New Decree on Protection of Personal Data in Vietnam and Comparison with GDPR

Date: 21 April 2024

On 17 April 2023, the Government issued Decree 13 on personal data protection (**Decree 13/2023**). Decree 13/2023 marks a significant milestone as the first comprehensive legal document that governs the protection of personal data in Vietnam. As compared to the draft decree on personal data protection (**Draft Decree**), Decree 13/2023 has been significantly improved to incorporate key aspects necessary to protect personal data to align with the General Data Protection Regulation (**GDPR**). In this post, we will discuss key issues under Decree 13/2023 while comparing it to the Draft Decree and GDPR. This post is written by Trinh Phuong Thao and edited by Nguyen Quang Vu.

1. Things to be done by 1 July 2023

Ideally, before 1 July 2023, both onshore and offshore entities involving in collecting and/or processing personal data of Vietnamese individuals or foreign individual residing Vietnam should do the following:

- having proper consents from the relevant data subject (see 7);
- if it is a data controller, having a contract with the relevant data processor (see 4);
- determining whether it deals with basic personal data or sensitive personal data;
- preparing and submitting an assessment of the impact of personal data processing to the Ministry of Public Security (**MPS**) (see 10);
- preparing and submitting an assessment of the impact of offshore transferring personal data to the MPS (see 11);
- setting up system to protect the safety and confidentiality of the personal data which it collects or processes; and
- setting up a personal data protection department and a data compliance officer if it deals with sensitive personal data.

Decree 13/2023 only exempts small and medium enterprises or start ups from complying with certain requirements until 1 July 2025.

One key missing ingredient though is the potential penalty which may apply in case of non-compliance. Accordingly, currently, Decree 13/2023 has no teeth in enforcing the above requirements. Unlike Decree 13/2023, the GDPR has clear penalties and fines applicable to violations of the GDPR.

2. Scope of application

As compared to the Draft Decree, Article 1.2 of Decree 13/2023 has clarified the entities that must comply with its provisions, including (i) Vietnamese organizations/individuals; (ii) Vietnamese organizations/individuals operating overseas; (iii) Foreign organizations/individuals in Vietnam; (iv) Foreign organizations/individuals directly participating in or related to personal data processing activities in Vietnam. While it is not clear, it appears that Decree 13/2023 will apply to:

- Personal data of Vietnamese individuals residing in Vietnam and residing overseas;
- Personal data of foreign individuals residing in Vietnam; and
- Offshore entities collecting and/or processing personal.

It is not clear if onshore entities collecting and processing personal data of foreign individuals residing outside of Vietnam will be subject to Decree 13/2023.

Unlike Decree 13/2023, the GDPR has a clear sope of application in terms of its material and territorial scope (see Articles 2 and 3 of the GDPR).

3. Definition of "personal data"

Under Article 2.1 of Decree 13/2023, personal data means any information that is expressed in the form of a symbol, text, digit, image, sound, or in similar forms in an electronic environment that is associated with a particular natural person or helps identify a particular natural person. This definition is broad enough to cover any type of personal data, much like the approach taken by the GDPR, which aims to protect a person's data privacy to the fullest extent possible.

Personal data includes basic personal data and sensitive personal data. Notably, information about the blood type of a person is not considered as sensitive personal data (Article 2.4(b) of Decree 13/2023).

4. Parties involved in the processing of data

For the first time, Decree 13/2023 distinguishes the terms "data controller" and "data processor" similar to those provided under the GDPR. Previously, the Draft Decree only uses the term "personal data processor" interchangeably for both the data controller and the data processor (see previous discussions here). This change will likely enhance the transparency of the allocation of rights and obligations among parties involved in the data processing and make Decree 13/2023 more aligned with international best practices, particularly, GDPR.

The table below compares definitions of the main parties involved in the data processing between Decree 13/2023 and GDPR.

	Decree 13/2023	GDPR	Comments
Data controller	The organization/individual who determines the purpose and the means of personal data processing (Article 2.9)	The person who, alone or jointly with others, determines the purpose and means of the processing of personal data (Article 4(7)) Where two or more controllers jointly determine the purpose and mean of processing, they shall be joint controllers (Article 26)	Decree 13/2023 does not clarify whether the data controller could determine the purpose and the means of data processing **alone or jointly with others.** Unlike GDPR, Decree 13/2023 does not have the term "joint controller".
Data processor	The organization/individual who processes the personal data on behalf of the data controller through a contract or agreement with the data controller (Article 2.10)	The person who processes personal data on behalf of the controller (Article 4(8)). Processing by a processor shall be governed by a contract or other legal act under Union or Member State law (Article 28.3)	The definition of "data processor" under Decree 13/2023 aligns with that of GDPR.
Data controlling and processing party (*Bên Kiểm soát và xử lý dữ liệu cá nhân*)	The organization/individual who determines the purpose, the means of data processing and directly processes the personal data (Article 2.11)	Not provided	It is not clear why Decree 13/2023 introduces this new concept in addition to the "data controller". It seems that the draftsman of Decree 13/2023 takes the view that a data controller itself cannot directly process the personal data, hence this concept is added to allow a data controller to process personal data on its own. Previously, the Draft Decree does not govern this concept.

