Update on Vietnam's Draft Decree on Personal Data Protection

By Giang Thi Huong Tran and Waewpen Piemwichai

On February 9, 2021, Vietnam's Ministry of Public Security (MPS) released the full text of the Draft Decree on Personal Data Protection ("Draft PDPD") for public consultation, after having released an outline in December 2019, with an ambitious goal for the Draft PDPD to be promulgated and take effect on December 1, 2021. This date has now passed and the Draft PDPD remains unissued, with no concrete details on when the situation will change.

Because this is a proposed decree not directly subordinate to any existing law, designed to be quickly issued to tackle the current situation in personal data protection, the Draft PDPD, after being approved by the government, would be subject to additional approval by the Standing Committee of the National Assembly before it could be promulgated and take effect.

Although there are many new contents introduced in the Draft PDPD (please see our previous articles here and here), the following issues are of the highest concern and have attracted the most attention from businesses in various industries and relevant national and international stakeholders:

1. How are data localization requirements being enforced now in Vietnam when the Draft PDPD and the draft Decree on Cybersecurity have not yet been promulgated and are not in effect?

The data localization requirement is one of the biggest concerns for businesses because it potentially creates a barrier to trade and the flow of data; an increase in cost, time, and human resources requirements; and additional burdens for businesses and industries.

The Draft PDPD regulates that Vietnamese citizens' personal data can only be transferred out of Vietnam **when four stipulated conditions are fulfilled**. These four conditions are:

(i) Consent must be obtained from the data subjects;

(ii) The original data must be stored in Vietnam;

(iii) The data transferor must have proof that the recipient country has personal data protection at a level equal to or higher than the level specified in the Draft PDPD; and

(iv) A written approval for transfer must be obtained from the Personal Data Protection Commission (PDPC).

One exemption is that if conditions (ii) and (iii) above cannot be fulfilled, these two conditions could be replaced by two other conditions, namely: (ii)': there is a commitment from the data processor to protect the data, and (iii)': there is a commitment from the data processor to apply measures to protect the data.

If a single condition is not met, for example, if there is no approval from the PDPC, then Vietnamese citizens' personal data could not be transferred out of Vietnam.

Because the Draft PDPD has not yet been promulgated and thus has not taken effect, the data localization requirement is not yet enforced in Vietnam, but businesses should be alert and prepare in advance as much as possible. Please also see the discussion in section 2 below.

Please note that another set of data localization requirements is also regulated in the Cybersecurity Law and the Draft Decree on Cybersecurity. Article 26.3 of the Cybersecurity Law regulates that: "Domestic and foreign enterprises providing services on telecommunication networks or the internet or value-added services in cyberspace in Vietnam with activities of collecting, exploiting, analyzing, and processing personal information data, data on the relationships of service users, or data generated by service users in Vietnam ***must store such data in Vietnam for the period prescribed by the government***. ***Foreign enterprises mentioned in this clause must open branches or representative offices in Vietnam***."

The Draft Decree on Cybersecurity (which has been available for public consultation) has narrowed down this broad language. Based on the draft decree, storing data and/or having branches or representative offices in Vietnam is only required when all three following conditions are met:

(i) Such enterprise provides telecom and/or online services under the list provided under the Draft Decree on Cybersecurity;

(ii) Such enterprise carries out activities of collecting, exploiting [using], analyzing and processing the regulated types of data; and

(iii) Such enterprise has been warned that the services it provides are used to commit a breach of the laws of Vietnam and it does not take any measures for remedying such breach, or it resisted, obstructed, or ignored requests from the relevant authorities.

The regulated services include 10 types of services, including telecom services; services of data storage and sharing in cyberspace; e-commerce; online payment; intermediary payment; service of transport connection via cyberspace; social networking and social media; and online electronic games. The regulated data include personal data, data on the relationships of service users, and data generated by service users in Vietnam.

However, thus far, the requirement specified in Article 26.3 of the Cybersecurity Law has not yet been enforced by the government although the law has been in force since January 1, 2019, because the government is still waiting for the Draft Decree on Cybersecurity to be finalized and issued.

