New decree on personal data protection: implications for enterprises

Ngoc Hoang

Issuance of new Decree

Right upon the enactment of the Cyber Security Law in 2018, the Government, in particular the Ministry of Public Security ("**MPS**"), began drafting a new decree on personal data protection. After a long period of preparation with multiple rounds of collecting public opinions, on 17 April 2023, the Government issued Decree 13/2023/ND-CP on personal data protection ("**Decree 13**") that will come into effect as of 1 July 2023. Decree 13 will reinforce the existing regulations on personal data protection and introduce new concepts and regulations, which help to address pending matters and to bring the regulations on personal data protection of Vietnam closer to the international regulations such as GDPR. However, it will certainly create a huge burden for both onshore and offshore enterprises.

Enterprises' obligations to protect personal data

Personal data is defined by Decree 13 to be any information that is expressed in the form of symbol, text, digit, image, sound or in similar form, in an electronic environment that is associated with a particular natural person or helps identify a particular natural person. Notably, it is the first time the concept of "personally identifiable information" is introduced, which is *"any information being formed from the activities of an individual and, when used with other archived data and information, can identify such particular natural person"*. This definition substantially broadens the scope of personal data to cover not only the information that directly identifies one individual but also the information that can identify a person in combination with other information.

Personal data is categorized into basic personal data (e.g., name, date of birth, gender, nationality, personal photos, marital status, family relations, phone number, a person'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, etc.) and sensitive personal data (e.g., health status, criminal record, etc.).

In the light of the scope of application and definition of personal data, it appears that Decree 13 will apply to most enterprises regardless their scale and registered business lines because they will, at the least, receive and process personal data of their employees. If an enterprise only determines the purposes of and measures for processing personal data, it will be named "personal data controller". If the enterprise, at the same time, directly processes the personal data, it will be named "personal data controller-cum-processor".[1] In practice, an enterprise will be either a personal data controller or a personal data controller-cum-processor. In addition to general obligations such as notification and cooperation with competent authorities to deal with breaches of personal data protection, below are the main specific tasks that an enterprise must undertake under Decree 13.

(1) Obtaining the consent of data subject for the data processing

The term "personal data processing" under Article 2 of Decree 13 encompasses various activities affecting personal data: *"obtaining, recording, analysis, confirmation, storage, alteration, publicity, combination, access, retrieval, recovery, encryption, decryption, duplication, sharing, transmission, provision, transfer, deletion, destruction of personal data or other relevant operations"*. Save for particular circumstances prescribed in Article 17 of Decree 13, the enterprise will need to notify and obtain the consent of the data subject before processing the data subject's data. Pursuant to Article 11, consent is required for all activities to be engaged in during the course of personal data processing, and is only valid when the data subject voluntarily agrees, upon knowing of the categories of the data to be processed, the purpose of the data processing, the organization or individual processing personal data, and the data subject's rights and obligations. The consent must be clearly and specifically expressed by written instrument, by voice, by ticking a consent box, by text message, by selecting technical settings,

1 In this article, we do not refer to the personal data processor (i.e., enterprise providing data processing services to the personal data controller under an agreement).

or by another equivalent action. The consent must be in the format that can be printed and/or reproduced in writing. The data subject must be able to give consent to one or multiple processing purposes if there are multiple purposes. This may be partial or conditional consent. Silence or non-response by the data subject cannot be regarded as their consent.

Regarding enterprises providing marketing services or advertising services, their customers must consent to the processing by such enterprises of the customers' personal data, with respect to the provision of the marketing services and to the introduction of the advertising products, on the basis that these customers know about the contents, methods, forms, and frequency in respect of the product introduction.

Notably, Article 11.11 of Decree 13 stipulates that the data subject may, pursuant to the Civil Code, empower another individual or organization to work with the data controller or data controller-cum-processor in connection with the processing of the data subject's data. Similarly, Article 17.4 allows the processing of personal data without the consent of the data subject if its purpose is to perform the data subject's contractual obligations to other individuals or organizations. Those provisions will provide enterprises with leeway to be more flexible in processing or engaging a third party to process personal data.