	Decree 13/2023	GDPR	Comments
			This is inconsistent with GDPR, which allows a data controller to directly process personal data.
Third party	The organization/individual who, other than the data subject, data controller, data processor, data controlling and processing party, is allowed to process the personal data (Article 2.12)	The person other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, is authorized to process personal data (Article 4(10))	This concept under Decree 13/2023 aligns with that of GDPR.
Recipient	Not provided	The person to whom the personal data are disclosed, whether a third party or not (Article 4(9)).	Similar to the Draft Decree, Decree 13/2023 also does not provide for this concept like GDPR.

5. Principles of data processing

Article 3 of Decree 13/2023 outlines eight principles, namely: (i) lawfulness; (ii) transparency; (iii) purpose limitation; (iv) data minimization; (v) accuracy; (vi) integrity and confidentiality; (vii) storage limitation; and (viii) accountability. These principles are quite similar to those set out in Article 5 of GDPR for processing personal data. The differences between Decree 13/2023 and GDPR in terms of principles of data processing include:

- Decree 13/2023 does not include the "fairness" principle. Under Article 5.1 of GDPR, personal data will be processed fairly; and
- Regarding the "purpose limitation" principle, Decree 13/2023 explicitly provides that the sale and purchase of personal data are not allowed in any form, except the laws provide otherwise.

6. Rights of the data subject

Article 9 of Decree 13/2023 specifies eleven rights of data subjects including (i) the right to know; (ii) the right to consent; (iii) the right to access; (iv) the right to withdraw consent; (v) the right to delete data; (vi) the right to restrict data

processing; (vii) the right to request the provision of data; (viii) the right to object to data processing; (ix) the right to complain, denounce and initiate lawsuits; (x) the right to claim compensation for damage; and (xi) the right to self-defense. This is similar to GDPR except that:

- GDPR does not provide for the right to self-defense of the data subject; and
- Decree 13/2023 does not regulate the right of "data portability" as provided under the GDPR. The lack of this right may prevent the data subject from transmitting his/her personal data to other controllers.

7. Consent by the data subject

In general, the data subject's consent is a crucial basis for ensuring the legality of the data processing. Under Decree 13/2023, except for certain cases not requiring consent (see 8), consent by the data subject will be applied in all activities of data processing. The consent by a data subject will be valid only when (i) it is freely given, and (ii) the data subject fully knows information about the type of personal data, purpose of data processing, parties processing the data, and the data subject's rights and obligations. In addition, the data subject's consent must:

- be clear, specifically expressed by written instrument, by voice, by ticking the consent box, by text message to consent, by selecting technical settings to consent, or by another action that demonstrates the same. Accordingly, pre-agreed forms set out by the service provider/website owners such as default settings, pre-ticked boxes or general terms and conditions may not be considered as consent by the data subject;
- Be made for a single purpose. In case of multiple purposes, the parties involved in data processing must list out all purposes for the data subject to choose to give consent to one or more of the stated purposes; and
- be expressed in a format that can be printed and/or reproduced in writing, including in electronic or verifiable formats.

Particularly, the data subjects' silence or non-response is not be regarded as their consent. This approach is similar to GDPR where all consents must be opt-in consents (i.e., a positive action or indication) and failure to opt-out is not consent as it does not involve a clear affirmative act.

8. Personal data processing in special cases

Decree 13/2023 specifies several special cases of personal data processing including:

(1) Personal data processing without requiring the consent of the data subject (Article 17). These cases include the followings:

- In emergency cases necessary to protect the life and health of the data subject or others;
- To conduct disclosure of personal data in accordance with the law;
- To serve the processing by a state competent authority in special cases (e.g., emergency on the national defense, national security, major disasters, dangerous epidemic,…);
- To fulfill the contractual obligations of the data subject with relevant entities in accordance with the law (except for the case of marketing and advertisement business – Article 21.1 and 21.2 of Decree 13/2023); and
- To serve the operations of state agencies as prescribed by specialized laws.

These cases are quite similar to those provided under the GDPR, although there is a notable difference. The GDPR includes an additional case, which is favorable to the data controller or third party, where processing is necessary for the legitimate interests pursued by the controller or by a third party (Article 6.1(f))). However, such "legitimate interest" must not be overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data;

(2) Processing of personal data obtained from audio and video recording in public locations for the protection of the national security, social order and safety, and their legitimate rights and interests in accordance with the law (Article 18);

(3) Processing of personal data of persons declared missing or dead. It is noted that processing of personal data in this case requires consent of their family members (e.g., spouse, parents) and if the dead/missing person has no family member, it is considered as no consent is given and therefore, the processing could not be carried out (Article 19). Meanwhile, GDPR does not apply to the data of deceased persons and leave this room for Member State's law (Recital 27); and

(4) Children's personal data processing (Article 20). Except for the cases covered by (1), when the child is 7 years old or older, any parties involved in data processing must obtain the consent of both the child and their parents or guardian.

