Decree on Personal Data Protection

Michael Lee, Partner
Trang Nguyen, Senior Associate
Duc Le, Paralegal

Dated 12 June 2023

On 17 April 2023, the Vietnamese government issued Decree No. 13/2023/ND-CP on Personal Data Protection (**"PDPD"**), Vietnam's first-ever comprehensive data privacy law. PDPD will take effect on 1 July 2023. This article provides an overview of its crucial aspects to business managers.

Scope of application

PDPD applies to any domestic or foreign organizations or individuals involved in "processing" personal data in Vietnam, even if some processing occurs outside of Vietnam.[1]

PDPD defines "*processing of personal data*" as "one or more actions affecting personal data, such as collecting, recording, analyzing, confirming, storing, editing, publicizing, combining, accessing, logging, retrieving, encrypting, decrypting, copying, sharing, transferring, supplying, assigning, deleting, destroying personal data or other connected actions."[2] This broad definition means PDPD is likely to affect most, if not all, businesses across all industries.

Types of data covered by PDPD

PDPD covers the processing of "Personal data," defined as "*any information associated with a particular individual or helps identify an individual"* when used with other maintained data and information. Personal data could be expressed as symbols, letters, numbers, images, sounds, or digital data.[3] PDPD classified personal data into two (2) types: (i) basic personal data; and (ii) sensitive personal data, and provide a *non-exhaustive* list of each type.

(a) ***"Basic Personal Data"*** consists of: [4] family name, middle name, and first name as stated in the birth certificate, and other names (if any) of a person; date of birth; date of death or missing; gender; place of birth, place of birth registration, place of permanent, temporary or current residence, hometown, contact address; nationality; personal image; phone number; people's identity card number, personal identification number, passport number, driver's license number, license plate number, personal tax identification number, social insurance number, health insurance card number; marital status, information of family members (parents, children); digital account and online activities; and other information associated with a specific person or helping identify a particular person that is not sensitive personal data.

[1] Article 1.2 and Article 2.14 of Decree 13.
[2] Article 2.7 of Decree 13.
[3] Article 2.1 and Article 2.2 of PDPD.
[4] Article 2.3 of PDPD.

(b) **"Sensitive Personal Data"** means personal data associated with an individual's privacy that, "*when being infringed upon, shall cause a direct effect on the legitimate rights and interests of such individual*," including:[5] political and religious views; health condition and information stated in health record (excluding information on blood type); information about racial or ethnic origin; genetic data; biometric data; sex life or sexual orientation; crime records; customer information held by credit institutions, foreign bank branches, intermediary payment service providers, and other authorized organizations; geographic location; and other personal data regarded by law as specific [to a person] and require necessary security measures.

PDPD imposes additional processing and safeguarding obligations for processing sensitive personal data, so each organization needs to identify the types of personal data processed and establish a management system for different types of personal data.

Roles in processing personal data

PDPD clearly distinguishes between different types of entities engaging in personal data processing. In particular:[6]

(a) *"***Data Controller***"* is defined as an individual or organization deciding on the purpose and method of processing personal data. Data Controller has the higher responsibility to notify and cooperate with authorities in case of personal data breaches. [7] The Data Controller is ultimately accountable to the data subject and bears the burden of proving that it has consent for all processing activities.[8]

(b) *"***Data Processor**" is defined as an individual or organization engaged in data processing on behalf of a Data Controller through a contract or agreement with the Data Controller. Data Processor is responsible for notifying the Data Controller of any breaches and cooperating with the authority in case of violations and investigations. [9]

(c) ***"Data Controller cum Processor"*** is defined as an individual or organization engaged in both of the above simultaneously. Data Controller cum Processor is a hybrid role. It must comply with the obligations of both Data Controller and Data Processor.

Each role in processing personal data has separate responsibilities, so each organization needs to identify its part in processing personal data.

Rules for personal data protection

PDPD clearly sets out rules for personal data processing.

Notable rules include:

(a) **Consent:** PDPD requires that the data subject consent to all personal data processing activities unless otherwise provided for by law.[10] Consent is only valid if given through affirmative and

[5] Article 2.4 of PDPD.
[6] Article 2.9, 2.10, and 2.11 of Decree 13.
[7] Article 23.1 of Decree 13.
[8] Article 11.10, Article 38 of Decree 13.
[9] Article 23.2, and Article 39 of Decree 13.
[10] Article 11 of PDPD.

voluntary action (in writing, by voice, by ticking the consent box, indicating consent via reply text message, by selecting technical consent settings, or through another action that demonstrates this) when the data subject knows: a) The type of personal data to be processed; b) Purpose of processing personal data; c) Organizations and individuals are allowed to process personal data; d) Rights and obligations of data subjects.

The silence or non-response of the data subject is inadequate for "consent." The data subject's consent must be expressed in a format that "can be printed or reproduced in writing, including electronic or verifiable formats" (i.e., saved electronically). In the event of a dispute, the responsibility for proving the consent of the data subject lies with the Data Controller/Data Controller cum Processor.

