CHANDLER MHM

Personal Data Protection Act: A New Era of Privacy Rights in Thailand

14 March 2019

Introduction

After years of anticipation, on 28 February 2019, the National Legislative Assembly ("**NLA**") approved the Draft Personal Data Protection Act ("**PDPA**"), a law that was originally drafted in 2009. The PDPA is now awaiting royal endorsement and publication in the Royal Gazette.

Although the right to privacy is recognized under Section 32 of the Constitution, Thailand has never had a centralized law regarding data protection. Instead, there are a number of sector-specific laws regulating personal data (e.g. telecoms, financial institutions, securities etc). Consequently, up until now, issues relating to this matter arising between private parties were largely governed by Section 420 of the Civil and Commercial Code ("**CCC**"), the main body of laws governing general civil matters in Thailand. Section 420 of the CCC provides that if any person willfully or negligently injures any right of another person; such person shall make compensation to the affected individual. Note that the disclosure of personal data, in the case where a criminal offence is applicable, only related to the conduct of certain professionals as listed in Section 323 of the Penal Code. However, to date, the right to protection of personal data in Thailand has always been a blurred and a relatively untouched subject.

The PDPA is therefore drafted with the intention to provide better protection for individual's rights and the recent enactment of the EU's General Data Protection Regulation ("**GDPR**") has significant influence on the PDPA, its Thai counterpart. According to news sources, the Deputy General of the Ministry of Digital Economy and Society, the body overseeing this Act, has advised that 30 subordinated regulations are in the pipeline to supplement the PDPA. Under the PDPA, such subordinated regulations shall be issued within one year after the PDPA's promulgation. Note that PDPA will come into effect on the day after the PDPA's promulgation in the Royal Gazette (except certain provisions, i.e. Chapter 2: personal data protection, Chapter 3: right of personal data's owner, Chapter 5: petition, Chapter 6: civil liabilities, Chapter 7: penalties and Sections 95 and 96 which will come into effect one year after the PDPA's promulgation).

Notable Terms and Definitions

Before addressing each topic, the below terms are defined by the PDPA as follows:

- "**Personal Data**" means any data pertaining to a natural person which enables the identification of such person, whether directly or indirectly.
- "**Data Controller**" means any person or an entity which has the power to make decisions regarding collection, use, and disclosure of Personal Data.
- "**Data Processor**" means a person or an entity that conducts any

Key Contacts

Jutharat Anuktanakul
TEL+66-2-266 6485 Ext 151
(jutharat.a@chandlermhm.com**)**

Nuanporn Wechsuwanarux
TEL+66-2-266 6485 Ext 158
(nuanporn.w@chandlermhm.com**)**

Keiko Shirai
TEL +66-2-266-6485 Ext 345
(keiko.shirai@chandlermhm.com**)**

Kiratika Poonsombudlert
TEL +66-2-266-6485 Ext 153
(kiratika.p@chandlermhm.com**)**

Chandler MHM Limited
7th-9th, 12th, 16th Floor
Bubhajit Building
20 North Sathorn Road
Bangkok 10500, Thailand
www.chandlermhm.com

collection, use and disclosure of Personal Data on behalf of, or under the instruction of, the Data Controller.

- "**Person**" means natural person. Note that this means that juristic entities are not subject to the protection under the PDPA.

Scope of Applicability

The PDPA shall not apply to personal or household activities.

In terms of territory, the PDPA will apply to:

- any Data Controller or Data Processor residing in Thailand, regardless of whether or not the acquisition, usage or disclosure of the data is carried out in Thailand;
- in the case that the Data Controller or the Data Processor resides outside of Thailand, if the subject of the aforesaid activities is data belonging to a person residing in Thailand, the PDPA shall apply only when:
    - goods or services are being offered to such persons, regardless of whether any payment is involved; and
    - behavior surveillance activities of such persons take place within Thailand.

What if there is a sector-specific law for my organization?

According to Section 3 of the PDPA, in the case that there is a sector-specific law regarding Personal Data protection for an activity or an organization, such sector-specific law shall prevail, however:

- the provisions in the PDPA regarding collection, use or disclosure of Personal Data including the liabilities thereof shall apply along with and in addition to such sector-specific law, whether or not the two are repetitious.
- the provisions in the PDPA regarding filing claims and vesting of rights in officials, including the relevant liabilities thereof, shall be applicable insofar that:
    - The sector-specific law lacks provisions regarding filing claims; or
    - The sector-specific law contains provisions that vest the relevant authority the right to issue orders that protects the rights of the data owner, but not so extensive as the rights of the official under the PDPA.

Rights of the Data Owner

Consent is key (except when it is not)

When mentioning the rights of the owner of Personal Data, the basis of "consent" should be kept in mind. Unless the law specifies otherwise (this is discussed in more detail below), consent must always be obtained before acquiring Personal Data. Note that such consent must also be given in writing; or via electronic means, unless electronic acquisition of consent cannot be done due to its nature.

When acquiring Personal Data, the Data Controller shall inform the owner of Personal Data of the following particulars:

- purposes of data collection;
- types of Personal Data to be collected and time period for which it will be kept;

- types of relevant third parties to whom the Personal Data will be disclosed;
- information regarding the Data Controller and their contact information; and
- their rights of Personal Data owner under the PDPA, for example, right to withdraw consent, right to data portability, right to access their Personal Data and right to request the deletion or anonymization of their Personal Data.

