LAW GAZETTE

CORPORATE LAW, GLOBAL NEWS - February 2022

Thailand's New Personal Data Protection Act

10 min read
by Dr Andreas Respondek, Sutthida Norasarn and Piriya Kimsawat

Thailand's Personal Data Protection Law will become fully effective on 1 June 2022. Businesses and organisations in Thailand and abroad still have a few months to prepare themselves to become fully compliant with the requirements under the new law. Since Thailand is an increasingly important trading partner of Singapore (exports to Thailand increased to 1,714.80 SGD million last year), it is highly recommended that all Singapore entities engaging in trade with Thailand and their professional advisors ensure that any compliance gaps with the new Act can be closed within the remaining short time period.

The first version of the **Personal Data Protection Act, B.E. 2562 (2019)** (**PDPA** or **Act**) was introduced in Thailand on 27 May 2019. To ensure the protection of personal information of individuals (hereinafter referred to as a "personal data"), the PDPA introduced a number of new statutory duties, responsibilities, restrictions and above all potential fines. Currently, the PDPA is only partially effective by virtue of **the Royal Decree on the Organizations and Businesses of which Personal Data Controllers are exempted from the Personal Data Protection Act B.E. 2562 (2019), B.E. 2563 (2020) No.2**. The significant highlights of the PDPA that are important for all companies have been summarised below.

1. Definitions

To get a full grasp of the new law, it is important to start off with the most crucial definitions under the Act:

- **Data Subject:** an identifiable natural person who can be distinguished from other individuals by considering personal data relating to such person.
  For example: customer, employee, service receiver, contracting party, website user.

- **Data Controller** – a natural person or a legal person **who has decision-making authority and control** on the collection, use and disclosure of personal data. The data controller is liable for any breaches of the obligations stipulated under the PDPA. **(Section 6** [1] **)**
  For example: business enterprise, government sector, institutions, organizations, owners of business websites.

- **Data Processor** – a person or entity **who processes personal data following an order or on behalf of the data controller**. **(Section 6)**
  For example: outsourcing service providers or subcontractors, cloud service providers, market researcher, accounting companies.

- **Ministry of Digital Economy and Society (MDES)** – the Ministry in charge of all PDPA matters.

- **Personal Data Protection Committee (PDPC)** – an independent public authority empowered by the MDES responsible for issuing sub-notifications, promoting public awareness of the PDPA, monitoring, investigating, interpreting and making decisions for all PDPA cases along with handling complaints involving violations of the PDPA. Any data breach or incident shall be notified to the PDPC through the Office of the Personal Data Protection Commission (**OPDPC**).

- **Data Protection Officer (DPO)** – an expert designated by a data controller or data processor under section 41 to provide help and advise the organisation and personnel, in particular monitoring internal PDPA compliance and personal data protection activities, and likewise, to handle PDPA cases that may be addressed, and liaise with the PDPC to ensure that the organisation fulfils all the requirements in line with the PDPA.

2. The PDPA and Related Regulations

The PDPA is the governing statute for every organisation in Thailand – and eventually abroad – which wishes to process personal data for specific purposes, where the processing of the personal data must be carried out based on legitimate grounds. The Act aims to protect an individual's privacy rights as well as to provide remedies to a person who may be violated in respect of the protection rights of personal data. The PDPA determines the duties and responsibilities for all organisations and every type of business both in Thailand and overseas ("covered entities" or "data controllers"), when collecting or keeping personal data of individuals residing in Thailand ("data subjects"). The Act brings new challenges including fines and extra obligations for both local and foreign businesses that are responsible for taking actions to ensure the protection of personal data.

Meanwhile, regardless of the postponement of the PDPA's entering into force on 31 May 2022, data controllers are still required to conform with **the Notification of the Data Protection Security Standards,** [2] i.e. to follow the guidelines prescribed by MDES applicable to all data controllers to implement measures towards security standards of personal data covering administrative, technical and physical safeguards, comprising the following key aspects:

1. Implementation of adequate data access control including data storage systems and data processing devices;
2. Determination and designation of personal data access authorisations or user logon rights;
3. Implementation of user access management to allow or limit the data accessibility specifically for authorised personnel;
4. Determination of user responsibilities to prevent security violations i.e., unauthorised access or copying, disclosure, recognition, and stealing of data storage and processing devices; and
5. Arrangement of tracking monitoring systems in order to trace back an access log, amendment, removal, or transfer of personal data.

"Security" of personal data under this Notification is defined as the maintenance of confidentiality, integrity, and availability of personal data including the protection of loss, access, use, modification, or disclosure of

personal data in violation of the law. Alternative security standards could as well be adopted but they must not be lower than the standards prescribed in the Notification.

3. What is Personal Data Information under the PDPA?

"Personal Data/ Personal Information/ Personal Subject" (Section 6) means any information maintained by data controllers that can be used to distinguish, identify or trace identity of a person ("data subject") either directly or indirectly i.e., name, identification number, photo, social security number, date and place of birth, gender, home address, e-mail, phone number, taking into account any other information that is linked or linkable to an individual such as educational, current occupation and employment history, IP address, financial statement, credit card number, access card, audio recording, location data and other highly sensitive information.

