SOME HIGHLIGHTS OF THE DECREE ON PERSONAL DATA PROTECTION

HUYEN THU

On April 17, 2023, the Government issued Decree 13/2023/ND-CP on personal data protection (**Decree 13**) with the goal of meeting requirements on protecting personal data rights, preventing acts of infringing personal data and affecting the rights and interests of individuals and organizations. In particular, Decree 13 recognizes the definition of "personal data", and comprehensively recognizes the basic rights of Data Subjects, and the responsibilities of enterprises processing and controlling data. In addition, the functions and competence of the department in charge of personal data protection, abroad transfer of personal data, and measures for protecting personal data, etc. are also specified in this Decree. The followings are some outstanding contents of Decree 13:

Firstly, defining and classifying personal data. Decree 13 stipulates that personal data is information in the form of symbols, letters, numbers, images, sounds, or similar forms in the electronic environment that are associated with a certain individual or used to identify an individual. Also, personal data is classified into two groups of "basic personal data" and "sensitive personal data", specifically:

- Basic personal data as stipulated in clause 3, Article 2 of Decree 13 includes such information as first name, middle name, birth name, other names (if any); gender; nationality; individual photos; phone number, ID Card number, and personal identification number.
- Sensitive personal data as stipulated in clause 4, Article 2, Decree 13 is personal data associated with individual privacy rights which will directly affect an individual's legal rights and interests once it is infringed, including such information as political perspective, religious perspective, and information related to racial or ethnic origin.

Secondly, stipulating the rights of Data Subjects. According to Decree 13, a Data Subject is an individual presented by personal data. The rights of a Data Subject gather many rights of individuals to

data, including 11 rights: Right to be informed; Right to give consent; Right to access; Right to withdraw consent; Right to delete data; Right to restrict data processing; Right to file complaints, denunciations, and lawsuits; Right to provide data; Right to object to data processing; Right to claim damages; Right to self-protection. In general, in accordance with Decree 13, the consent of Data Subjects (the clear and voluntary presentation by the data subject to affirm permit for the processing of their personal data) applies to all activities within the procedure of personal data processing; however, in some cases of processing personal data, the consent of Data Subjects is not requested, namely:

- Immediately processing relevant personal data in emergency cases to protect the life and health of Data Subjects or others (it should be noted that Personal Data Controllers, Personal Data Processors, Personal Data Controller-cum-Processors, and the Third Parties are responsible for proving the emergency in this case);
- Disclosing personal data under the law;
- Processing data by competent state agencies in case of national defense emergency, national security, social order and safety, major disasters, or dangerous pandemics; when there is a risk threatening security and national defense but not to the extent of declaring a state of emergency; in case of prevention and fight against riots and terrorism, crimes and law violations by law;
- Performing obligations under a contract of the Data Subject with relevant agencies, organizations, and individuals by law;
- Serving activities of state agencies prescribed by specialized laws;
- Processing personal data obtained from audio and video recordings in public places.

Thirdly, stipulating responsibilities of Personal Data

Controllers, Personal Data Processors, and Personal Data Controller-cum-Processors in the process of controlling and processing personal data. Accordingly, Decree 13 specifies the responsibilities of data controllers, data processors, and relevant third parties to ensure the protection of personal data during personal data processing in Articles 38 to 40, for example:

- The Personal Data Controller is responsible for performing appropriate organizational and technical measures with safety and security to demonstrate that the data processing activities have been implemented in accordance with the regulations on protecting personal data, and also reviewing and updating these measures if necessary.
- The Personal Data Processor only receives personal data after signing a contract or an agreement on data processing with the Personal Data Controller; handles personal data according to the contract or agreement signed with the Personal Data Controller.

