L&P

Newsletter No. 224 (EN)

The Personal Data Protection Act B.E. 2562 (2019)

March 2020

All rights reserved © Lorenz & Partners 2020

Although Lorenz & Partners always pays great attention on updating information provided in newsletters and brochures we cannot take responsibility for the completeness, correctness or quality of the information provided. None of the information contained in this newsletter is meant to replace a personal consultation with a qualified lawyer. Liability claims regarding damage caused by the use or disuse of any information provided, including any kind of information which is incomplete or incorrect, will therefore be rejected, if not generated deliberately or grossly negligent.

1. Introduction

The importance of handling of personal data steadily increases for businesses. Following Europe and the USA which both have a strict data protection law in place, Thailand has now also taken steps to assure that personal data is not freely used and traded. Data controller businesses who collect, use and disclose personal data as part of their business model shall keep in mind that after the effective date of the Personal Data Protection Act ("**PDPA**"), certain information cannot be as freely processed and used as in the past.

The company must comply with the legal requirements under the PDPA. Legal compliance will increase cost, so companies must wisely choose to collect only necessary data.

2. Thai Laws related to Personal Data Protection

- **Personal Data Protection Act B.E. 2562 (2019)**

The PDPA was enacted on 27 May 2019 and is effective since 28 May 2019. Certain requirements under the PDPA (e.g. Chapter 2, 3, 5, 6, 7, Section 95 and 96) will become effective on 27 May 2020, after the PDPA committee has been properly established.

The PDPA provides protection for personal data which can identify an individual, regardless of the format of the data (e.g. online database, but also printed data on paper).

This law constitutes legal obligations between the data subject and the data controller. The data controller (normally a company) is the key person who collects and utilizes personal data of the data subject (such as an employee, a client, or a customer). If personal data is damaged or lost due to insufficient privacy protection and preventive measures, the data controller shall be liable. The PDPA makes it easier for the data subject to claim damages against the responsible person, who can be easily identified. The PDPA also applies to an individual or juristic person who processes the data as per instruction or on behalf of the data controller (so-called data processor).

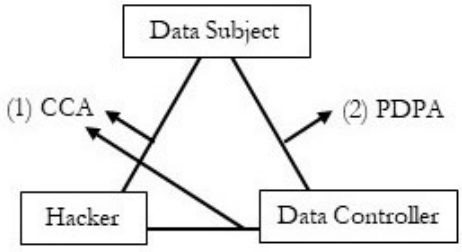
The PDPA's content is mostly adapted from the EU's General Data Protection Regulation. However, there are some parts that have been developed with regard to special local practices in Thailand.

- **Computer Crime Act B.E. 2560 (2017)**

Besides the PDPA, the Computer Crime Act provides protection for information that is computer data or stored in a computer systems against outside threats (e.g. hacker, unauthorized access etc.).

Often times, cybercrime offenders (hackers) are difficult to identify. Therefore, most of the time they cannot be arrested, which means damage incurred by the data subject cannot be recovered. This was one of the major factors that drove the implementation of the PDPA.

The diagram below shows the laws that govern each specific relationship.



In this newsletter, we will only focus on protection of personal data under the PDPA.

3. Personal Data

Under the PDPA, there are two types of personal data:

- **Personal data** (Section 6 PDPA) is any data pertaining to a person, which enables the identification of such person, whether directly or indirectly. For example: name, address, phone number, customer ID, age, gender, height, username, password, IP address. The PDPA does not cover data of juristic persons and data of dead persons.

- **Sensitive personal data** (Section 26 PDPA) is personal data regarding race, ethnic origin, political opinion, beliefs, religion, philosophical opinions, sexual orientation, criminal record, health, disability, labour union information, genetic features, biography, or other information which may affect the data subject in the same or a similar way.

