FRASERS
LAW COMPANY

EU'S GENERAL DATA PROTECTION REGULATION AND VIETNAM'S DRAFT DECREE ON PERSONAL DATA PROTECTION: AT INTERPLAY OR AT CROSS-CURRENTS?

MARCH 2022

INTRODUCTION

On 25 May 2018, the European Union's (***EU***) General Data Protection Regulation (***GDPR***) became enforceable, which was touted to be the "*toughest privacy and security law in the world*"[1] and is considered as the benchmark for personal data protection regulation all over the world imposing data protection obligations on organisations (regardless of location, whether in the EU or outside the EU), so long as they collect data or target data relating to data subjects in the EU (regardless of citizenship).

The GDPR arguably led the transition for more jurisdictions to take a more robust approach on data protection. Vietnam is one such jurisdiction. With Vietnam's increasingly developing infrastructure and legal framework for technological advancements in various aspects of daily life – e.g. online banking, fin tech-led processing of online payments, tele-medicine and virtual working – there is the concomitant necessary regulation for the right to personal data protection for individuals as well. The Vietnamese Government has issued the second version of the draft decree on data personal protection (***Draft Decree***) and, with amendments or feedback from the relevant State agencies, is expected to take effect soon.

The GDPR's extraterritorial scope could mean it could be applicable toward organisations located in Vietnam. If an organisation in Vietnam collects data of data subjects in the EU, whether in its capacity as data processor or data controller, the GDPR provisions could be engaged and made applicable on that organisation. The Draft Decree, on the other hand, is to be made applicable to personal data of individuals in Vietnam, without specification of citizenship requirements, save for the cross-border transfer of data. There is thus a possibility by which both the GDPR and the Draft Decree could be triggered in the processing of data with a Vietnam component. In this article, we highlight the major differences between the GDPR and the Draft Decree that could potentially have an impact on organisations processing data with a Vietnam component. It is not clear yet at this stage which provisions would prevail in the event of conflicting provisions or how the conflicting provisions could be reconciled.

[1] See "*What is GDPR, the EU's new data protection law?*" at https://gdpr.eu/what-is-gdpr/.

I. Sensitive Personal Data

Although Article 4.1 of the GDPR and Article 2.1 of the Draft Decree provide similar definitions in relation to "personal information", the Draft Decree provides a distinct definition of "sensitive personal data" (***Sensitive Personal Data***), which is subject to restrictions under the Draft Decree. A majority of items considered as Sensitive Personal Data under the Draft Decree are listed in Articles 9 and 10 of the GDPR as special categories of personal data or personal data relating to criminal convictions and offences.

There are narrower restrictions relating to Sensitive Personal Data resulting to higher threshold of protection over this discrete category of personal data:

(a) Data processors are not allowed to disclose Sensitive Personal Data;[2]

(b) The data subjects must be informed that the data to be processed is considered Sensitive Personal Data and their consent must be obtained in a format that can be printed or copied in writing.[3] As data processors are not allowed to disclose Sensitive Personal Data, it could be argued that the act of processing requiring consent is restricted to data processors' 'collection, recording, analysis, storage, alteration, retrieval recovery, encryption, decryption, copy, deletion, or destruction of personal data' within the relevant data processor's organisation. It could be argued that processing of Sensitive Personal Data does not include the processing activities of 'disclosure, granting of access to personal data, copy or transfer' to third parties. This requirement is also aligned with the principle under the Civil Code 2015 of Vietnam, whereby the collection, storage, use, and publication of information related to the private life or personal privacy of an individual must have the consent of that person, and the collection, storage, use, and publication of information related to family privacy must have the consent of the family members, except where otherwise prescribed by law;[4]

(c) The processing of Sensitive Personal Data must be registered with the Personal Data Protection Commission (***PDPC***) – which is yet to be established - prior to undertaking any processing activity.[5]

II. Conditions for Consent to Processing Personal Data

Under the GDPR, data processing could be based on consent of the data subject, with the onus on the data controller to be able to demonstrate that the data subject has consented to the processing of his or her personal data. There is a clear delineation of rights and obligations between data controllers and data processors in the GDPR; none of such categorisation appears in the Draft Decree.

Article 8.1 of the Draft Decree provides that the data subjects' full consent to the processing of their personal data shall only be valid if it is based on their *informed discretion* with regard to the

[2] Article 6.3 of the Draft Decree.
[3] Article 8.5 of the Draft Decree.
[4] Article 38 of the Civil Code 2015.
[5] Article 20 of the Draft Decree.

following:

(a) Types of personal data to be processed;

(b) Purpose of personal data processing;

(c) Relevant subjects with whom personal data is processed and shared;

(d) Conditions for transferring or sharing personal data to a third party;

(e) Data subjects' legitimate rights related to the processing of their personal data.

