additional requirement apply to sensitive personal data, including:

- Notifying the data subject that the data to be processed is sensitive personal data.
- Designate departments and personnel with functions to protect personal data

Restrictions on Processing: PDPD prohibits the following actions:

- Processing personal data contrary to the provisions of law on personal data protection.
- Purchasing or selling personal data in any form.
- Processing personal data to create information and data aimed against the State of the Socialist Republic of Vietnam.
- Processing personal data to create information and data that affects national security, social order and safety, and the legitimate rights and interests of other organizations and individuals.
- Obstructing personal data protection activities of competent authorities.
- Taking advantage of personal data protection activities to violate the law.

pwc

Transparency Requirements

Data subjects must be informed about the processing extent of their personal data, even if obtained indirectly through a third party. Transparency obligations are often fulfilled via privacy notices.

Data Subject's Rights

The data subject is entitled to have the rights under PDPD as follows:

- Right to know
- Right to consent
- Right to access
- Right to withdraw consent
- Right to erasure of data
- Right to restrict of data processing
- Right to data provision
- Right to object to data processing
- Right to complain, denounce and initiate lawsuits
- Right to claim damage
- Right to self-protection

Security & Data Breaches

Security Requirements: Personal data protection measures must be applied from the beginning and throughout the processing of personal data, including:

- Management measures.
- Technical measures.
- Measures implemented by competent state management agencies.
- Investigation and litigation measures implemented by competent state agencies.
- Other measures as prescribed by law.

Data Breaches: Committing any violation of personal data protection regulations under PDPD are considered data breaches.

Notification to supervisory authority: Data controller, data processor, data controller cum processor must notify A05 within 72 hours after the breach occurs. Any late notifications must include valid reasons

Notification to Individuals: no requirement.

Other Business Obligations

Data Protection Officer: The PDPD does not explicitly regulate the position of a data protection officer. Instead, it mandates the appointment of a department or designated personnel responsible for safeguarding sensitive personal data and liaising with relevant authorities.

Risk Assessments: no requirement.

Audits: The cybersecurity of systems and means, equipment serving the processing of personal data is examined before processing, and devices containing personal data are irreversibly deleted or destroyed.

Record Keeping: Data controller has to record and store system logs of personal data processing activities.

Trainings: Agencies, organisations, and individuals are responsible for propagating and disseminating knowledge, skills, and raising awareness of personal data protection for agencies, organisations, and individuals.

Service Providers & Cross-Border Transfers

Service Provider Arrangements: In case a organisation or individual, as a data controller or data controller cum processor, engages the data processor to process personal data on its behalf, it is required to have a data processing agreement. The formality and content of such agreement is not yet regulated by PDPD.

Cross-Border Data Transfers: Personal data is transferred abroad in case the party transferring the data abroad prepares a impact assessment dossier of transferring personal data abroad and submit it to A05 within 60 days from the date of processing of personal data.

Localisation Requirements: There are no localisation requirement under the PDPD, however, it may require to have a data localisation according to the law on cyber security.

Other/To Watch

- A draft Decree on administrative penalties for cyber security violations will be soon take effect. Accordingly, committing violations in cyberspace (such as such as unauthorised collection, transfer, purchase, or sale of personal data; violations of regulations on impact assessment of personal data processing, etc.) will be subject to administrative penalties including: (i) a warning, (ii) monetary fines (e.g., up to 5% of revenue in the Vietnamese market of the previous fiscal year based on the violations nature), (iii) additional penalties (e.g., revocation of operational licence / permit; prohibition of practising or doing work related to cybersecurity), and (iv) remedial measures depending on the nature and severity of the violation.
- A draft of law on personal data protection is currently being prepared by the Ministry of Public Security ("**MPS**"). From the legislative process in Vietnam, the MPS has released a draft proposal on drafting the law on personal data protection in 1st quarter of 2024 to collect public feedback and serve as a basis for drafting the law on personal data protection to the National Assembly for review in the upcoming National Assembly's session..

Let's connect to discuss how we can help:

Tran Thi Than Niem

Legal Services
Senior Associate, PwC Legal Vietnam

+ (84) 908 893 987
tran.thi.than.niem@pwc.com