LAW UPDATE PAPER
Vision & Associates Legal
28 April 2023

New regulations on personal data protection in Vietnam

On 17 April 2023, the Government issued the long-awaited Decree No.13/2023/ND-CP ("Decree 13") on Personal Data Protection. This Decree is the first-ever comprehensive legal document regulating personal data protection in Vietnam, which provides new requirements for collecting and processing personal data. Decree 13 will take effect on 1 July 2023. Below are some notable issues from Decree 13.

1. Scope of application

Decree 13 has an extra-territorial scope of application, which shall cover nearly all types of both Vietnam-based and foreign individuals and entities directly participating in or relating to data processing activities in Vietnam.

2. Classification of personal data

Decree 13 has inherited from previous definitions of personal information specified in various legal documents, and developed a new and extended definition of personal data, as quoted below:

"*Personal data means information in the form of signs, letters, numbers, images, sounds or other similar forms on the electronic environment, which is attached to a specific individual or helps identify a specific individual."*

In addition, Decree 13 has finally provided an ever specific definition of the term "*information helps identify a specific individual*", which means information derived from an individual's activity that, when combined with other stored data and information can identify a particular person.

In brief, personal data are classified by Decree 13 into two major groups:

(a) *"basic personal data"*, which include, inter alia:

(i) Image of the individual;
(ii) Driver's license number, license plate number;
(iii) Marital status;
(iv) Information on family relationships (parents, children); and
(v) Information about the individual's digital account; personal data reflecting activities, history of activities on cyberspace.

and

(b) *"sensitive personal data*", which include, inter alia:

(i) Political views, religious views;
(ii) Health status and private life recorded in the medical record, excluding information about blood type;
(iii) Information related to racial or ethnic origin;
(iv) Information about inherited or acquired genetic characteristics of the individual;
(v) Information about the individual's physical attributes and biological characteristics;
(vi) Information about an individual's sex life and sexual orientation; and
(vii) Location data of an individual identified through location services.

3. Classification of processing entities

Decree 13 has introduced four new concepts of processing entities, which include:

(a) Personal Data Controller meaning organizations or individuals who decide the purposes and means of processing personal data ("**Data Controller**");
(b) Personal Data Processor meaning an organization or individual that performs data processing on behalf of the Personal Data Controller, through a contract or agreement with the Personal Data Controller ("**Data Processor**");
(c) Personal Data Controller cum Processor meaning an organization or individual who simultaneously decides the purposes, means and directly processes personal data ("**Data Controller cum Processor**"); and
(d) Third Party meaning an organization or individual other than the Data Subject, Data Controller, Data Processor, Data Controller cum Processor that is authorized to process personal data.

In which, stricter requirements are applied to the Data Controller and the Data Controller cum Processor.

4. Consent requirements

Decree 13 has specifically defined "**consent**" to be a clear, voluntary, and affirmative expression of the data subject's permission to process personal data. In particular, the data subject's consent must be made in writing, by voice, by ticking the consent checkbox, by consent messages, by selecting consent technical settings, or by other methods that can express such consent.

The Data Subject's consent is only valid when he/she voluntarily and clearly 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; and (d) Rights and obligations of Data Subjects.

Furthermore, such data subject's consent must also be expressed in a format that is printable and able to be copied in writing.

On the other hand, Decree 13 also provides the following exceptions where the data subject's consent is not required for data processing:

(a) In urgent cases where it is necessary to immediately process relevant personal data in order to protect the life and health of the data subject or others. The Data Controller, Data Processor, Data Controller cum Processor, Third Party are responsible for the burden of proof;
(b) The disclosure of personal data in accordance with the laws;
(c) The processing of data by competent state agencies in the event of a state of emergency on national defense, security, social order and safety, major disasters or dangerous epidemics; when there is a risk of threatening security and national defense but not to the extent of declaring a state of emergency; to prevent and combat riots and terrorism, to prevent and combat crimes and violations of the law in accordance with the law;
(d) To fulfill the contractual obligations of the data subject with relevant agencies, organizations and individuals as prescribed by law; and
(e) To serve the activities of State agencies prescribed by specialized laws.

5. Data Processing Impact Assessment

Decree 13 requires the Data Controller, Data Processor, and Data Controller cum Processor to formulate and store a personal data processing assessment dossier ("**Data Processing Dossier**") in writing, which must always be available to serve the inspection and assessment by the Ministry of Public Security ("**MoPS**"). Such assessment shall be made according to standard form prescribed in an Appendix attached to Decree 13 at the time they start processing personal data.

Furthermore, an original of the Date Processing Dossier must be sent to the Department of Cybersecurity and Prevention of Crimes Using High Technologies directly managed by the MoPS (the "**Cybersecurity Department**") within 60 days from the date of processing.

The Data Controller, the Data Controller cum Processor, and the Data Processor shall update and supplement the Data Processing Dossier according to standard form prescribed in an Appendix to Decree 13 when there is a change in the contents of the dossier already sent to the Cybersecurity Department.

6. Notification of personal data processing

Decree 13 requires the Data Controllers and the Data Controller cum Processors to notify the Data Subjects of their personal data processing, and the notice thereof must contain statutory contents, be made once prior to the personal data processing, and be expressed in a format that is printable and able to be copied in writing.

7. Notification of personal data breach

Decree 13 requires individuals and organizations to notify the Cybersecurity Department upon detection of a violation of personal data regulations. Unlike the current regulations, which require a "prompt notification", Decree 13 sets a time limit of 72 hours for notification of such violation.

8. Stricter requirements for cross-border data transfer

Decree 13 has introduced new requirements applied to cross-border data transfer, which has been an unregulated sector before its issuance. In particular, in case where the data is intended to be transferred outside of Vietnam, any processing entities, including Third Party, that conduct a cross-border transfer of data are required to perform the following obligations:

(a) Formulating an Overseas Data Transfer Impact Assessment dossier ("**Data Transfer Dossier**") in standard form;
(b) Submitting 01 original of the Data Transfer Dossier to the Cybersecurity Department within 60 days from the date of processing, which shall evaluate and may request to complete if founding out such Dossier is incomplete and does not conforms to regulations;
(c) Notifying the Cybersecurity Department of the data transfer and contact details of the organization or individual in charge thereof in writing after a successful transfer; and
(d) Updating and supplementing such Data Transfer Dossier according to statutory form when there is a change in the contents of this dossier already sent to the Cybersecurity Department within 10 days from the date of request.

9. Data Protection Staff appointment

Sensitive data processing entities must designate a personal data protection unit and personnel and notify the Cybersecurity Department. In case where a processing entity is an individual, the information on the implementing individual shall be notified.

10. Personal Data Protection Agency

Decree 13 designates the Cybersecurity Department as the specialized Personal Data Protection Agency, which is responsible for assisting the MoPS in performing the state management on nation-wide data protection in Vietnam.