RUSSIN & VECCHI

Coming Changes to Vietnam's Personal Data Protection Law

By Philip Ziter
Senior Associate in Russin & Vecchi's HCMC Office

In Vietnam, there are many regulations that govern the collection, receipt, transmission, and use of data. The government has drafted a new decree on the protection of personal data. It is expected to come into effect at the end of 2021. This article outlines, highlights coming changes, and provides guidance on how to be prepared.

Existing Laws that impact the collection, transfer, and storage of data:

- **Law on Cyberinformation Security** No. 86/2015/QH13 (November 19, 2015) ("**CISL**") establishes requirements for all entities involved in the collection, receipt, transmission, and use of data over any network. General rules on protection of personal data can be found in the CISL.
- **Law on Cybersecurity** No. 24/2018/QH14 (June 12, 2018) ("**Cybersecurity Law**") regulates cyber activities that impact national security and social order and safety. Article 26 of the Cybersecurity Law requires establishment of a physical presence in Vietnam and the storage of certain data in Vietnam. However, these requirements are yet to be enforced as guidance is missing.
- **Law on Medical Examination and Treatment** No. 40/2009/QH12 (November 23, 2009) includes rules and regulations on protection of Hospital, Patient and Health related Data.
- **Decree 52 on E-Commerce** No. 52/2013/ND-CP, and its draft decree amending it ("**Decree 52**") (May 16, 2013)
- **Decree 72 on Internet Services and Online Information** No. 72/2013/ND-CP ("**Decree 72**") (July 15, 2013)

DRAFT DECREE ON PERSONAL DATA PROTECTION

On February 9, 2021, Vietnam's Ministry of Public Security ("**MPS**") released the full text of the Draft Decree on Personal Data Protection ("**Draft Decree**") for public comment. It reflects public comments based on an earlier version. The Draft Decree is expected to take effect on

December 1, 2021. It has six chapters and 30 articles which regulate the cross-border transfer of data,

processing of sensitive personal data, and the rights of data subjects. Based on the existing draft, the free flow of data will be adversely affected.

Scope and definition:

The Draft Decree applies to every agency, organization and individual involved in the *processing* of *personal data* which originates in Vietnam ("**Processor**") It applies to both local and foreign processors, whether the processor is based in Vietnam or abroad.

What is "Personal Data"?

As defined, "personal data" concerns an individual or relates to the identification or possible identification of a particular individual. Personal data is subdivided into two categories:

- **Basic personal data** which includes name, date of birth, blood type, marriage status, data that reflects activity or history of an individual's activity on the internet; and
- **Sensitive personal data** which includes political opinion, financial data, religious views, physical and mental health data collected and identified during registration for or provision of medical services, plus social relationships, biometrics, one's actual location, crime records, etc.

Financial data and health-related data was previously considered to be a State Secret and it enjoyed additional protection. In late 2020, however, the Prime Minister revised what are considered to be State Secrets and such data is no longer considered to be a state secret. This seems to be paving the way for the implementation of the Draft Decree in 2021. Under the existing regime, such data does not receive special protection. The Draft decree considers this data to be "sensitive personal data", and is afforded additional protections.

What is *processing* of personal data?

Personal data processing is broadly defined as any action having to do with personal data, including its *collection, recording, analysis, storage, alteration, disclosure, the grant of access to personal data, retrieval, recovery, encryption, decryption, copying, transfer, deletion, or destruction*.

Who is a data processor?

- **Personal data processors** are domestic and foreign agencies, organizations and individuals engaged in processing personal data which originates in Vietnam.
- **Third-parties** are domestic and foreign agencies, organizations and individuals allowed to receive personal data and which are engaged in some processing activities and are other than personal data processors or data subjects.

These definitions are similar and can lead to confusion. The terms "data controller" and "data processor" have been suggested instead. Moreover, there are issues of enforcement as foreign agencies and the like may not be subject to Vietnamese law.

Rights of data subjects under Article 5 of the Draft Decree

- Discretion to allow or not to allow personal data processors or third-parties to process their personal data.
- Receive notices from personal data processors at the time of processing or as soon as possible.
- Request personal data processors to view, correct and provide a copy of their personal data.
- Request personal data processors to terminate the processing of personal data, restrict the right to access personal data, terminate the disclosure or access to personal data, delete or close collected personal data, unless otherwise specified by law.
- File complaints in accordance with the law, or submit complaints to the Personal Data Protection Commission in the following cases:

  a) Their personal data has been compromised.

b) Their personal data has been processed for the wrong purposes, and not in accordance with the agreement or the law (ie, not for the purposes for which the data subject has given consent).

c) Right of access to their personal data has been breached or has not been exercised properly.

- Claim compensation when there are grounds to believe that their personal data has been breached.

The Consent Principle:

The collection, storage, use, processing, publication, disclosure, and transfer of information and materials related to the private life or personal information of an individual must be consented to by that person, unless consent is exempted by law, and the use of such personal information must be consistent with the scope of the consent. Children (*below full 15 years old*) lack the legal capacity to give consent. Consent must be obtained from the child's parent or legal guardian.

For the most part, existing data protection laws do not expressly state whether the data subject's consent must be affirmative or may be implied. The Draft makes it clear that consent:

- Must be voluntary;
- Must be based on full information; and that
- Failure of a data subject to respond does not constitute consent.

This means that consent must be explicit and affirmative.

Furthermore, under the Draft Decree, consent can be partial or conditional, and it can be withdrawn at any time. Consent, under the Draft Decree, must be capable of being printed or copied in writing, and is valid throughout the life of the data subject and for 20 years after the data subject's death ("*for the authorized activities of state agencies*") unless the data subject

decides otherwise. In the case of a dispute, the burden of proving consent rests with the data processor.

