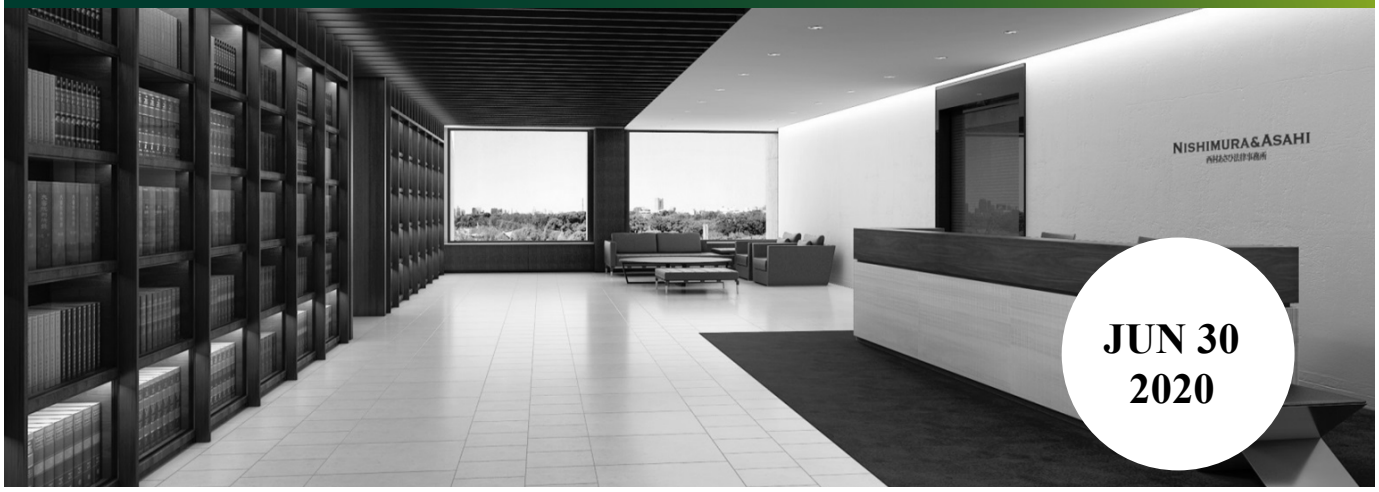
西村あさひ法律事務所
NISHIMURA & ASAHI
Corporate Crisis Management Newsletter
Asia Newsletter



Outline of the 2019 Personal Data Protection Act in Thailand

Jun Katsube, Chanakarn Boonyasith, Pitchabsorn Whangruammit

Introduction

The 2019 Personal Data Protection Act (the "**PDPA**") is the first personal data protection law generally applicable to most private sectors in Thailand. Previously, data protection in Thailand merely applied to specific sectors/businesses, such as the government sector (in relation to personal data kept with government authorities), telecommunication businesses, credit bureaus, etc. For said specific businesses, the PDPA requires that they continue to comply with both the previously existing applicable laws and the PDPA.

The PDPA was issued on, and has been in force since, 27 May 2019. Most of its provisions, most importantly those governing personal data protection, rights of personal data, filing of complaints, and punishments, were planned to become effective on 27 May 2020. However, due to the COVID-19 outbreak, a Royal Decree was issued on 21 May 2020 suspending enforcement until 31 May 2021. The purpose of this suspension was to allow more time for business operators to familiarise themselves with, and prepare for full enforcement of, the PDPA. As of the date of preparation of this newsletter, none of the subordinate legislation under the PDPA has been passed (except those regarding the criteria for selecting and appointing a Chairperson and honorary directors in the Personal Data Protection Committee). Therefore, in certain areas, we are still awaiting clear guidelines from the relevant authority. Despite this, business operators would be well-advised to prepare for PDPA compliance and take the necessary measures required by the PDPA before 1 June 2020.