(2) Technical and managerial measures

The enterprise must implement organizational and technical measures and appropriate safety and security measures to prove that data processing activities have been carried out in accordance with the applicable regulations. Such measures must be appropriately monitored and updated. In particular, the enterprise must set up a department in charge of protecting personal data and appoint personnel in charge of personal data protection.

(3) Issuance of internal rules

Pursuant to Articles 27 and 28 of Decree 13, the enterprise must develop and issue policies on the protection of personal data. This can be understood as a type of internal rules that clearly specify the tasks that the enterprise or its functional units (e.g., human resources department, sales department, IT department) must perform in order to comply with the regulations on personal data protection.

(4) Archive of personal data processing

Recording and archiving a system log for personal data processing is a new requirement under Decree 13. However, Decree 13 does not provide any form or template for the system log. It is likely that enterprises will, pursuant to their own conditions and demands, create their own logs to record the processing of personal data.

(5) Preparing and maintaining a dossier for assessment of impact of personal data processing (AIPDP)

The enterprise must prepare an AIPDP when it starts processing personal data, and the AIPDP must contain the following:

- enterprise's information and contact details, as well as the full name and contact details of its unit and staff in charge of personal data processing;
- description of purposes and types of personal data to be processed;
- time required for personal data processing; estimated time for removal or destruction of personal data (if any);
- circumstances of cross-border transfer of personal data;
- description of data protection measures;
- assessment of the impact of personal data processing; potential and undesirable consequences and/or damage, and measures for minimization or elimination thereof.

The AIPDP must be in the form of a written instrument that has legal validity. Although Decree 13 does not explain how an AIPDP is considered to have legal validity, a logical understanding is that it must be approved in accordance with the charter and internal rules of the enterprise (e.g., it must be approved by the Board of Management and/or signed by the legal representative in accordance with the charter of enterprise). A copy of the AIPDP must be made available (i.e., kept in the enterprise's head office) for assessment and inspection by the MPS. The enterprise must send one copy of the AIPDP to the Department of Cybersecurity and High-Tech Crime Prevention and Control ("**A05**") under the jurisdiction of the MPS, within 60 days from the date on which it processes the personal data.

A05 will review and request the enterprise to complete the AIPDP if it fails to satisfy the regulatory requirements. Decree 13 does not specify the timeframe within which A05 must review the document and send notification of its requests (if any); thus, it will be troublesome if, as seems to be the case, A05 may, subject to its own assessment, request the enterprise to revise the AIPDP at any time. In addition, the enterprise must update its AIPDP and send an updated copy to A05 when there is any change to the submitted AIPDP.

(6) Transfer of personal data abroad

Transfer of personal data abroad is defined in Article 2.14 to be the activity of using cyberspace, equipment, electronic means or other forms of transferring personal data of Vietnamese citizens to a location outside Vietnam, or using a location outside Vietnam for the processing of personal data of Vietnamese citizens, including: (i) transfer of personal data of Vietnamese citizens to offshore organizations for their processing; and (ii) using an automatic system located outside Vietnam to process the personal data of Vietnamese citizens. Such transfer must be in line with the purposes agreed with the data subjects. This regulation does not refer to the transfer of personal data of foreigners.

The enterprise sending personal data abroad must prepare a dossier assessing the impact of transferring personal data abroad ("**AIPDT**") that contains the following:

- enterprise's information and contact details, as well as the full name and contact details of its unit and staff in charge of transferring and receiving the personal data of Vietnamese citizens;
- description and explanation of compliance with Decree 13 and details of the protection measures that have been used;
- assessment of the impact of the personal data processing; unexpected consequences and damage that may occur, as well as the prevention measures in relation thereto;
- the consent of the data subject;
- documents evidencing the binding obligations/responsibilities, as between the personal data sender and receiver, regarding the personal data processing.

The AIPDT dossier must be made available for inspection or assessment by A05 and submitted to A05 within 60 days from the date on which the personal data is processed. A05 may request the enterprise to update or supplement the AIPDT, and the enterprise must fulfill this obligation within 10 days.

Upon its successful transfer of personal data abroad, the enterprise must notify A05 of its data transfer and of the contact details of the individual or unit in charge of date transfer. It is unclear whether the enterprise may notify A05 of its transfer of personal data periodically (e.g., semi-annually, annually) with respect to personal data of the same type, to be transferred abroad, or whether the enterprise needs to notify A05 upon its completion of every transfer. Further guidance from the MPS is awaited.