In addition to the above responsibilities, Personal Data Controllers, and Personal Data Controller-cum-Processors must conduct and save the dossier of personal data processing impact assessment from the time of starting to process personal data (with the document contents specified in clause 1, Article 24, Decree 13). Personal Data Processors shall conduct and save the dossier of the personal data processing impact assessment in the case of performing a contract with the Personal Data Controller (with the document contents specified in clause 2, Article 24, Decree 13). The dossier of impact assessment of personal data processing must be available for inspection and evaluation by the Ministry of Public Security and sent to the Department of Cyber Security and Hi-tech Crime Prevention under the Ministry of Public Security, the department in charge of protecting personal data, within 60 days from the date of processing personal data.

Also, the rights and responsibilities of Personal Data Controllers, Personal Data Processors, and Personal Data Controller-cum-Processors are stipulated scatteredly in many other clauses such as the right to edit personal data of Personal Data Processors, the Third Parties in Article 15, the responsibility to delete personal data which cannot be restored of Personal Data Controllers, Personal Data Controller-cum-Processors, the Third Parties stipulated in clause 7, Article 16.

Fourthly, stipulating the abroad transfer of personal data. According to Decree 13, abroad transfer of personal data is an activity using cyberspace, electronic equipment, tools, or other forms of transferring personal data of Vietnamese citizens to a location outside the territory of Viet Nam or using a location outside the territory of Viet Nam to handle personal data of Vietnamese citizens, including the case that:

(i) Organizations, enterprises, and individuals transfer the personal data of Vietnamese citizens to foreign organizations, enterprises, and management departments for processing in relevance to the purposes consented by Data Subjects;

(ii) Vietnamese citizens' personal data is processed through automated systems located outside Viet Nam of Personal Data Controllers, Personal Data Controller-cum-Processors, and Personal Data Processors processing in relevance to the purposes consented by Data Subjects.

It should be noted that when transferring personal data of Vietnamese citizens abroad, the Parties transferring data abroad (including Personal Data Controllers, Personal Data Processors, Personal Data Controller-cum-Processors, and the Third Parties) must prepare the dossier of impact assessment of transferring personal data abroad (with contents specified in clause 2, Article 25, Decree 13), and submit the original dossier to the Department of Cyber Security and Hi-tech Crime Prevention, as well as send a written notification to this department about this transfer and detailed contact information of the organization or individual in charge when the data is transferred successfully. Notably, based on the specific situation, the Ministry of Public Security shall decide to inspect the transfer of personal data abroad once a year, except for the case of detecting violations of the law on personal data protection in Decree 13 or the case of revealing or losing a Vietnamese citizen's personal data.

Fifthly, stipulating measures to protect personal data. According to Decree 13, to avoid the illegal collection, transfer, and trading of personal data, organizations and individuals related to personal data processing must perform personal data protection measures to prevent the unauthorized collection of personal data from their systems, equipment, and services. In addition, measures to protect personal data must be described specifically in the impact assessment dossier of personal data

processing and transferring personal data abroad when the dossier is submitted to the Ministry of Public Security for approval; and must be applied at the beginning of and throughout the personal data processing. The measures to protect personal data specified in this Decree comprise:

- Management measures taken by organizations and individuals related to personal data processing;
- Technical measures taken by organizations and individuals related to personal data processing;
- Measures taken by competent state management agencies by this Decree and relevant laws;
- Investigative and procedural measures taken by competent state agencies;
- Other measures as prescribed by law.

COMMENTS AND RECOMMENDATIONS

The promulgation of Decree 13 is considered as a breakthrough, creating a legal framework to protect personal information and data, raising the parties' awareness and responsibility on personal data protection, and avoiding disclosing, appropriating, and trading personal data. Decree 13 will take effect from July 1, 2023, thus individuals and organizations need to study this new document, especially the provisions on the rights and responsibilities of Data Subjects, Personal Data Controllers, Personal Data Processors, requirements to protect personal data during personal data processing (section 2, Chapter II), prohibited acts (Article 8) to ensure the maximum interests of individuals and organizations, as well as their responsibilities in the process of using and processing personal data, avoiding administrative sanctions, criminal handling due to violation of regulations on personal data protection.