The PDPA largely embraces provisions of the EU's General Data Protection Regulation ("**GDPR**"). Therefore, it might be helpful for business operators to familiarise themselves with the GDPR in order to understand how likely it is that the PDPA will

affect personal data protection in Thailand. Nonetheless, it is important to be aware that there are still differences between the GDPR and the PDPA; therefore, the PDPA should not be interpreted in necessarily the same ways as the GDPR in all respects. Some of the PDPA's important provisions* are summarised below:

**Note:* *This Article is aimed to be a friendly introduction to the PDPA. It does not include all the obligations of Data Controllers and Data Processors as required by the PDPA.*

1. The PDPA controls acts involving the collection, use, or disclosure of Personal Data

Instead of governing the 'processing' of personal data, like in the GDPR, the PDPA generally refers to protection against 'collection, use or disclosure' of personal data. Under the PDPA, for example, it will be necessary to obtain a data subject's consent during collection, use or disclosure of their personal data. Although the term 'process' is clearly defined under the GDPR, there are no definitions for the phrase 'collect, use and disclose' or the individual terms thereof in the PDPA. For general meaning, the said words have relatively broad scopes in the Thai context and should be able to cover most activities concerning Personal Data.

2. Definitions

Section 6 of the PDPA sets out definitions of a few terms. Interestingly, some of the important terms under the GDPR, such as 'consent', 'personal data breach' and 'profiling', are not defined under the PDPA.

According to the PDPA, *key legal terms* are defined as follows:

'*Personal Data'* means any information relating to a person, which enables the identification of such person, whether directly or indirectly, but not including the information of deceased persons.

'*Data Controller*' means a person or juristic person having the power and duties to make decisions in regard to the collection, use or disclosure of personal data.

'*Data Processor*' means a person or juristic person who performs operations in regard to the collection, use or disclosure of personal data under the order or on behalf of the Data Controller.

'*Person*' means a natural person.

3. What will happen to Personal Data collected before the PDPA came into force?

With respect to Personal Data that was collected before the effective date of the PDPA (i.e. 1 June 2021), a Data Controller will still be able to continue to collect and use said personal data, but only for the original purposes of such collection (in accordance with transitional provisions under Section 95 of the PDPA). In a case where the original purpose is unclear, the Data Controller should limit the collection and use of said Personal Data only to the extent that an ordinary person reasonably would expect the Data Controller to do so. Furthermore, Section 95 also requires the Data Controller to determine and publicise the method through which data subjects are able to easily notify the Data Controller of his/her intent to withdraw consent when he/she does not wish the Data Controller to continue collecting and using his or her Personal Data.

For the disclosure of Personal Data and activities other than collection and use thereof, the Data Controller will be required to comply with the provisions of the PDPA.

4. Extraterritorial Applicability

The new concept of 'Extraterritorial Applicability', which appeared in the GDPR, also applies to the PDPA. Section 5 paragraph 1 of the PADA notes that it shall apply to the collection, use or disclosure of Personal Data by **a Data Controller or Data Processor located in Thailand.** In addition to this, by virtue of PDPA Section 5 paragraph 2, the PDPA shall also apply to the collection, use or disclosure of the Personal Data of a data subject who is located in Thailand if it is performed by **a Data Controller or Data Processor located outside Thailand**, for activities which are related to the following:

(1) Offering of goods or services to data subjects in Thailand, irrespective of whether or not a payment has been made by the data subject; or

(2) Monitoring of a data subject's behaviour which takes place within Thailand.

Should this be the case, a Data Controller who is subject to the provisions of the PDPA in accordance with Section 5 paragraph 2 is required to designate, in writing, its representative; who must be located in Thailand and be authorised to act on its behalf without limitation of liability, in accordance with Section 37 paragraph 5 of the PDPA. Affiliates of the Thai entity located outside Thailand thus may also need to comply with the PDPA if they conduct activities stated in Section 5, paragraph 2 of the PDPA.

5. General Principles of Collection, Use or Disclosure of Personal Data

First, a Data Controller shall not be able to collect, use and disclose Personal Data unless the data subject grants his/her consent before or at least at the time such collection; except where the PDPA or other applicable laws allow him/her to do so without the data subject's consent. Exemptions provided under the PDPA are, for example, Section 24 for general Personal Data (please refer to Part 7 below); and Section 26 for sensitive Personal Data (please refer to Part 8 below).