Conclusion

While the influence of the Cyber Security Law over the enterprise community seems not to be as strong as the legislators' expectation, Decree 13, which stipulates specific and clear requirements, will obviously have considerable impact on their operation. Save for micro-enterprises, small enterprises, medium-sized enterprises, and start-up enterprises, which are entitled to choose to be exempted from the requirement with respect to the designation of personnel and of a unit in charge of personal data protection for the first two (2) years from their date of establishment,[2] Decree 13 applies to all other enterprises from its effective date. Thus, the relevant enterprises, especially foreign invested enterprises having regular information exchange with their parent companies and engaging in cross-border transfer of personal data, need to put in place appropriate technical measures as well as to designate departments and personnel in charge of personal data protection.

In addition, to enhance compliance with the regulations on cyber security in general and the regulations on personal data protection in particular, the Government is drafting a decree on administrative sanctions with respect to the cyber security sector. The draft decree that was available for public opinion reserves a separate chapter to prescribe the administrative sanctions applicable to violation of the regulations on personal data

2 This exemption does not apply if those enterprises provide personal data processing services.

protection. It is expected that this draft decree will be enacted shortly.

End

www.noandt.com

NAGASHIMA OHNO & TSUNEMATSU

JP Tower, 2-7-2 Marunouchi, Chiyoda-ku, Tokyo 100-7036, Japan
Tel: +81-3-6889-7000 (general) Fax: +81-3-6889-8000 (general) Email: info@noandt.com

Nagashima Ohno & Tsunematsu is the first integrated full-service law firm in Japan and one of the foremost providers of international and commercial legal services based in Tokyo. The firm's overseas network includes locations in New York, Singapore, Bangkok, Ho Chi Minh City, Hanoi, Jakarta and Shanghai, and collaborative relationships with prominent local law firms throughout Asia and other regions. The over 500 lawyers of the firm, including about 40 experienced attorneys from various jurisdictions outside Japan, work together in customized teams to provide clients with the expertise and experience specifically required for each client matter.

Singapore Office
(Nagashima Ohno & Tsunematsu Singapore LLP)

6 Battery Road Level 41
Singapore 049909
Tel: +65-6654-1760 (general)
Fax: +65-6654-1770 (general)
Email: info-singapore@noandt.com

Bangkok Office
(Nagashima Ohno & Tsunematsu (Thailand) Co., Ltd.)

34th Floor, Bhiraj Tower at EmQuartier
689 Sukhumvit Road, Klongton Nuea
Vadhana, Bangkok 10110, Thailand
Tel: +66-2-302-4800 (general)
Fax: +66-2-302-4899 (general)
Email: info-bangkok@noandt.com

HCMC Office
(Nagashima Ohno & Tsunematsu HCMC Branch)

Suite 1801, Saigon Tower
29 Le Duan Street, District 1
Ho Chi Minh City, Vietnam
Tel: +84-28-3521-8800 (general)
Fax: +84-28-3521-8877 (general)
Email: info-hcmc@noandt.com

Hanoi Office
(Nagashima Ohno & Tsunematsu Hanoi Branch)

Suite 10.04, CornerStone Building
16 Phan Chu Trinh, Hoan Kiem District
Ha Noi City, Vietnam
Tel: +84-24-3266-8140 (general)
Fax: +84-24-3266-8141 (general)
Email: info-hanoi@noandt.com

Jakarta Office (*Associate office)
(IM and Partners in association with
Nagashima Ohno & Tsunematsu)

Jakarta Mori Tower 14th Floor, Unit 1401
Jalan Jenderal Sudirman Kav. 40-41
Jakarta 10210, Indonesia
Tel: +62-21-25098080 (general)
Fax: +62-21-25098090 (general)
Email: info-jakarta@noandt.com

Shanghai Office
(Nagashima Ohno & Tsunematsu
Shanghai Representative Office)

21st Floor, One ICC, 999 Middle Huaihai Road
Xuhui District, Shanghai 200031, China
Tel: +86-21-2415-2000 (general)
Fax: +86-21-6403-5059 (general)
Email: info-shanghai@noandt.com

For more details on our global practice