NISHIMURA & ASAHI

西村あさひ法律事務所

Vietnam: The Government has just issued the Personal Data Protection Decree – the hottest legislation in Vietnam's data privacy practice

Asia & Data Protection Newsletter

April 21, 2023

Author:
E-mail Tomonobu Murata
E-mail Nguyen Tuan Anh

Following our last newsletter on the latest draft Personal Data Protection Decree (accessed here), the Government of Vietnam has just issued the official Personal Data Protection Decree (i.e., Decree No. 13/2023/ND-CP; the "**PDPD**"). The PDPD comprises 44 articles divided into 4 chapters and will take effect from 1 July 2023.

Below are some key PDPD takeaways:

1. **Governing subjects.** The PDPD applies to (i) Vietnamese entities and individuals, (ii) foreign entities and individuals in Vietnam, (iii) Vietnamese entities and individuals operating offshore, and (iv) foreign entities and individuals directly engaging in or relating to processing of personal data in Vietnam.

2. **Personal data and other key definitions**. Personal data means information in the form of symbols, letters, numbers, images, sounds, or equivalences in an electronic environment that is about a specific individual or helps to identify a specific individual, including basic personal data and sensitive personal data. Information that helps to identify a specific individual means information created from activities of an individual that can be used to identify such individual when combined with other data.

   Personal data includes basic personal data (e.g., full name, DOB, address, gender, phone number, ID card number, digital account information and personal images) and sensitive personal data (e.g., religious and political opinions, health information as recorded in medical examination files (excluding blood type), biometric data, financial information, sexual orientation and engagement, and location data determined via location services.).

   In addition, the PDPD introduces other key definitions, including "data subject," "data processing," "profiling," "data subject consent," "data controller," "data processor," and "data controlling and processing entity," and "overseas personal data transfer.".

3. **Principles for personal data protection**. There are eight principles for personal data protection, including principles of lawfulness, transparency, purpose limitation, minimization, accuracy, security, storage limitation, and accountability. These eight principles are relatively similar to those in the EU General Data Protection Regulation ("**GDPR**").

4. **Data subject rights**. The PDPD provides for 11 rights of a data subject. Those rights are (1) right to know, (2) right to consent, (3) right to access, (4) right to consent revocation, (5) right to erasure, (6) right to restriction of data processing, (7) right to data portability, (8) right to objection of data processing, (9) right to complaint and denouncement, (10) right to claim for compensation, and (11) right to self-defense.

A request for exercise of the rights to restriction and objection of data processing must be processed within 72 hours from the receipt of such request, unless otherwise provided by law. In addition, the PDPD provides detailed procedures and conditions for exercising certain rights such as data portability, data amendment and right to erasure.

5. **Consent of data subject**. Consent applies to all activities during data processing, unless otherwise stipulated by law. Consent must be granted voluntarily and with full data subject awareness of the data type to be processed, processing purpose, data processor or receiver, and data subject rights. For sensitive personal data, the data subject must be informed that the data to be collected is sensitive. Consent must be an affirmative act creating an explicit instruction (i.e., silence or non-objection is not consent), for instance, in writing, voice, box checking, confirmation SMS, selecting agreement options or similar forms of showing agreement.) Consent must be granted to each purpose. If there are multiple purposes, a list of purposes must be available for the data subject to consent to each individually. A consent to data processing for marketing and advertising business must be given upon the full customer awareness of the content, method, formality and frequency of the marketing and advertising activities. In case of disputes, data controllers must prove the existence of consent.

   Consent withdrawal must have the same formality as the consent (i.e., be no more complicated). In cases of consent withdrawal, the data subject must be informed of the potential consequences or damage that might occur.

6. **Processing of data without consent**. The PDPD keeps the five cases of data processing without consent mentioned in our previous newsletter unchanged, including (1) to protect the lives and health of data subjects or others in emergency cases (controllers, processors, controlling and processing entities and third parties that are allowed to process such data without data subject consent must prove eligibility therefor); (2) public disclosure of personal data under compulsion of law; (3) processing by competent authorities (i) in emergency cases of national defense, national security, social security and order, mass disaster, or dangerous epidemic; (ii) when there is a threat to national defense and security but an announcement of state emergency has yet to be made; (iii) to prevent and fight riots, terrorism, crimes and law violations; (4) to implement contractual obligations of data subjects towards relevant bodies, organizations and individuals in accordance with the law; and (5) to serve the operation of state authorities as set forth in specific laws.

   In addition, the PDPD enables competent bodies and organizations to conduct voice and video recording and process data collected in public places without data subject consent for certain purposes, including protection of national security, social safety and order and legitimate interests of organizations and individuals as long as they are informed that their voice and image are being recorded and captured.

7. **Processing of children's data**. The PDPD requires that the processing of data belonging to children age seven (7) or greater be consented to by both the target child and their parent or guardian, except for the cases mentioned in paragraph 6 above. A verification of the child's age must be conducted before processing their data.

