


The Personal Data Protection Decree

Are you ready for it?

Legal Update | April 2023



After more than two years since the first introduction of the draft in 2021, the Decree on Personal Data Protection, Decree No. 13/2023/ND-CP (*Decree 13*), was finally promulgated on 17 April 2023. In this legal update, we would like to highlight some remarkable provisions under Decree 13.

In this Issue

- I. Regulated stakeholders
- II. Consents from the data subjects
- III. Sensitive personal data
- IV. Consents from other persons
- V. Data processing without the data subject's consent
- VI. Rights of the data subject
- VII. Personal data protection in marketing and advertisement business
- VIII. Breach notification
- IX. Cross-border data transfer
- X. Measures for ensuring the personal data protection
- XI. Effect

I. Regulated stakeholders

Decree 13 provides definitions of the main parties involved in data processing as follows:

- a. Personal data controller means an organisation or an individual deciding on the purpose(s) and means by which personal data is processed. (**Data Controller**).
- b. Personal data processor means an organisation or an individual processing data on behalf of the data controller through a contract or agreement with the data controller (**Data Processor**).
- c. Personal data controlling and processing entity means an organisation or an individual who decides the purpose(s) and means of processing personal data, as well as directly processes personal data (**Data Controlling and Processing Entity**).
- d. Third-party means any organisation or individual, other than the data subject, Data Controller, Data Processor and Personal Data Controlling, and Processing Entity, that is permitted to process personal data (**Third Party**).

Compared to the latest draft version, Decree 13 has extended its categories of regulated subjects. Accordingly, among others, Decree 13 recognises the concept of “Data Controller”, which is substantially similar to the definition provided in the General Data Protection Regulation (**GDPR**).

II. Consents from the data subjects

Under Decree 13, except for certain limited cases, the data subjects’ consent is required for all activities falling within personal data processing. The data subjects’ consent will be valid only if the data subjects voluntarily and clearly understand the following:

- a. Type of personal data to be processed;
- b. Purpose(s) of personal data processing;
- c. Organisations and individuals that are entitled to process personal data; and
- d. Rights and obligations of the data subjects.

In addition, the data subjects’ consent must:

- a. Be given and specified in writing, orally, or by ticking a consent box, or through the syntax that reflects consent via text message, or by selecting a technique that reflects consent, or by performing another action that signifies consent;
- b. Be made for the same purposes. When there are multiple purposes, the Data Controller, Data Controlling, and Processing Entity shall list down the relevant purposes so that the data subjects may provide their consents to one or more purposes on the list; and

- c. Be expressed in a format that can be printed, or copied in writing, including in electronic or verifiable formats.

Partial consent is allowed under Decree 13.

Decree 13 clearly provides that silence or non-response by a data subject shall **not** constitute consent.

III. Sensitive personal data

In case of processing sensitive personal data, it is mandatory that the data subject shall receive notification thereof. Sensitive personal data refer to personal data in association with individual privacy which, when infringed, will directly affect an individual's legal rights and interests, including:

- a. Political and religious opinions;
- b. Health condition and personal information stated in health records, excluding information on blood type;
- c. Information about racial or ethnic origin;
- d. Information about genetic data related to an individual's inherited or acquired genetic characteristics;
- e. Information about the individual's physical attributes and biological characteristics;
- f. Information about an individual's sex life or sexual orientation;
- g. Data on crimes and criminal activities collected and stored by law enforcement agencies;
- h. Information on customers of credit institutions, foreign bank branches, payment service providers, and other licensed institutions, including customer identification as prescribed by law, accounts, deposits, deposited assets, transactions, organisations and individuals that are guarantors at credit institutions, bank branches, and payment service providers;
- i. Personal location identified via location services; and
- j. Other specific personal data as prescribed by law that requires special protection.

IV. Consents from other persons

Decree 13 provides 2 (two) exceptions whereby data processing requires the consent of other persons:

- a. If the data subject has been declared missing or deceased, the data processing of personal data in this case requires the consent of their family members (i.e. spouse, parents). If the data subject has no family member, it is then considered as no consent can be given and therefore, the processing is not permitted.
- b. If the data subject is a child 7 years of age or older, consent from such child and his/her parent or guardian must be obtained before the data processing.

V. Data processing without the data subject's consent

Article 17 of Decree 13 provides 5 (five) circumstances whereby personal data can be processed without the data subject's consent, including:

- a. In an emergency, whereby the processing of relevant personal data must be completed immediately in order to protect the data subject's or others' life and health;
- b. Disclosure of personal data as prescribed by law;
- c. The data processing conducted by competent authorities in case of emergency in connection with national defence, security, social order and safety, major disasters, or dangerous epidemics; when there is a risk of threat to security and national defence but short 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 fulfil the contractual obligations of the data subjects with relevant agencies, organisations, and individuals as prescribed by law; and
- e. To serve the operation of the relevant state authorities as prescribed by law.

The above exceptions related to consents are quite similar to those provided under the GDPR. A notable difference between GDPR and Decree 13 is that Decree 13 does not adopt "processing [being] necessary for the purposes of the legitimate interests pursued by the controller or by a third party" as an exemption to the requirement of consent.