Personal data may be disclosed to third parties without consent in certain cases, such as to protect the life, health, or freedom of the data subject, or where disclosure causes no harm to the legitimate rights and interests of a data subject and where obtaining consent would be impossible. This exception is not fully explained.

Consent and exceptions

The Draft Decree requires that a data subject give consent before her data is disclosed or processed, but it provides some exceptions:

- As provided by law;
- For matters of national security, social order and safety;
- In case of an emergency, a threat to life or when there is a serious risk to the health of the data owner (or to public health) as provided by law;
- When permitted under the Law on Press, if there is no material damage to the data owner's honor, or damage in an economic or spiritual sense;
- Investigating an act in violation of law;
- As permitted by regulations in international agreements or treaties of which Vietnam is a member; or
- Scientific research or statistics in encrypted form that is to be de-identified and replaced with a code.

Establishment of a Committee on Personal Data Protection

A Personal Data Protection Committee ("**PDPC**") will be set up by the MPS, which can appoint up to six members. The PDPC will be empowered to inspect for compliance with personal data protection regulations up to twice a year.

Permit required to process sensitive personal data

Under the current version of the Draft Decree, "sensitive personal data" must be registered with the PDPC prior to processing. Processors must submit an application which meets specific requirements to the PDPC for registration. The PDPC will process the application within 20 working days from the date of receipt of a valid application. This requirement would obviously be extremely burdensome for most companies which process financial or healthcare data.

Data localization - Permit required to make a cross-border transfer of personal data

Personal data of Vietnamese citizens can be transferred out of the territory of Vietnam when the following four conditions have been satisfied:

a) Data subject consents to the transfer;

b) Original data is stored in Vietnam (ie, *data localization*);

c) Data Processor must prove that the recipient country, territory has regulations on personal data protection at a level equal to or higher than those specified in the Draft Decree; and

d) Written approval of the transfer is obtained from the PDPC.

These new regulations on cross-border data transfer would create enormous barriers to trade and would unreasonably restrict the flow of data. This would result in increased costs for existing businesses, would certainly deter new business, and would negatively impact development of the digital economy.

The Draft Decree is a step beyond data localization requirements which have already been enacted. Requirements regarding cross-border transfers of data were highly criticized when the *Cybersecurity Law* was issued in 2018. A draft decree guiding implementation of the Cybersecurity Law has somewhat narrowed the broad language. If the draft decree guiding implementation of the Cybersecurity Law and the Draft Decree are both promulgated, it's unclear how the data localization requirement will be implemented and enforced.

Administrative fines under the Draft Decree

- Up to VND 100 million (approx. US$ 4,300) for violations of:
    - Rules on registration for processing of sensitive personal data; or
    - Rules on cross-border transfer of personal data.
- Up to 5% of the violator's annual revenue in Vietnam could be imposed for repeat violations.
- Suspension of personal data processing for a duration of up to 3 months.
- Suspension of *the right to obtain approval* of the PDPC to process sensitive personal data or to transfer data cross-border.
- Payment of a fine equivalent to the amounts gained by the violation.

PRACTICAL GUIDANCE

Labor Contracts and Internal Labor Rules

To ensure that employers comply with personal data obligations, employers should implement their obligations as they relate to the personal data of their employees, directors. Special consideration should also be made in relation to staff in employment agreements, employer's Internal Labor Rules, collective labor agreements.

To prevent future claims from employees over unpermitted processing of their personal data, employment agreements should clearly state that employees must be aware and must comply with requirements on personal data protection, and account for data processing by the Employer of employees' personal data for the purpose of employment (ie, tax information, health information, CVs, etc.). Employers should consider obtaining statements of clear and comprehensive consent from their employees, to treat their personal data.

Contracts

An enterprise should also consider updating current and future contracts with customers, to ensure that it is entitled to process and disclose specific personal data and that customers give consent.

Can companies of a multinational group located outside of Vietnam process personal data of a Vietnamese company member of the group? Yes, but the consent given by the employees should be drafted to cover this scenario.

In certain circumstances, the Internal Labor Rules must be registered with the authorities, but there is no requirement to register its Privacy Policy. As such, it may be beneficial if the Privacy Policy is separated from the Internal Labor Rules so it can be adjusted at will.

Key principles for the collection and processing of personal data under the Draft Decree

- **Lawful**: Personal data may only be collected/processed, when necessary, and as permitted by law.
- **Restricted use**: Personal data may only be used with the express consent of the data subject (or permission of a competent authority).
- **Purposeful**: Personal data may only be processed for the specific purposes for which the data subject has consented.
- **Security/confidentiality**: Measures must be in place to ensure the security and confidentiality of personal data during data collection, retention and processing.
- **Informed**: Data subjects must be informed of activities related to the processing of their personal data.
- **Minimization**: The personal data collected must be within the scope required to accomplish the specific authorized purpose.

Vietnam's data privacy protection regime continues to evolve. But enterprises should take measures to be prepared when the Draft Decree takes effect in December 2021. The Draft Decree introduces a number of new and material changes to the existing regime on data privacy protection. As more and more enterprises embrace industry 4.0, and increase their digital footprints, they naturally collect, receive, transmit, and use ever-increasing amounts of data from their customers, employees, and various other data subjects. Under the current language of the Draft Decree, indeed, it is hard to imagine an enterprise that would not qualify as a *Data Processor*.

The Government has solicited and received public comments on the Draft. The final version is likely to include a number of changes. However, we believe the most prudent approach, will be to prepare. Hence, enterprises are urged to work with the information available, and make a plan based on the current draft's language. Conducting a legal data audit, examining current policies, including the possibility to amend existing agreements, privacy policies, is a good starting point.