8. **Privacy notice**. A notice on personal data processing that contains compulsory content (e.g., processing purpose, type of data to be processed, process method, information of other organizations and individuals relating to processing, possibly unexpected consequence and damage, starting time and ending time of processing) must be served to the data subject once before the processing. The notice must be in a printable format, copiable in writing, including in electronic format or other verifiable formats.

9. **Data breach notice**. In case of a data breach, the data controller and data controlling and processing entity must inform the Department for Cybersecurity and Hi-tech Crime Prevention ("**A05**"), a subordinated body of the Ministry of Public Security ("**MPS**"), of the breach (together with other compulsory content, including, among others, possible consequences and damage resultant of the breach as well as the measures implemented to mitigate and eliminate the impacts of the breach) within 72 hours of the breach and provide a reason for delay if the notice is served to A05 after such 72 hours. Additionally, the data processor must notify the data controller as early as possible after noticing the breach. The PDPD does not specify an obligation to notify data subjects of data breaches, however, it seems data subjects' right to know under the PDPD might infer such obligation.

10. **Data processing impact assessment**. Data controllers (a data processor in case of implementing a contract with a data controller) or, as the case may be, data controlling and processing entities, are required to prepare and officially issue a written dossier for data protection impact assessment that contains compulsory contents in a prescribed form (including, among others, assessment of the impact level of data processing, possibly unexpected consequences and damage, and measures for mitigating or eliminating such risks and impacts) from the commencement of processing activities. The dossier must be sent to the A05 for review and supervision within 60 days after commencement of the data processing. This dossier must be up to date and available at any time for authority inspection. In case of any change in such dossier, the updated dossier must be sent to A05.

    The PDPD provides a very broad scope of captured subjects by providing no exceptions. Hence, it seems that all businesses in Vietnam processing personal data will be required to conduct data processing impact assessments and send the results to the MPS in due course.

11. **Cross-border personal data transfer procedure**. Vietnamese' personal data can be transferred overseas if the transferor (i.e., data controller, controlling and processing entity, processor and a third party) prepares a dossier for impact assessment of overseas data transfer which contains compulsory content in a prescribed form and certain enclosures (including, among other things, consent of data subjects in line with paragraph 5 above, and binding documents stipulating the responsibilities of transferors and transferees) and complies with the following requirements:

    (1) It must make the dossier available at any time for inspection and assessment by MPS;
    (2) An original of the dossier must be sent to A05 in 60 days from the start of transferring, and if the dossier is incomplete and inconsistent with the law, A05 shall request revision of the dossier within 10 days from the date of request; and
    (3) It has notified A05 in writing of the data transfer and details of the transferee who will be in-charge of the data after completion of the transfer.

    The transferor must send an updated dossier to A05 if there is any change to the one previously submitted. MPS might conduct an inspection of cross-border data transfers once per year. More frequent inspection might be conducted if there is violation or risk of data leakage and loss. MPS might request suspension of the data transfer if the transferred data is used to infringe Vietnam's interest and security, there is non-compliance with certain requirements above or potential exists for leakage or loss of Vietnamese' data.

    The current language of the PDPD suggests that the above requirements are not applicable to overseas transfers of a foreigner's personal data regardless of the fact that he/she is living in Vietnam. More interestingly, unlike the previous published draft PDPD, the PDPD mentions no specific requirement on data localization in this case. It looks as if the data localization requirement applicable to personal data processing shall comply with Decree No. 53/2022/ND-CP guiding the cybersecurity law.

12. **Processing of sensitive personal data.** As projected in our previous newsletter, the pre-processing registration with a PDP Committee noted in the public draft is officially abolished in the PDPD. Instead, in addition to the data processing impact assessment in paragraph 10 above and general data protection requirements (e.g., compulsory issuance of internal personal data protection rules and other technical requirements), it is required to appoint a unit specializing in personal data and a person in-charge of personal data protection and to inform MPS (i.e., A05) of such unit and person. Although the PDPD does not mention any clearer requirements concerning such persons, we think that they might play the same role as a data protection official - DPO under the GDPR.

    The PDPD allows some specific enterprises, e.g., super small, small, medium-size enterprises and start—up enterprises, except for those directly engaged in data processing business, to enjoy a relaxation of this requirement during their first two years of establishment.

13. **Introduction of the National Portal for Personal Data Protection**. MPS is assigned to build and operate a portal that contains information relating to personal data protection, including receiving notice of data breaches.

The introduction of the PDPD is a strong data protection action, setting the first solid brick to create a centralized legal framework on personal data protection aligning with regional and international practices and standards. Nonetheless, we think that in order to make the PDPD come to life effectively and smoothly, practical guidance from the governmental authorities, in particular the MPS, is necessary given certain ambiguities in the PDPD (e.g., the time-limits for conducting data breach notices or sending data processing impact assessment dossiers to A05 if a controller has been processing personal data before 1 July 2023).

Should you want to know further details about the newly issued PDPD, please contact us.

Public Relations Section, Nishimura & Asahi E-mail✉