2. How should companies prepare themselves for compliance with personal data protection requirements while the status of the Draft PDPD is uncertain?

If the Draft PDPD is approved as it is, there would be big changes which mostly affect enterprises processing personal data.

First of all, enterprises would need to reassess how they collect, process, disclose, store, transfer and/or share personal data of relevant parties (e.g., customers, partners and employees). For instance, once the Draft PDPD takes force, affirmative express opt-in consent must be in place. Unlike in current existing personal data protection legislation, the consent requirement stipulated in the Draft PDPD is clearly express consent which excludes implied consent (i.e., the silence or non-response of data subjects). Moreover, data subjects' consent must be in a format that can be printed or copied in writing. This clarification would require enterprises to start developing mechanisms for their users/customers to express their clear, affirmative opt-in consent (such as a click-to-accept mechanism or a tick box on online platforms). For those enterprises who need to share data with their affiliated companies or other third parties outside of Vietnam, they need to ensure that the transferees of such data are in jurisdictions

with adequate levels of data protection and are prepared to obtain prior approval from the PDPC. For those enterprises that need to share sensitive data, prior approval from the PDPC is also required.

For the field of labor and human resources, enterprises will need to review and audit their internal systems of employment agreements, internal labor rules, internal policies (e.g., internal privacy policy rules) and collective labor agreements to ensure that relevant provisions therein relating to the processing of their employees' personal data are consistent with the Draft PDPD. If there are any inconsistencies or the company documents have not adequately addressed personal data protection requirements specified in the Draft PDPD, the enterprises would need to arrange for all relevant employees to sign new addendums to the employment agreements, or to agree with amended internal privacy policy rules which incorporate necessary changes to be in line with the Draft PDPD, or to report new changes to the internal labor rules to the labor authorities.

Additionally, enterprises would need to update current and future agreements with their users/customers, business partners and third-party vendors (including the relevant terms of use and privacy policies) to eliminate any provisions which are inconsistent with the Draft PDPD. Enterprises also would need to ensure they have obtained relevant parties' consent for such amendments and updates.

With regard to the PDPC's approval, although the Draft PDPD does not clarify how the approval would be carried out, whether it is one-time approval or required every time enterprises process sensitive personal data, we lean on the possibility that it would be more likely to be one-time approval, taking into account the limited resources of the PDPC, the frequency and instantaneous nature of data processing (especially in the case of location data and biometric data, which is classified as sensitive), and the aim of business facilitation. So, it would be a more pragmatic and feasible solution if enterprises only have to apply for one-time regulatory approval.

Although there is uncertainty as to whether and when the Draft PDPD will be promulgated and take effect, a number of large domestic and multinational corporations, due to their constant transactions with business partners/counterparts in countries which require a high standard of personal data protection such as the EU, the U.S., Japan, Singapore, etc., have good systems and infrastructures in place which can be upgraded to be in compliance with the proposed regulations. Therefore, those companies appear to be proactively preparing themselves to be compliant, and are capable of fulfilling the data localization requirements.

However, with regard to SMEs, they may find it more difficult and burdensome, and may need much more effort in terms of time, finance, and human resources to upgrade their operation systems in order to comply. However, looking at the positives, if the SMEs have good systems in place for better personal data protection, it will facilitate business operations in the long run, especially when they later on could expand their businesses to transact more with international partners in countries which have high standards for personal data protection. At the same time, they could build up more trust from customers when they transact with the SMEs.

It has been strongly recommended that the Draft PDPD should facilitate the operations of SMEs, not create burdens and deter their development. Vietnamese enterprises, especially SMEs, would benefit most from a policy which facilitates the cross-border flow of data. This is especially true in Covid-19 times, when online activities play a vital role in provision of essential services such as health care and education and when people mostly work from home.

Businesses and industries should closely monitor the development status of the Draft PDPD and Draft Decree on Cybersecurity in order to have time to prepare for compliance, avoiding the situation of being surprised and not having enough time to adjust their systems or plans accordingly.