9. Notification obligation in case of violation of regulations on personal data protection

Under Article 23 of Decree 13/2023, upon detection of a violation of the regulations on personal data protection, the data controller, data controlling and processing party must notify the Ministry of Public Security (**MPS**) (Department of Cybersecurity and Hi-tech Crime Prevention) (**A05**) within 72 hours of the occurrence of the violation in a prescribed form with compulsory contents (e.g. Descriptions the measures put in place to handle and minimize the harm of such violation). In case of notifying after 72 hours, the reason for delay or late notification must be included. This obligation aligns with that provided under Article 33.1 of GDPR.

10. Assessment of the impact of personal data processing

Under Article 24 of Decree 13/2023, in all cases, from the commencement of personal data processing, the data controller, the data controlling and processing party must prepare and maintain a dossier for assessment of the impact of personal data processing. In particular,

- The dossier made by data controller, the data controlling and processing party must include several contents, *among others*, cases of cross-border transfer of personal data; assessment of the impact of personal data processing; potential and unwanted consequences and/or damage, and measures for minimization or elimination thereof;

- In case there is a data processor acting on behalf of a data controller, such data processor must also formulate a separate dossier for assessment of the impact of personal data processing with required contents; and

- The dossier must be made available at all times for the inspection and evaluation by the MPS and 01 original copy shall be submitted to A05 within 60 days from the date of processing of personal data.

Previously, the Draft Decree only requires an impact assessment report in case of sensitive personal data and cross-border transfer of personal data. This new obligation under Decree 13/2023 will place a significant burden for <u>all</u> data controllers and data processors, such as service providers while processing data during the performance of contract. Under Article 35.1 of the GDPR, a data protection impact assessment is only required in case the processing uses new technologies and is likely to result in a high risk to the rights and freedoms of natural persons.

11. Cross-border transfer of personal data

Article 25 of Decree 13/2023 specifies procedures that a data transferor must comply with for the cross-border transfer of personal data as follows:

- The transferor must prepare a dossier for assessment of the impact of cross-border transfer of personal data with required contents including, *among others*, descriptions and explanations of the objectives of the personal data processing of Vietnamese citizens after being transferred;
- The transferor must keep the dossier available at all times for the inspection and evaluation by the MPS and send 01 original copy to A05 within 60 days from the date of processing of personal data; and
- The transferor notifies and submits A05 the information on the data transfer and the contact details of the responsible organization and/or individual in writing upon the successful completion of the data transfer.

Except for cases requiring the transferor to cease the cross-border transfer of personal data (Article 25.8 of Decree 13/2023), Decree 13/2023 does not impose restrictions on the transferring of personal data to third countries like the GDPR. Under the GDPR, transferring of personal data to a third country is restricted unless (i) the European Commission decided that such third country ensures an adequate level of data protection; or (ii) the controller/processor has implemented appropriate safeguards; or (iii) an exemption or derogation applies (Article 45, 46, 48 and 49 of GDPR).

12. Measures for ensuring the personal data protection

Under Article 26 of Decree 13/2023, measures for ensuring personal data protection must be applied from the commencement of and throughout personal data processing. These measures include (i) management and technical measures implemented by entities related to personal data processing; (ii) measures implemented by competent authority; (iii) investigation and procedural measures taken by competent authority; and (iv) other measures in accordance with the laws. Such measures are quite general and therefore, it could be interpreted that the involved parties processing the personal data could determine appropriate measures at their discretion on a case-by-case basis.

With respect to each type of personal data, Decree 13/2023 will require specific measures in addition to those set forth in Article 26 (e.g., To designate a department functioned with personal data protection or appoint personnel in charge of personal data protection in case of processing sensitive personal data).

13. Specialized agency for the personal data protection

As compared to the Draft Decree, Decree 13/2023 has removed the concept

Personal Data Protection Committee (*Ủy Ban Bảo Vệ Dữ Liệu Cá Nhân*) and all related provisions. Under Article 29 of Decree 13/2023, the Department of Cybersecurity and Hi-tech Crime Prevention under the MPS (A05) will act as the specialized agency on the protection of personal data. The choice of the MPS as the authority in charge of personal data protection seems to suggest that Vietnam considers protection of personal data as a security issue as opposed to a civil right issue.

This is different from Article 51 of GDPR, which requires each Member State to establish one or more independent public authorities to be responsible for monitoring the application of the GDPR in relation to the processing of personal data within the Union.