4. Enforcement Scope of the PDPA

The PDPA applies to any data controller and data processor:

- who is in Thailand, regardless of whether the data is processed inside or outside of Thailand; and

- who is outside of Thailand, but the data subject is in Thailand for certain activities (e.g. offering goods or services, monitoring the behavior of the data subject in Thailand). In this case, the data controller must appoint a representative in writing to operate in Thailand.

The main protections under the PDPA are against (i) data collection and (ii) data usage and disclosure.

5. Data Collection

5.1 General protection

"The collection of personal data shall be limited to the extent necessary in relation to the lawful purpose of the data controller." (Section 22 PDPA)

Moreover, in principle, the data controller shall collect such data from the data subject directly (Section 25 PDPA).

5.2 Notification to the data subject

In order to collect personal data, the data controller shall notify the data subject, on or before the time of data collection, of the following details according to Section 23 PDPA (unless the data subject already knows such information):

- collection purpose
- reason why data collection is necessary
- data to be collected and period
- person/entity to whom the data will be disclosed to
- contact details of the data controller
- rights of the data subject

5.3 Consent required for data collection

Theoretically, personal data cannot be collected without consent. In fact, consent required for general personal data and sensitive personal data is different. To be more specific, general personal data requires consent, either implied or explicitly. In contrast, sensitive personal data requires explicit consent (consent to be further discussed under item 7 below).

5.4 Exemptions for data collection without consent

The exemptions for personal data and sensitive data collection are slightly different.

- **Personal data** (Section 24 PDPA):
  (1) **Historical documents or archives**: necessary for making historical

documents or archives for the public, research/statistics, with appropriate data protection measures;
(2) **Vital interests**: to prevent harm to a person's life, body, or health;
(3) **Performance of a contract**: for the performance of a contract as intended by the data subject;
(4) **Necessary for public interest**: to carry out tasks for the public interest, or exercise official authority vested to the data controller;
(5) **Legitimate interests**: for the legitimate interests of the data controller or other third parties, unless the fundamental rights of the data subject outweigh such legitimate interest.
(6) **Legal compliance**: for compliance with legal obligations.

- **Sensitive personal data** (Section 24 PDPA):
(1) **Vital interests**: same as above;
(2) **Non-profit organization**: for legitimate activities of a non-profit organization, for political, philosophical, religious, or trade union purpose, for its members, former members, or persons who regularly contact the organization (without disclosing to third parties);
(3) **Public domain**: disclosed to the public with the consent of the data subject;
(4) **Legal claims**: necessary for establishing, exercising, or defending legal claims;
(5) **Necessary for legal compliance for the below purposes:**
a) Medical purposes;
b) Public health;
c) Labour protection and social security;
d) Scientific, historical, or statistical research;
e) Substantial public interest.

6. Data Usage and Disclosure

Apart from the data collection as mentioned above, the data controller must also obtain consent for any data usage and disclosure. However, if the data collection purpose falls under the exemption (as mentioned above), the consent is not required for usage and disclosure of the same data (Section 27 PDPA).

In case personal data is transferred outside of Thailand or to an international organization, the destination country or the international organization must have sufficient data protection measures. There are exemptions and specific circumstances as specified in Section 28 and 29 PDPA.

7. Consent

7.1 Type of consent

- **Explicit consent** is consent that is clearly given by the data subject, provided that he/she has the option to agree or disagree with the collection, use, or disclosure of personal data.

- **Implied consent** is usually inferred from the actions and the relevant circumstance.

7.2 Legal requirements for consent

(Section 19 PDPA)

- **Form**: Consent must be expressly given, in writing or through an electronic system, unless consent cannot be given by such methods.

- **Format**: The request for consent must be easy to understand, explicitly separated from other messages, and the purpose of data collection must be stated.

- **Freedom**: The data subject's freedom must be taken into account when asking for consent (freely given).

If the request for consent does not fulfil the aforesaid requirements, such given consent will **not** bind the data subject. Therefore, the data controller cannot legally collect, use, or disclose personal data.