3. What is the relationship between the Draft PDPD once issued with the existing regulations on personal data protection?

One of the big questions is what will be the relationship of the PDPD, once promulgated, with existing personal data protection legislation in Vietnam? Although the MPS aims for the PDPD to be a comprehensive, uniform law/regulation on personal data protection in Vietnam, according to the MPS, this Draft PDPD, once issued, will co-exist and be co-effective with current scattered data privacy laws, instead of replacing the existing legislation. In the event that there is any conflict between the existing legislation and the Draft PDPD, in our opinion, the relevant parties will need to comply with the one with the more stringent requirement (in most if not all cases, this is the Draft PDPD). Failure to do so could potentially lead to administrative sanctions.

4. Harmonization of the Draft PDPD with Vietnam's international commitments, international laws and other domestic regulations (especially the Draft Decree on Cybersecurity)

Another big concern is that the Draft PDPD needs to be in line with Vietnam's international commitments in international agreements such as the WTO, CPTPP, and RCEP which facilitate the flow of data. However, these international agreements have a legal justification ground of "legitimate public policy objective" which allows member states to adopt or maintain measures inconsistent with the cross-border transfer of information rule, as long as the measures would not constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and would not impose restrictions on transfer of information greater than required to achieve the objective.

Despite this justification ground, the need for data flow is inevitable in the digital economy and digital society toward which Vietnam has directed its development; thus, the approval or registration process could still be arguably considered as imposing restrictions greater than required to achieve the objective because it imposes much greater cost, time, and human resources requirements for industries and authorities, and delays transactions and business operations and the flow of data. Instead, the government could use its manpower in a more efficient way such as enforcement of the law, building capacity for enterprises, etc. It is recommended that the post-check mechanism should be used instead of pre-check of registration/approval.

The Draft PDPD should also be harmonized with other international laws, for example, the EU's GDPR, as much as possible in order to facilitate businesses' cross-border transactions. One example for consideration is the need to differentiate between data controller and data processor to regulate their respective obligations and responsibilities to personal data owners, which is not addressed in the Draft PDPD. According to GDPR, the data controller determines the purposes for which and the means by which personal data is processed, thus, the data controller is the main party responsible for data breaches and to consumers, while the data processor processes personal data only on behalf of the data controller. The data processor is usually a third party external to the company. The duties of the data processor toward the data controller must be specified in a contract or another legal act.

One further concern is the harmonization between the Draft PDPD and the Draft Decree on Cybersecurity with regard to data localization requirements. Under the Draft PDPD, personal data must be retained and stored in Vietnam, and is only allowed to be transferred abroad if four stipulated conditions are met, while under the Draft Decree on Cybersecurity, there is no mandatory requirement of storing personal data in Vietnam unless all three conditions which trigger this mandate are fulfilled. Therefore, the policy rationales of these two decrees appear to be contradictory and need to be carefully considered so that once issued, they will not negate each other.

5. What is the current status of the Draft PDPD and Draft Decree on Cybersecurity and what is the best way to move forward?

Regarding the Draft PDPD: Although there is no official news regarding the status of the Draft PDPD and there is no official latest version available for public access, to our best knowledge, the MPS has finalized the Draft PDPD after hearing comments from the public and relevant stakeholders and submitted it to the Ministry of Justice (MOJ) for review and appraisal. Once the MOJ finishes its review, the draft will be submitted to the government for review and approval before the government submits it to the Standing Committee of the National Assembly for review and approval. There is no program in 2021 for the Standing Committee to work on this Draft PDPD. Therefore, it is very likely that the Draft PDPD will not be promulgated and take effect during this year of 2021 as planned. To date, it is difficult to assess the likelihood of when the Draft PDPD will be issued and take effect.

Regarding the Draft Decree on Cybersecurity, to the best of our knowledge, it has been submitted back and forth to the government for review and approval but there is no official news or certainty as to whether and when the government would issue this decree.

It is strongly recommended that companies should closely watch the status of these two draft decrees in the year 2022 in order to prepare themselves if the decrees are likely to be promulgated.