Second, consent is still required from data subjects under 'legal age' (legal age in Thailand is 20 years old; or 17 years old if the person is legally married) or otherwise incompetent under Thai law. For a minor who is 10 years old or above, consent must be required from both the minor and the holder of parental responsibility over the child. If the minor is under 10 years old, consent must be required only of the holder of parental responsibility over the child. Likewise, in the event where the data subject is incompetent, consent must be obtained from a custodian who has the power to act on behalf of the incompetent person. In the event where the data subject is quasi-incompetent, consent must be obtained from a curator who has the power to act on behalf of the quasi-incompetent person. The aforesaid also applies to the withdrawal of consent; notice given to the data subject; exercise of the data subject's rights; complaints of the data subject; and any other acts under the PDPA involving data subjects considered minors, or incompetent or quasi-incompetent persons.

Third, a Data Controller must collect, use or disclose Personal Data only for the purposes of which the data subject has been informed prior to, or at least at the time of, the collection. Any uses incompatible with said purposes are prohibited unless: (i) such

new purpose has been informed to the data subject and his/her consent has been given before said collection, use or disclosure of the Personal Data; or (ii) provisions of the PDPA or other laws allow it.

6. Conditions of Consent

A Data Controller needs to take into account the following conditions when obtaining a data subject's consent:

(1) The request for consent must be clearly made in writing or via electronic means;

(2) The Data Controller must inform a data subject of the purposes for which his/her personal data will be collected, used or disclosed. The request for consent must be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language, and not deceptive or misleading to the data subject in respect of such purpose. Said form may thereafter be determined by Notification of the Committee of Personal Data Protection.

(3) Utmost care must be taken to ensure the data subject's consent has been given freely. Moreover, in entering into a contract or providing a service, it must not be conditional upon obtaining consent to the collection, use or disclosure of Personal Data that is not necessary for or relevant to such execution of contract or provision of services.

(4) The data subject shall have the right to withdraw his or her consent at any time. It must be accomplishable in a manner that is as easy as the manner the consent was given. Withdrawal of consent shall not affect the collection, use or disclosure to which the data subject has already consented legally under the PDPA.

7. Exemptions for Consent

The PDPA provides that 'consent' is the only basis on which the Data Controller must focus in the collection, use or disclosure of personal data; unless provisions of the PDPA itself or any other laws allow Personal Data to be collected, used or disclosed without consent of the data subject. For Personal Data which is not sensitive data (for sensitive data, please refer to Part 8 below), Sections 24 and 27 of the PDPA stipulate the exemptions where consent is not required for collecting, using or disclosing thereof, which could be summarised as follows:

(1) For achievement of purposes relating to the preparation of historical documents or archives of public interest, or for purposes relating to research or statistics;

(2) For preventing or suppressing danger to a person's life, body or health;

(3) Necessary for the performance of a contract to which the data subject is a party;

(4) Necessary for the performance of a task carried out in public interest by the Data Controller;

(5) Necessary for legitimate interests of the Data Controller; and

(6) Necessary for compliance with law.

8. Sensitive Data

For sensitive data, 'explicit consent' of a data subject is required in collecting, using or disclosing thereof, pursuant to Sections 26 and 27 of the PDPA. Sensitive data includes Personal Data pertaining to racial and ethnic origin, political opinions, cults, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disabilities, trade union information, genetic data, biometric data or any data which may affect the data subject in the same manner. For 'biometric data', the PDPA further defines it as the Personal Data arising from the use of techniques or technologies related to the physical or behavioral dominance of a natural person, which can be used to identify such person apart from other persons, such as facial recognition data, iris recognition data or fingerprint recognition data. It is noteworthy that exemptions of the consent required for collection, use or disclosure of sensitive data are more limited and different from general Personal Data as stated under Section 24 above (for information on general Personal Data, please refer to Part 6 above). A Summary of exemptions where 'explicit consent' does not need to be required for collecting, using or disclosing sensitive data follows:

(1) Where it is to prevent or suppress a danger to the life, body or health a person;

(2) Where it is carried out in the course of legitimate activities with appropriate safeguards by the foundations, associations or any other not-for-profit bodies with political, religious, philosophical or trade union purposes for their members, former members of the bodies or persons having regular contact with such foundations, associations or not-for-profit bodies in connection with their purposes - without disclosing the Personal Data outside of such foundations, associations or not-for-profit bodies;

(3) Where it is information that is disclosed to the public with the explicit consent of the data subject;

(4) Where it is necessary for the establishment, compliance, exercise or defence of legal claims; and

(5) Where it is necessary for compliance with a law to achieve purposes in respect of specific matters described in the PDPA.