Under the Draft Decree, processing of personal data means any action(s) to do with personal data, including collection, recording, analysis, storage, alteration, disclosure, granting of access to personal data, retrieval, recovery, encryption, decryption, copy, transfer, deletion, or destruction of personal data or other relevant actions.

In addition, according to the Draft Decree, the data subjects may provide partial or conditional consent and it is up to the data subject to set out conditions or restrictions.

On 7 March 2022, the government of Vietnam issued Resolution No. 27/NQ-CP (***Resolution 27***) which sets out circumstances where processing of personal data could be had without the requirement of consent, *viz*:

(a) If the processing is necessary in response to an emergency situation that threatens the life, health, or safety of the data subject or other individual. The data processor is responsible for proving that the situation is an emergency. This exception is found in the Draft Decree but without the requirement for proof;

(b) If the processing is necessary because of national defence and security requirements, and the processing must be carried by competent authorities in accordance with other laws;

(c) If the disclosure of personal data is in accordance with the law;

(d) If competent state agencies investigate and handle law violations according to the provisions of the law;

(e) If the processing by a competent state agency is made to serve the operation of the state agency in accordance with the law.

The exceptions set out above, as opposed to the exceptions in the Draft Decree, mainly provide for data processing by State agencies for the purpose of maintaining their operations, but they do not appear to address legitimate use of personal data by the private sector.

III. Processing of Personal Data

Under the GDPR, the concepts and obligations between a "data controller" and a "data processor" are clearly delineated. There is no such separation of concepts in the Draft Decree where only the term 'processor' is used.

Under the GDPR, a data controller is required to notify the data subject (with information required for such notification that ensures fair and transparent processing) at the time when personal data is obtained, and when the data controller intends to further process the personal data for a purpose other than that for which the personal data was collected. There is thus no continuing requirement of notification of *all* activities falling under the rubric of processing.

Meanwhile, under Article 11 of the Draft Decree, data subjects must be informed of *all* activities related to the processing of personal data, except in the following instances:

(a) If the data subjects have provided full consent as to the content and activities related to processing of personal data;

(b) If the processing of personal data is regulated by laws, international agreements and treaties; and

(c) Such processing shall not affect the rights and interests of the data subjects and it is impossible to notify the data subjects of *all* such processing activities.

The manner by which notification is effected is unclear under the Draft Decree. In the event of partial or conditional consent, the notice requirement may prove to be troublesome and may overburden the processor with more costs to be incurred in order to comply with the notification requirement for each consented processing activity.

IV. Processing of Personal Data of a Deceased Data Subject

Under the GDPR, consent given prior to the death of a data subject is believed to extend beyond death, and any identifiable data that relate to a person who has died will be subject to any duty of confidence established prior to death. The duty of confidence extends beyond death for certain personal data such as hospital records of the deceased etc., communications falling under litigation or legal advice privilege.

Meanwhile, Article 9.1 of the Draft Decree requires a data processor to process personal data of a deceased data subject in accordance with the will of the deceased data subject or written consent of his or her legitimate heirs, if the latter's agreement or disagreement is different from the agreement consented to by the data subject. This appears to create additional (if not impossible) obligations for data processors upon the death of a data subject to keep track of every data subject's (or his or her heirs written consent) will or consent prior to or upon death.

V. Conditions Applicable to a Child's Consent

Unlike the GDPR, the Draft Decree is silent on the age of a child whose parent/guardian's consent must be required prior to processing personal data of a child.

In addition, Article 14.4 of the Draft Decree provides that the processing of children's personal data must be terminated in the following cases:

(a) The collection has been completed or is no longer necessary and whenever required by the data subject and guardian in accordance with the law;

(b) Parents or guardians withdraw their consent for the processing of the child's personal data;

(c) At the request of a relevant authority when there are sufficient grounds to prove that the processing of personal data affects children's legitimate rights and interests.

VI. Cross-border Data Transfer

The GDPR provides that transfers of personal data to any country outside the European Economic Area (***EEA***) may only take place subject to the following conditions:

(a) The third country ensures an adequate level of protection for the personal data as determined by the European Commission;

(b) In the absence of an adequate level of protection, the controller or processor wishing to transfer the data provides for adequate safeguards (on the condition that enforceable data subject rights and effective legal remedies for data subjects are available);

(c) In the absence of an adequate level of protection, or of appropriate safeguards, a transfer or a set of transfers of personal data fits within one of the derogations covered under the GDPR.

The above conditions could be applicable in Vietnam if data processing of EU citizens is undertaken in Vietnam, a third country outside the EEA.

Under the GDPR, there is no requirement to register and obtain approval from a data protection authority for cross-border transfer of personal data so long as the above conditions are met.

