VERITAS LAW

# Overview of Personal Data Protection Act

## Introduction

Until recently, Thailand had no specific legislation regarding personal data protection. Instead, personal information was protected by:

- general laws (eg, the Constitution and laws pertaining to wrongful acts specified by the Civil and Commercial Code); and
- specific laws which protect only certain information (eg, the Official Information Act 1997 (BE 2540), which protects only personal information that a state agency possesses or controls).

In 2009 the first Personal Data Protection Bill was introduced, followed by various drafts and amendments thereto. On 28 February 2019 the National Legislative Assembly approved the latest version of the Personal Data Protection Bill. On 28 May 2019 the first consolidated Personal Data Protection Act (PDPA) (BE 2562) took effect.

## Effective date

Although the PDPA took effect on 28 May 2019, some of its operative chapters were originally due to take effect one year later (ie, 28 May 2020). This was to provide sufficient time for entities and government authorities to comply with the new law's provisions. Further, it was initially intended that the Personal Data Protection Committee – which will determine the details, criteria, processes, standards and guidelines pertaining to the PDPA – would be appointed through the issuance of subordinate legislation or regulations before 28 May 2020.

However, on 20 May 2020 the Cabinet issued a royal decree to postpone the enforcement of the PDPA's operative chapters for another year due to the COVID-19 pandemic. Therefore, subject to any further amendments, the PDPA will fully take effect on 1 June 2021.

Until this date, no specific legal restrictions exist regarding the collection, use, transfer or disclosure of personal data, since the enforcement postponement primarily affects the PDPA's key operative provisions. However, after 1 June 2021, these actions must

comply with the PDPA, regardless of whether the committee has been appointed and the subordinate legislation or regulations have been issued.

**Key definitions**

The PDPA provides various definitions, which help users to understand to what extent and to which parties the PDPA applies, including:

- 'personal data' – any information relating to a person which enables their identification, whether directly or indirectly, excluding information relating to deceased people;
- 'sensitive data' – data which includes:
    - personal data that pertains to a person's racial or ethnic origin, political, religious or philosophical beliefs, sexuality, criminal record, health or trade union;
    - genetic and biometric data; and
    - any other data that may affect the data subject in the same manner as the aforementioned categories of data;
- 'biometric data' – personal data that arises from the use of technology, relates to a person's physical or behavioural character and can be used to identify such person (eg, facial, iris or fingerprint recognition data);
- 'data controller' – a natural or juristic person that has the power and duties to make decisions regarding the collection, use and disclosure of personal data; and
- 'data processor' – a natural or juristic person that is not a data controller but operates in relation to the collection, use or disclosure of personal data pursuant to orders given by or on behalf of a data controller.

**Relevant parties**

Four major parties are subject to the PDPA:

- data subjects;
- data controllers;
- data processors; and
- the committee.

### *Data subjects*

The PDPA protects only individuals whose personal data has been processed by data controllers or data processors by means regulated thereunder. Therefore, the PDPA does not protect the data of juristic people.

### *Data controllers and processors*

Data controllers are individuals or entities which collect, use or disclose data subjects' personal data. Data controllers have most duties under the PDPA, the main categories of which are:

- duties towards data subjects, including:
    - providing data subjects with the minimum information necessary when processing personal data; and
    - ensuring that data subjects' rights are recognised; and
- duties within their business, including:
    - implementing security measures (eg, data disposal procedures);
    - notifying the relevant parties of data breaches;
    - preparing data processing agreements;
    - keeping records of processing activities; and
    - ensuring that sufficient data protection standards exist in foreign countries to which data is transferred.

The PDPA imposes fewer duties on data processors. However, a data processor may be liable under the PDPA where it processes personal data beyond the data controller's instructions.

Data controllers and data processers may also have to appoint:

- a data protection officer; and
- a local representative, where personal data is processed overseas.

### *Committee*

The committee will act as a regulator to ensure compliance with the PDPA. The duties of the committee include:

- devising a masterplan for the protection of personal data;
- determining operational measures or guidelines regarding personal data protection; and
- issuing notifications or rules for the execution of the PDPA.