Some general personal data does not require the data subject's consent if it can be predicted that such information will be kept or used according to objectives of use that the data subject was already informed of a "legitimate interest" earlier. For example, information required for opening a bank account on account of banking transactions and online banking, CCTV monitoring for the purpose of safeguarding security, individual verification for government sectors etc.

"Sensitive Personal Data" is information related to or can identify an individual person specifically such as biometrics, disabilities, medical or health record, face ID, fingerprint, device ID which is connected to a server and can identify an owner. Disclosure of some of the sensitive personal data such as race, religion, political opinion, criminal records, health data, disability, genetic data, biometric data, sexual behavior, or relationship etc. can lead to social consequences or unfair treatment, in particular negative impacts on an individual's personal life and fundamental rights and freedoms. For this reason, using all of these information details is strictly prohibited unless explicit consent is given or other purposes as stipulated in section 26 are prevailing. Data controllers and data processors must process sensitive personal data carefully to avoid any data breach.

For example, a fitness club member maybe required to give personal data such as height, weight, or body mass index for the purpose of registration and the aim for body improvement, training, and other treatments. These details could also be targeted for the purpose of beauty and weight loss advertisement or offering dietary supplements, which is not the original purposes that fitness members were informed in the first place. There may be sensitive data included with such personal data gathered i.e., allergies, health records or other underlying conditions. Hence, if the fitness center wishes to process these sensitive personal data, it must obtain first explicit consent from the members to do so.

4. Enforcement – Jurisdiction

Unless exempt from section 4 of the Act, the PDPA applies to all data controllers and data processors in Thailand and those in overseas entities who wish to collect, store, use, or disclose personal data (Section 5), i.e.:

- a natural person or a legal person residing in Thailand;
- a juristic person or an overseas business operator who offers products or services to a natural person in Thailand (all nationals);

- a legal person or a business situated outside of Thailand, as a third-party who receives cross-border data transfers from Thailand; and
- any person who monitors behavior associated with individuals in Thailand.

For any data collected prior to the effective date of this Act, data controllers may continue to collect and use such data based on the original purposes. However, the data controller must provide and publish a consent withdrawal method to facilitate data subjects who wish to revoke their consent (Section 95).

5. Legal Basis

Key aspects for personal data processing include:

- Before collecting an individual's personal data, the data controller must ask for clear consent [3] in a form of a physical document or through an electronic system that is not deceptive or misleading (Section 19).
- It is essential that data processing activities be consistent with specific purposes as the data subject is informed at the beginning.
- The collection of personal data shall be limited to the extent necessary according to lawful purposes (Section 22).
- The data controller must inform the data subject about the following details (Section 23):
    - Scope of information that is necessary to be collected, purpose of use, clarification on data processing steps, and retention period;
    - In case that personal data must be given in compliance with a law, or contract including the possible consequence if such information is not provided;
    - Persons or entities where the data controller plans to share or disclose the collected personal data to;
    - Contact details of the data controller or persons related to the data controller; and
    - The rights of the data subjects.
- In case that the data controller obtains personal information from other sources, a 30-day notification period to inform the data subjects is required (Section 25).
- Sensitive personal data is prohibited to be kept i.e., disabilities, biometrics, sexual behavior or relationship, politics opinion, religion etc., unless a consent is given explicitly (Section 26).
- For cross-border personal data transfer, the destination country or international organisation that receives personal data transferred from Thailand abroad is required to have adequate data protection standards, unless consent is given by the data subject who has been informed of such inadequate standard (Section 28).
- The data controller has various legal obligations and responsibilities under section 37 to:
    - Secure personal data with appropriate measures;
    - Prevent others from using or disclosing personal data unlawfully or without authorisation;
    - Provide an inspection data management system for the erasure and destruction of unused personal data when its retention period ends or as required by the data subject; and
    - Notify data subjects and the OPDPC of any personal data breach for further remedial measures.
- The data subject is entitled to withdraw the consent at any time.
- The data processor has a legal obligation under section 40 to:
    - Carry out the activities related to the collection, use, or disclosure of personal data pursuant to instruction given by data controller;

- Secure personal data and notify the data controller when personal data has been violated; and
- Prepare and maintain records of personal data processing activities.

The table below gives insights into the exceptions of data collection (section 24 for general personal data and section 26 for sensitive personal data) and data processing (section 27) insofar as it is necessary in terms of purpose of use and based on the grounds of a lawful or legal norm.