VI. Rights of the data subject

Article 9 of Decree 13 provides 11 (eleven) rights of the data subjects, including:

- a. Right to be informed;
- b. Right to give consent;
- c. Right to access;
- d. Right to withdraw consent;
- e. Right to delete;
- f. Right to restrict data processing;
- g. Right to be provided with data;
- h. Right to object to data processing;
- i. Right to bring complaints, denounce, and initiate lawsuits;
- j. Right to claim compensation for damage; and
- k. Right to self-defence.

These rights are quite similar to those provided under the GDPR except that the GDPR does not provide for the right to self-defence

and the right of data portability under the GDPR does not appear in Decree 13.

Another significant distinction is that Decree 13 establishes a strict deadline for the Data Controller to enforce certain rights of the data subjects. In particular, the Data Controller is required to implement the right to restrict data processing, and the right to object to data processing within 72 hours upon the receipt of the request of the data subject. This limited time frame will definitely place a burden on the Data Controller, especially if they have to deal with excessive and extensive requests at the same time.

VII. Personal data protection in marketing and advertisement business

Processing the personal data of customers for purposes of providing marketing and advertising services requires consents from the customers, on the basis that the customers know the contents, methods, forms, and frequency of the introduction, marketing, and advertising of the products.

VIII. Breach notification

Under Article 23 of Decree 13, organisations and individuals shall notify the Department of Cybersecurity and High-tech Crime Prevention (**DCHCP**) under the Ministry of Public Security upon detecting the following cases:

- a. There is a breach of the law with respect to personal data;
- b. Personal data is processed for wrong purposes, not in accordance with the original agreement between the relevant data subject and the Data Controller, the Data Controlling and Processing Entity, or it violates the provisions of the laws;
- c. The data subject's rights are not guaranteed (or properly guaranteed and protected?) or are not properly implemented; and
- d. Other cases as prescribed by law.

The language of this provision is rather broad enough to cover any situation involving a breach of personal data. We note that a notification must be delivered to the DCHCP within 72 hours upon the detection of any of the aforementioned breaches. In case of notification made after 72 hours, the reason for late notification must be included.

IX. Cross-border data transfer

Cross-border transfer of personal data of Vietnamese individuals must satisfy the following main requirements:

- a. The transferor must prepare a dossier for assessment of the impact of cross-border transfer of personal data that shall include the following contents (among others): a) the data subjects' consent, and b) legally binding agreement(s) between the transferor and transferee;
- b. The transferor must keep the dossier readily accessible at all

times for the inspection and evaluation by the DCHCP and must send one (1) original copy to such department within sixty (60) days from the date of processing of personal data; and

- c. The transferor must notify the DCHCP of the information on the data transfer and the contact details of the responsible organisation, and individual in writing after the data transfer has taken place successfully.

Compared to the latest draft version, Decree 13 has removed the requirements regarding (i) a document proving the data-receiving country has data protection regulations similar to or higher than the laws of Vietnam; and (ii) a written approval from the Personal Data Protection Commission of Vietnam, which, in sum, could ease the burden on data transferors, giving them more liberty and flexibility.

Article 25 also specifies the following circumstances in which the Ministry of Public Security may request the data transferor to suspend its cross-border data transfer activities:

- a. When it is discovered that the transferred personal data is used for activities that violate the interests and national security of the Socialist Republic of Vietnam;
- b. The data transferor fails to complete the dossier for assessment of the impact of cross-border data transfer at the request of the DCHCP; and
- c. There has been an incident of unauthorised disclosure or loss or leaking of personal data of Vietnamese citizens.

We note that there are no similar protections for the cross-border data transfer of personal data of non-Vietnamese citizens living or transiting in Vietnam.

X. Measures for ensuring the personal data protection

Measures for ensuring personal data protection must be put in place from the commencement of and throughout the personal data processing cycle. These measures include (i) management and technical measures implemented by entities related to personal data processing; (ii) measures implemented by the competent authority; (iii) investigation and procedural measures taken by the competent authority; and (iv) other measures in accordance with the laws.

Decree 13 also provides specific actions with regard to each type of personal data. We refer specifically to sensitive personal data where Decree 13 mandates the designation of a department and personnel in charge of personal data protection (**Data Protection Department/Officer**) and provide their information to the specialised personal data protection authority (to be created by the relevant state authority).

XI. Effect

Decree 13 will come into force on 1 July 2023. Accordingly, all related entities shall comply with the regulations of Decree 13 as of 1 July 2023, except for the requirements on the designation of Data Protection Department/Officer. We note that this exception only applies to enterprises within the first 2 years of incorporation if they satisfy the following conditions:

- a. Being micro-enterprises, small enterprises, medium enterprises, and start-ups; and
- b. The mentioned enterprises must not directly engage in personal data processing activities.

Frasers Law Company | April 2023

Author



Duong Thi Mai Huong
Senior Associate
huong.duong@frasersvn.com

Ho Chi Minh City

Unit 19.01, 19th Floor, Deutsches Haus
33 Le Duan Boulevard, District 1
Ho Chi Minh City, Vietnam
Tel: +84 28 3824 2733

Email: legalenquiries@frasersvn.com

Hanoi

Unit 1205, 12th Floor, Pacific Place
83B Ly Thuong Kiet Street, Hoan Kiem District
Hanoi, Vietnam
Tel: +84 24 3946 1203

Website: www.frasersvn.com

This article provides a summary only of the subject matter covered, without the assumption of a duty of care by Frasers Law Company. The summary is not intended to be nor should it be relied on as a substitute for legal or other professional advice.