As mentioned above, there are still certain exemptions to the consent requirements. Under the PDPA, consent is always required except when the Personal Data is collected in certain scenarios including:

- where it is collected for the interest of education, research, or statistics, and such Personal Data is protected appropriately in accordance with the announcement;
- where it is collected for purpose of preventing or suppressing danger to a person's life, body or health;
- where it is necessary for compliance with a legal obligation relating to public interest to which the Data Controller is the subject;
- where it is necessary for the performance of a contract to which the data owner is a party, or in order to take steps at the request of the data owner prior to entering into a contract; and
- where it is necessary for the purpose of the legitimate interests pursued by the controller or by a third party except where such interest are overridden by the data owner's fundamental rights relating to Personal Data.

Based on the scenarios above, it remains to be seen how these scenarios will be interpreted by the Thai authorities. For example, would acquiring Personal Data that the data owner voluntarily posts on social media constitute a violation of the PDPA? Or how extensive is the term "necessary" in this context?

Handling Personal Data

Specific Duties for Data Controllers

Other than ensuring that the Personal Data's owners are accorded to their rights discussed in the topic above, a Data Controller is also required to perform the following:

- implement suitable measures to prevent loss, unauthorized access, alteration or disclosure of Personal Data. However, what shall count as "suitable measures" will be prescribed by the subordinated regulations, which are yet to be issued;
- ensure that a third party who is not a Data Controller that acquires the Personal Data does not use or disclose the Personal Data wrongfully, or without authorization;
- maintain written records relating to processing activities, that can be inspected by data owners;
- delete Personal Data when the storage period expires, or the Personal Data is no longer relevant, exceeds the scope of necessity or consent is withdrawn; and
- notify the commission within 72 hours in case of a data breach, except in cases where such breach will not have a detrimental effect to the rights of the individual. If the breach will adversely affect the Personal Data owner, the Personal Data owner must also be presented with compensation measures.

Specific Duties for Data Processor
Other than the Data Processor's duty not to use Personal Data in manners that are not lawfully instructed by the Data Controller, the PDPA also requires the Data Processor to:

- implement suitable measures for preventing loss, unauthorized access, alteration or disclosure of Personal Data; and
- maintain written records for processing activities that can be inspected by the data owners.

*Common duties: Data Protection Officers ("**DPO**")*

Similar to the GDPR, both the Data Controller and the Data Processor are required to appoint DPOs to inspect their handling of Personal Data. The types of organizations that are required to have a DPO are:

- a governmental body designated by the Commission;
- an organization wherein the activities of the Data Controller/Data Processor consist of collecting, using and disclosing Personal Data by virtue of the organization's nature, or it requires routine monitoring due to the large scale of Personal Data being controlled or processed. However, the threshold of such scale remains to be prescribed by subordinated regulations; and
- an organization of which the core activities involve collecting, using and disclosing sensitive Personal Data.

What qualifications does a DPO need to have? Do I need to hire them?

Their qualifications are to be announced by subordinated regulations. However, considering that their duties are, for example, to provide advice to the Data Controller and the Data Processor in matters of compliance with PDPA and be the "contact persons" of the organization with regards to personal data protection matters, expertise and specialization in personal data protection matters is crucial.

A DPO can be an internal staff of the Data Controller or the Data Processor, or they can be an outsourced person.

Transfer to Third Countries

Similar to the GDPR, when transferring data to third countries, such recipient countries or recipient organization shall have a sufficient standard of data protection, except in circumstances as specified in the PDPA.

Liabilities and Penalties

Civil Liability

Actual damages

If the Data Controller or the Data Processor carries on any action that does not comply with the PDPA and such action damages the Personal Data owner, regardless of whether such noncompliance was carried on intentionally or negligently, the Data Controller and Data Processor shall be liable for actual damages arising therefrom, except where they can prove that (i) the damages were a result of force majeure, or by actions of the data owner; or (ii) the noncompliant act was a carried out in order to comply with an official's lawful order.

Punitive damages

Under the PDPA, the court is also empowered to order the Data Controller or the Data Processor to pay "punitive damages" in addition to actual damage. Such punitive damages shall not exceed two times the actual damages owed. Factors that the court will take into consideration when considering whether to order the punitive damages are, for example, financial status of the Data Controller or the Data Processor, and/or the extent of participation/involvement of the Data Controller or Data Processor in the act that resulted in causing such damage.

Penal Penalties

Failure to comply with the PDPA may result in penalties being imposed on both the entity and any directors who collaborate to commit the offence or do not reasonably manage to prevent such offence. Such penalties include both fines and imprisonment.

Administrative Penalties

Administrative penalties in the case of violation of the PDPA shall not be in excess of THB 500,000, or not in excess of THB 5 million, depending on the severity and type of violation.

Transition Period

Any Personal Data collected or retained prior to the enactment of the PDPA can be kept and used in accordance with the purposes informed to the Personal Data owner when their Personal Data was collected. However, the Data Controller is required to inform the data owner a method in which they may withdraw consent. The consent withdrawal method must also be publically available.

As the PDPA will unquestionably have a significant impact on business transactions, Chandler MHM will continue to monitor this important legislation, and will issue updates on further developments as they occur.