Article 21 of the Draft Decree appears to impose stricter requirements on cross-border transfer of personal data of Vietnamese citizens outside of the border and territory of Vietnam. The cross-border transfer of personal data will only be allowed subject to the satisfaction of the following 4 conditions:

(a) Data subject's consent is granted for the transfer;

(b) Original data is stored in Vietnam;

(c) A document is granted proving that the recipient country, territory or a specific area within the recipient country or territory has issued regulations on personal data protection at a level equal to or higher than that specified in the Draft Decree;

(d) A written approval is obtained from the PDPC of Vietnam.

This provision on cross-border data transfer in the Draft Decree specifies applicability to personal data of Vietnamese citizens. It is not clear if it’s an exclusion for cross-border transfer of personal data of non-citizen residents in Vietnam.

In order to obtain the approval from the PDPC, the application dossiers shall comprise the following:

(a) An application form;

(b) An impact assessment report for cross-border transfer of personal data, which consists of: a detailed description of the cross-border transfer of personal data, purpose of transferring personal data abroad; assessment of potential harm; measures to manage, minimise or eliminate such harm;

(c) Documents related to the contents mentioned in the application for processing sensitive personal data and the impact assessment report for processing sensitive personal data.

The PDPC shall examine the application dossier within 20 working days from the date of receipt of the application. Crucially, the PDPC has the right to **physically** inspect the contents of the information stated in the application for cross-border transfer of personal data.

In addition, according to Article 26.3 of the Law on Cybersecurity of Vietnam (***Law on Cybersecurity***), domestic and foreign service providers who provide their services on telecom networks, the internet and other value added services in cyberspace in Vietnam and carry out activities of collecting, exploiting, using, analysing and processing personal data, data about service users' relationships and data generated by service users in Vietnam (collectively, the ***Users' Data***) must store the Users' Data **in Vietnam** for a specified period to be stipulated by the Government. Also, overseas-domiciled enterprises will need to open subsidiaries, branches or representative offices in Vietnam.

The Draft Decree and the Law on Cybersecurity are silent on the manner of storing data that could be deemed as being "stored in Vietnam" (being the "data localisation" requirement under the Draft Decree and the Law on Cybersecurity). They are also unclear on whether or not the storage of data in a cloud infrastructure could be deemed to satisfy the condition of storing data in Vietnam. Notwithstanding, as the PDPC has the right to **physically** inspect the contents of the information stated in the application for the cross-border transfer of personal data, it could be interpreted that if the data processor uses cloud infrastructure to store personal data collected, the server for such cloud infrastructure must be located in Vietnam, so that the PDPC can easily go to a physical location to inspect, to the extent the PDPC may deem necessary.

In addition, the personal data processor that transfers data abroad must build a system to store data transfer history for 3 years, and should comprise the following (Article 21.4 of the Draft Decree):

(a) Time of transferring personal data abroad;

(b) Receiver's identity, including name, address and contact form;

(c) Type, quantity and sensitivity of the personal data transferred abroad;

(d) Other contents as prescribed by the PDPC.

In our view, the above requirements are impractical and could be perceived as unduly burdensome on data processors in Vietnam and will potentially restrict data transfers that will impact urgent scenarios such as fraud detection on financial and payment transactions.

On 10 February 2022, the Ministry of Public Security (***MPS***) issued its response to Official Letter No. 470/BCA/ANKT from the Ministry of Planning and Investment in relation to comments on the recommendations of the business community at the annual Vietnam Business Forum 2021. According to the MPS' response, it is suggested that enterprises can freely transfer user data so long as the transfer is made with data security measures that meet international standards and comply with Vietnam regulations. If enterprises fully comply with MPS' requests regarding coordinating and providing information serving the investigation and handling of criminal activities, they are not required to store data and set up a representative office or branch in Vietnam. The Ministry of Information and Communication (***MIC***) also issued a response, Official Letter No. 527/BTTTT/CNTT, that while recognizing the importance of data and cross-border data flow in the digital transformation of many countries, and MIC maintains that a data localisation policy is a mechanism to ensure national politics and security, to secure information

in cyberspace, protect people's privacy thereby providing businesses and individuals a safe and reliable cyberspace for operations and businesses. The opinion of the MPS and MIC would most likely have certain effects to the Draft Decree, which is still under the process of finalisation prior to issuance.

VII. Conclusion

There are many more differences between the GDPR and the Draft Decree and this article aims to discuss the major differences only.

In our view, the above differences indicate that the GDPR and the Draft Decree could be more at cross-currents and it will be difficult to reconcile their conflicting provisions in scenarios where both the GDPR and the Draft Decree could be applicable.

We note the more restrictive provisions of the Draft Decree, compliance of which could cost more for organisations undertaking data processing in Vietnam. The requirement for a more conservative, bureaucratic approach toward personal data protection and upholding an individual's right to privacy is arguably a common stance for developing economies. In our view, whilst this stance is understandable, it should also not unduly burden business organisations engaged in data processing with higher costs for compliance than that required in other jurisdictions.

Key Contact

Please contact us if you have any questions relating to this Legal Update.

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