Based on the aforementioned, the Data Controller thus firstly needs to assess whether the Personal Data they collect, use or disclose is sensitive data; since different concepts of consent and exemption apply.

9. Informed Consent

To remain in compliance with Section 23 of the PDPA when obtaining consent, a Data Controller is required to inform data subjects, at the very least, of the following matters:

(1) Purpose of collection (including the purposes that allow for collection of Personal Data without the data subject's consent under Section 24 of the PDPA, as referred to in Part 7, above);

(2) Notification of the case where the data subject is required to give Personal Data to be in compliance with laws or contracts, or where such Personal Data is necessary for entering into a contract, and any possible effects arising from refusing to provide such Personal Data;

(3) Personal Data to be collected and the period of time such collected Personal Data will be retained;

(4) Person(s) to whom the Personal Data may be disclosed;

(5) Contact information of the Data Controller or, where applicable, the Data Controller's representative (please refer to Part 4, above) or data protection officer (please refer to Part 11, below), if any; and

(6) Rights of the data subject.

10. Transfer of Personal Data to Foreign Country

Section 28 of the PDPA requires that, in the event where the Data Controller sends or transfers the Personal Data to a foreign country, the destination country or international organisation which receives such Personal Data must have adequate data protection standards, and such transfer shall be carried out in accordance with the rules for the protection of Personal Data to be prescribed by the Personal Data Protection Committee. The Data Controller may otherwise make such transfer based on certain exemptions provided under the PDPA, such as for purposes involving compliance with the law or performance of a contract to which the data subject is a party, or where data subject's consent has been obtained.

Alternatively, to be considered exempt from compliance with Section 28 of the PDPA when sending or transferring Personal Data to a Data Controller or Data Processor in the same affiliated business or group of undertakings located in a foreign country (for the purpose of jointly operating such business or group of undertakings), a Data Controller or Data Processor located in Thailand must put in place a 'personal data protection policy' that has been reviewed and certified by the Personal Data Protection Office. Nonetheless, regulations on the Personal Data protection policy, the nature of the same affiliated undertaking or affiliated business considered to be "jointly operating" the undertaking or business, and the rules and methods for the review and certification in the above paragraph have not yet been prescribed bythe Personal Data Protection Committee.

11. Data Protection Officer

Not all Data Controllers and Data Processors are required to have a data protection officer ("DPO"). Indeed, DPO are only required in the following cases:

(1) Where the Data Controller or Data Processor is a public authority as prescribed and announced by the Personal Data Protection Committee;

(2) Where the activities of the Data Controller or Data Processor in the collection, use or disclosure of Personal Data require regular monitoring of the Personal Data or the system, by reason of their having control over a large amount of Personal Data according to the standards prescribed by the Personal Data Protection Committee; or

(3) Where the core activity of the Data Controller or Data Processor is the collection, use or disclosure of sensitive Personal Data according to Section 26 of the PDPA (please refer to Part 8, above).

The DPO's duties are, among others, to give advice to the Data Controller or Data Processor, including the employees or service providers of the Data Controller or Data Processor with respect to compliance with the PDPA. The DPO can be either a staff member of the Data Controller or Data Processor, or a service provider under contract with the Data Controller or Data Processor. Nonetheless, as of the date of preparation of this newsletter, it is not practical to appoint a DPO due to a lack of regulations clarifying the required qualifications of a DPO, which are yet to be prescribed by the Personal Data Protection Committee.