PDPA Legal Basis	Breach of the PDPA
• **Consent**: Data controllers require data subjects to give clear consent for a specific use of individual's personal data **Exceptions to Informed Consent** • **Scientific or historical research**: Historical documents or archives conducted for public interest or research studies, statistics, and data analysis • **Vital Interest**: To protect or stop danger to life, health or bodily harm of individuals • **Contract**: General personal data provided in order to carry out a contract agreed between parties i.e., banking, e-commerce, or subscription service • **Public Task**: A performance considered to be important to the public interest or the exercising of official authority who has a duty to act empowered by law • **Legitimate Interest**: The information that is necessary for data controllers or any other persons unless it does conflict with the fundamental rights of data subjects. i.e., organisation must submit monthly salary of its employees to the Social Security Office • **Legal Obligations**: To comply with a law. For instance, Thai post office requires a sender's ID card for verification	• Deceptive or misleading consent form that implies or lead data subjects to have a wrong understanding • Processing personal data other than specific usage activities • Processing personal data without the consent of data subject despite that such activity is related to unlawful benefit or might lead to damage of data subject (Section 79) • Lack of security standard compliance (Section 37 for data controller and Section 40 for data processor) • Disclosure of personal data discovered from performance of duties under this Act to any other person (Section 80) **Administrative Liability** • Collecting personal data without consent from other sources • Lack of maintenance records for the OPDPC's inspection • Failing to provide a DPO with supporting tools or equipment in order to facilitate his tasks • Failing to notify the impact of the consent withdrawal

6. Rights of Data Subjects

A data subject's specific rights are stipulated in detail in section 30-35 of the PDPA as follows:

6.1 Right to be Informed

To be informed, prior to or during data collection and processing, purposes of use, retention period, detail of data controller and data processor, and other important things that should be addressed including potential impacts, to be notified immediately of any breach of personal data.

6.2 Right of Access

To request for an access or a copy of personal data including a disclosure of personal data obtained without his or her consent.

6.3 Right to Data Portability

To request for personal data that can be read or used with automatic devices, and to request data controller to send or transfer personal data to other data controllers by automatic system.

6.4 Right to Object

To object a collection, utilization, publishing, and disclosure of personal data.

6.5 Right to Erasure/ Right to be Forgotten

To request for change, removal, disposal, or any action to make the personal data unidentifiable or does not match with the individual.

6.6 Right to Restrict Processing

To request a data controller to cease the use of personal data, to request of data retention for the purpose of legal claims.

6.7 Right to Rectification

To ensure that personal data is accurate, up-to-date, complete, and not misleading.

7. Liabilities

Any person, organisation or business, which is a data controller failing to comply with the PDPA will incur civil, criminal, or administrative penalties as listed below.

7.1 Civil Liability

If the data controller or the data processor fails to comply with the PDPA, which causes damages to the data subject, he/they shall be subject to **a compensation plus punitive damages up to twice the amount of actual losses and damages**. Except that it could be proved that it is (1) a force majeure event, or the data subject's own act; or (2) an action taken pursuant to an order of a government official when exercising duties and power under the law (section 77 and section 78).

The limitation period for a compensation claim on grounds of wrongful acts against the Personal Data Protection Act shall be three years from the date that the data subject becomes aware of damages and the identity of the data controller or the data processor, or after 10 years from the date of the incident which caused such damages.

7.2 Criminal Liability

Without being granted consent, offenses against the personal data protection obligations in a way that could cause any damages to the data subject or his/her reputation, or exposing such person to be hated or humiliated, the data controller shall be subject to punishment with imprisonment not exceeding six months and/or a fine up to THB 500,000.

Aiming to unlawfully benefit him-/herself or a third party, shall be subject to punishment with imprisonment not exceeding one year and/or a fine up to THB 1,000,000 (section 79). In addition, the offences under this section are compoundable offenses.

In case of a juristic person, its directors could be punished with imprisonment (Section 81).

7.3 Administrative Liability

Failing to inform the data subject regarding data collection, purposes and related matters, rejecting the rights of access, without granting consent, lack of preparation of records pursuant to the Act, failing to appoint a DPO or providing support thereof shall be punished with a fine up to THB 1,000,000.

Data collection, use, or disclosure without legal grounds, illegal international data transfer, failing to inform additional purpose or data breach, obtaining consent by deceiving or misleading the data subject, lack of adequate security standard, or failing to appoint domestic representative shall be punished with a fine up to THB 3,000,000. Unlawful processing of sensitive personal data is punishable with a fine of up to THB 5,000,000 (Section 82-89).

Within the framework of PDPA exemptions for 22 types of organisations and businesses by virtue of the Royal Decree No. 2, if there is any use or disclosure of personal data and/or sensitive personal data causing damages to an individual, such data subject shall be entitled to exercising their rights under the Civil Law for filing a claim for compensation on the basis of a wrongful act according to section 420 of the Thailand Civil and Commercial Code.

Endnotes

1 Unless specifically mentioned, all Section quotations refer to the PDPA

2 Notification of the Ministry of Digital Economy and Society, RE: Personal Data Security Standards B.E. 2563 (2020), effective from 18 July 2020 until 31 May 2020, and No.2 with the amendment of enforcement to be effective as from 25 May 2021 until 31 May 2022.

3 GDPR Art. 7 – Freely given, specific, informed and unambiguous by a statement or by a clear affirmative action.

Tags: EDITOR'S PICK, PERSONAL DATA

Dr Andreas Respondek
Attorney at Law (USA)
Rechtsanwalt (D)
Chartered Arbitrator (FCIArb)
Respondek & Fan Pte Ltd
E-mail: respondek@rflegal.com

Sutthida Norasarn
Respondek & Fan Ltd

Piriya Kimsawat
Attorney at Law (Thailand)