8. Rights of the Data Subject

Under the PDPA, the data subject has the following legal rights:

- **Right to access** (Section 30 PDPA):
  The data subject can request a copy of the personal data under the responsibility of the data controller, and request the data controller to reveal how they obtained the personal data for which the data subject did not give its consent.

- **Right to data portability** (Section 31 PDPA):
  The data subject can request for his/her personal data to be transmitted to another controller without hindrance.

- **Right to object** (Section 32 PDPA):
  The data subject can object to the collection, usage, or disclosure of personal data.

- **Right to be forgotten** (Section 33 PDPA):
  The data subject can request for his/her personal data to be erased, destroyed or anonymized in specific cases.

- **Right to cease usage** (Section 34 PDPA):
  The data subject can request the data controller to cease the usage of his/her personal data.

9. Other Specific Duties

9.1 Data controller

The duties of the data controller under Section 37 PDPA are as follows:

- Imposing appropriate measures to protect and secure personal data;
- Creating a system to erase and destroy unused/unnecessary data;
- Notifying any violation of personal data to the Office of the Personal Data Protection Committee without delay; and
- Appointing a representative in writing (for the data controller outside of Thailand only).

9.2 Data processor

The duties of the data processor under Section 37 PDPA are as follows:

- Processing the data under instruction of the data controller;
- Imposing appropriate measures to protect and secure personal data; and
- Making and keeping records of processing activities.

9.3 Data Protection Officer (DPO)

For the private sector, the data controller and/or the data processor must appoint a DPO in case their activities involve massive amounts of data (to be defined by the Committee) or their major activities are to process sensitive data.

The duties of the DPO under Section 42 PDPA are as follows:

- Giving advice in relation to compliance with the PDPA;
- Checking and monitoring related entities concerning data processing under the PDPA;
- Cooperating with the Office of the Personal Data Protection Committee; and
- Keeping confidentiality of the personal data known from the duties under the PDPA.

10. The Personal Data Protection Committee (Committee)

The duties of the Committee (Section 16 PDPA) are mainly to enact specific regulations under the PDPA, provide official interpretation, render orders in relation to the PDPA.

11. Liability/Penalty

There are three types of liability/penalty under the PDPA:

11.1 Civil liability

The data controller and data processor are liable for damages from violations (intentional/negligent) of the PDPA, which include the expenses for preventive measures against the occurred or future damages. Additionally, the court can order to pay punitive damages, on top of the actual damages.

The prescription period of the claim for damages is 3 years after knowing about the damages and responsible person, or 10 years after the violation of the personal data.

11.2 Criminal penalty

There are criminal liabilities for:

- data controllers who use or disclose personal data or send sensitive data abroad in violation of the law, which may lead to damages or humiliation, or to illegally acquire benefits;
- persons who acquire knowledge of the personal data due to the duties under the PDPA and disclose it to another person.

The criminal penalties are imprisonment for 6 months – 1 year, or fines of up to THB 1,000,000, or both, depending on the violation.

11.3 Administrative penalties

The authority may also impose an administrative penalty for the violation of the PDPA with the maximum administrative fine between THB 500,000 – 5,000,000.

12. Data Protection Best Practices

Besides the legal duties under the PDPA, the company may decide to adopt new policies and procedures to strengthen data protection within the company. For example:

- Perform gap analysis on the areas that are not compliant with the law;
- Identify data flows in the company;
- Create a data protection risk framework;
- Review all consent forms and contracts;
- Create data breach monitoring and response program; and
- Appoint DPO to manage organizational data protection and oversee compliance.

Additionally, the company may consider establishing related policies (e.g. IT, social media/social network policy) on top of the data privacy policy.

We hope that the information provided in this newsletter is helpful for you.
If you have any further question, please do not hesitate to contact us.

LORENZ & PARTNERS Co., Ltd.
27th Floor Bangkok City Tower
179 South Sathorn Road, Bangkok 10120, Thailand
Tel.: +66 (0) 2-287 1882
E-Mail: info@lorenz-partners.com