12. Rights of Data Subject

The following Data Subject rights are recognised under the PDPA:

- Right of access by Data Subject
- Right to data portability
- Right to object
- Right to erasure of data
- Right to rectification
- Right to restrict the collection, use, or disclosure of their data

The PDPA does not yet entail the process of how a Data Subject should go about applying their rights; the details may be determined in subordinate legislation at a later stage.

13. Complaint

A data subject is entitled to lodge a complaint with an Expert Committee* in cases where the Data Controller, Data Processor or its respective employee or contractor violates, or does not comply with a provision of the PDPA. The Expert Committee will have the authority to review and decide on said complaint. It is important to be aware that the Expert Committee is empowered to impose administrative fines (please refer to Part 14, below) against the wrongdoer, if considered appropriate.

**Note* *At the time of preparation of this newsletter, the Expert Committee has not yet been established.*

14. Punishment

Punishments imposed under the PDPA are unique and different from most legislation in Thailand because it provides three types of liabilities: (i) civil liability; (ii) criminal liability; and (iii) administrative liability.

With regard to *civil liability*, in addition to normal actual damages granted by the court in the event of a general wrongful act, the PDPA allows the court to award punitive damages not exceeding twice the amount of such actual compensation, by taking into account the related circumstances, such as the severity of damages incurred by the Data Subject, the interest obtained by the Data Controller or Data Processor, the financial status of the Data Controller or Data Processor, the remedy provided by the Data Controller or Data Processor, or the Data Subject's role in creating the damages (if any). Claims for compensation deriving from a wrongful act involving Personal Data under the PDPA shall be barred by prescription after the lapse of three years (whereas for a general wrongful act it is only one year) from the date on which the injured person first knows of the damages and identity of the

liable Data Controller or Data Processor, or after 10 years from the date on which the wrongful act involving the Personal Data took place.

Criminal liability is generally limited to violations committed by the Data Controller against sensitive data that is likely to cause damage to another person, impair his or her reputation, or expose such other person to scorn, hate or humiliation; or in order to unlawfully benefit him/herself or another person. In case the Data Controller is a juristic person, and the offence is conducted as a result of the instructions given by or the act of omission by any director, manager or other person who shall be responsible for such act of the juristic person, such person shall also be subject to the punishment prescribed for such offence. Criminal liability may also extend to apply to any person who comes to know the Personal Data of another person as a result of performing duties under the PDPA, such as a PDO, and who discloses such information to any other person without consent of the Data Subject. Criminal liability includes imprisonment, a fine or both.

As for *administrative liability*, as mentioned in Part 12, above, when a matter is lodged with the Expert Committee, the Expert Committee is empowered to impose an administrative fine over the wrongdoer in such case. Administrative fines under the PDPA are quite high. The highest administrative fine imposed under the PDPA is equivalent to Baht 5,000,000 (five million Thai baht).

Jun Katsube
Partner, Nishimura & Asahi
j_katsube@jurists.co.jp

Jun Katsube joined Nishimura & Asahi in 2006. He obtained his LL.M. from the University of Southern California Gould School of Law in 2013, was admitted in New York and California in 2014 and 2017, respectively, and worked for the Asia Pacific Legal Division of Mitsui & Co. from 2014 to 2016. He specializes in corporate crisis management matters, including competition law issues, accounting fraud, and quality data falsification.

Chanakarn Boonyasith
Partner, SCL Nishimura
chanakarn@siamcitylaw.com

Chanakarn Boonyasith specialises in corporate & commercial law, labour & employment law, and commercial contracts. She advises multinational clients on matters of private and public transactions from a wide range of industries. Chanakarn Boonyasith has been a guest speaker on Thai employment law and data protection law in various domestic and international events and a part-time lecturer with several universities in Thailand. Chanakarn is also a regular contributor to a number of domestic and international law journals.

Pitchabsorn Whangruammit
SCL Nishimura
pitchabsorn@siamcitylaw.com

Pitchabsorn Whangruammit is an enthusiastic associate specializing in employment and personal data protection law-related matters. She provides timely advice, deals with relevant authorities, and reviews and provides comments on various types of contracts and legal documents. As a versatile member of the SCL team, she also has experience in international arbitration and trade and commercial law.