There are limited exceptions to the consent rules, which mainly include the following:[11] emergency circumstances to protect the data subject's or another person's life or well-being; for fulfilling the contractual obligations to the data subject by relevant agencies, organizations; and other limited exceptions.

(b) **Privacy notice:** PDPD requires organizations to provide compliance notice to the data subjects before processing their data. The privacy notice shall include the purpose, type, method of processing, the identity of the data processor or third party involved, the risks of processing (consequences, unwanted damage likely to occur), and the timing (start time, end time) of data processing. [12] The privacy notice must be given in a format that can be printed and reproduced in writing, including in electronic or other verifiable form.

When processing "sensitive" personal data, the data subject must be informed that the data is considered sensitive personal data under the law.[13]

(c) **Privacy impact assessment:** PDPD requires that in all cases, from the commencement of personal data processing, the Data Controller, the Data Processor, and the Data Controller cum Processor must prepare and maintain a dossier to assess the impact of personal data processing. The dossier must include several contents, among others, cases of cross-border transfer of personal data; assessment of the effects of personal data processing; potential and unwanted consequences or damage, and measures for minimization or elimination thereof.

If a data processor is acting on behalf of a data controller, such a data processor must also formulate a separate dossier to assess the impact of personal data processing with required contents.

The dossier must always be made available for inspection and evaluation by the Ministry of Public Security (**"MPS"**). One original copy shall be submitted to the Department of Cybersecurity and Hi-tech Crime Prevention (A05) within 60 days of the processing of personal data. The dossier must be updated from time to time by the submitting entities upon any change to its content or upon request of the MPS.[14]

[11] Article 17 of PDPD.
[12] Article 13 of PDPD.
[13] Article 11.8 of PDPD.
[14] Article 24 of PDPD.

In addition, the transfer of Vietnamese citizens' data abroad for processing (a "cross-border transfer") will trigger a separate impact assessment. [15]

An appendix to the PDPD provides the required forms for submitting the dossier to assess the impact of personal data processing and cross-border data transfer.

(d) **Handling the rights of data subjects:** PDPD provides data subjects with certain rights.[16] These include the right for the data subject to be notified before the conduct of data processing; the right to consent or not consent to the processing of their personal data, except for the cases where personal data processing is not required; the right to access to view, edit or request to edit their personal data; the right to withdraw consent; the right to be provided with their personal data from the Data Controller or the Data Controller cum Processor; the right to restrict data processing, or object to the processing of their personal data; the right to request the amendment, deletion, and destruction of their personal data; and most critically, a right to bring a cause of action and seek damages for misuse of data.

Note that PDPD requires Data Controller to guarantee the data subjects these rights,[17] and any request to restrict data processing or objection to data processing or provision/revisions/deletion of personal data must be addressed within 72 hours of the request.[18] Therefore, Data Controller/Data Controller cum Processor should implement a system through which the data subjects can exercise their rights, and the appropriate personnel can receive, evaluate, authenticate, and respond to these requests.

(e) **Log records requirements:** PDPD requires Data Controller to "*record and store the system log of personal data processing*."[19]

(f) **Security measures:** PDPD specifies the security measures that must be implemented by a Data Controller, Data Processor, or Data Controller cum Data Processor.[20] These include applying management and technical measures concerning personal data processing, promulgating internal regulations on personal data protection under PDPD, and conducting cybersecurity examinations of systems and devices for processing personal data. Notably, entities processing **sensitive** personal data **must appoint specialized departments and personnel** to protect personal data and inform the Cybersecurity Department under the MPS of such departments and personnel details. Small and medium size enterprises and start-ups "not directly engaged in data processing" of sensitive personal data are exempt from this requirement for the first two years of their establishment. [21]

(g) **Reporting security breaches:** PDPD requires relevant entities to report to the MPS within 72 hours from the occurrence of certain events, including a violation of personal data protection laws, processing of personal data for improper purposes, or a failure to protect or adequately implement

[15] Article 25 of PDPD.
[16] Article 9 of PDPD.
[17] Article 38.5 of PDPD.
[18] Article 9.6(b), Article 9.8(b), Article 14.3, Article 15.2, Article 16.5 of PDPD.
[19] Article 38.2 of PDPD.
[20] Articles 26, 27, 28 of PDPD.
[21] Article 43.2 of PDPD.

the protection of the rights of data subjects.[22] In case of notifying after 72 hours, the reason for delay or late notification must be included.

PDPD also provides forms for notification of data breaches.

The impact of PDPD on Businesses

Compared to previous legislation, PDPD provides a broader scope of application and stringent legal requirements for protecting personal data. The business affected by PDPD should move quickly to ensure compliance with the PDPD, which is scheduled to take effect on 1 July 2023 without a grace period.

Please get in touch with Michael at michael.lee@dilinh.com for more information.

[22] Article 23 of PDPD.