**Scope of application**

The PDPA applies both territorially and extra-territorially. Therefore, data controllers and processors both in Thailand and overseas will be subject to the PDPA where they process personal data of data subjects in Thailand, subject to certain exceptions.

**Legal bases**

Data subject consent is the main legal basis on which data may be processed. The PDPA also provides that data may be processed:

- for historical, research or statistical purposes;
- for a vital interest (ie, to prevent or eliminate danger to an individual's life, body or health);
- to comply with a legal obligation;
- on a contractual basis (ie, for the performance of a contract to which the data subject is a party);
- in the public interest (ie, in compliance with a legal obligation relating to the public interest); or
- for a legitimate and lawful interest, provided that such interest does not override the data subject's fundamental rights.

The processing of sensitive data must meet certain additional legal criteria.

**Data subject rights**

Under the PDPA, subject to various exceptions, data subjects have the right to:

- be informed about the collection and retention of their data;
- access and obtain their data records;
- send or transfer their data (known as 'data portability');
- object to the collection, use or disclosure of their data;
- request the erasure of their data;

- restrict the processing of their data;
- rectify their data;
- withdraw their consent to the collection, use or disclosure of their data; and
- complain about the collection, use or disclosure of their data.

**Penalties**

The PDPA imposes the following penalties for non-compliance:

- for civil liability – compensation up to two times the amount of the actual damages;
- for administrative liability – an administrative fine of up to Bt5,000,000;
- for criminal liability:
    - between six months' and one year's imprisonment;
    - a fine of between Bt500,000 and Bt1 million; or
    - both imprisonment and a fine.

In cases of criminal liability, where an offender violates the PDPA because of the actions or instructions of a director, manager or authorised person, such party will receive the same criminal penalty as the offender.

**Effect on business practices**

The PDPA applies to any party which collects, uses or discloses personal data, regardless of the quantity of personal data that it processes. However, certain exceptions may apply to small or medium-sized enterprises, subject to additional criteria which the committee will issue.

Businesses must:

- change the way in which they collect, use and disclose not only their customers' personal data, but also that of their employees and business partners;
- create a new culture regarding the processing of personal data and ensure that all parties are aware of and remain compliant with the PDPA.

**Preparation for PDPA compliance**

During the transition period, businesses must:

- identify any areas in which they do not comply with the PDPA and bridge such gaps;
- determine the legal basis for each activity which involves the processing of personal data;
- prepare a new privacy policy or revise their existing policy and any underlying documentation to ensure compliance with the PDPA;
- train all relevant parties about the PDPA; and
- ensure that all business partners acknowledge their new personal data protection culture.

Businesses may wish to simultaneously implement IT-related personal data management processes.

**Comment**

Even though the PDPA has yet to fully take effect and the committee has not yet issued the expected subordinate legislation and procedural framework, most businesses have begun implementing measures to ensure their compliance with the PDPA.

Given the current lack of regulations, many businesses have used the EU General Data Protection Regulation (GDPR) as a guideline during this uncertain period. However, businesses should be aware that GDPR-compliant companies may not be fully compliant with the PDPA. Therefore, businesses should monitor the promulgation of any subordinate legislation.

While the PDPA remains partially effective (ie, until 1 June 2021), businesses should comply with the Ministry of Digital Economy and Society's Notification on Personal Data Security Standards 2020 (BE 2563), which establishes the minimum security standards that should be in place during the transition period. Even though the notification imposes no penalties for non-compliance, businesses should consider maintaining their security standards regarding data confidentiality, integrity and availability to ensure a smooth transition when the PDPA takes full effect.

*For further information on this topic please contact Chotika Lurponglukana or Ruengrit Pooprasert at Veritas Law Limited by telephone (+66 2 286 5191) or email (chotika@veritaslaw.co.th or ruengrit@veritaslaw.co.th). The Veritas Law Limited website can be accessed at www.veritaslaw.co.th.*