Chapter 13

PERSONAL DATA PROTECTION

CHAPTER 13 | PERSONAL DATA PROTECTION

This chapter will discuss and provide basic background information on the Personal Data Protection Act, B.E. 2562 (2019) (the "**PDPA**"), which was due to come into full effect in May 2020. However, the Royal Decree on the Organizations and Businesses of which Personal Data Controllers are Exempted from the Applicability of the Personal Data Protection Act, B.E. 2562 (2019), B.E. 2563 (2020) and its amendment (the "**Royal Decree**"), were issued to postpone the enforcement until 31 May 2022. During the postponement period, the main provisions of the PDPA including Chapter 2 (Personal Data Protection), Chapter 3 (Use or Disclosure of Personal Data), and Chapter 7 (Punishment) will not be enforced with all Personal Data Controllers in 19 business industries and three groups of organizations. Those business industries and organizations cover most types of businesses in Thailand, government agencies, foreign government agencies and international organizations, foundations, associations, religious organizations, and non-profits organizations. The PDPA is expected to be fully enforced for all Personal Data Controllers on 1 June 2022. Legally speaking, this Royal Decree does not provide postponement of enforcement for Personal Data Processors. Therefore, Personal Data Processors should perform their duties and obligations as prescribed in PDPA, such as providing security measures for prevention of loss of Personal Data.

(1) Overview of Historical Practices and Legislation

Protection of personal data and privacy has long been a heated topic in Thailand. Personal data that is commercially useful is often gathered, processed, stored, sold, and transferred without justification, knowledge, or consent of the person who owns such data. This legally unsupported use of data covers the most basic of commercially usable data such as names and phone numbers, to other more sensitive data such as health information. Most breaches were committed when commercializing data to, for example, enable cold calls or to facilitate targeted marketing or general market analysis, but some breaches were committed without any malfeasant intentions, such as useless and perpetual storage of personal data. In the past, any breach of personal data would rely on tort law in the Thai Civil and Commercial Code, which contains a catch-all provision that prohibits and penalizes wrongful acts in general. In this sense, a breach involving personal data, whether protection or privacy, has been treated as a simple tort.

Due to the nature of the law, the vast majority of people would simply not pursue a claim because any pursuit is time-consuming (both inside and outside of a court), costly (cost of court case-filing fees and lawyer fees), and the possible benefits to be reaped from the justice system would be very minimal and far outweighed by the costs as the Thai justice system only affords actual damages to cases of tort. The practical implication of this has been the enabling of the private sector and government to continue using people's data without any fear of repercussions. However, the PDPA will bring significant changes to such domestic practices. The PDPA, which is mainly based on the General Data Protection Regulation of the European Union (the "**GDPR**"), will create obligations on the private sector and government (both Personal Data Controllers and Personal Data Processors), especially on burden of proof. The private sector and government must prove that they meet the requirements under the PDPA for all types of treatment of personal data. The PDPA will establish a supervising authority (i.e., the Personal Data Protection Commission (the "**PDPC**") and the Office of the PDPC) to regulate operators.

(2) Current Legislation

The PDPA was enacted on 27 May 2019. A one-year transition period was granted to the private sector and government to prepare themselves to comply with the key provisions of the PDPA. Even though two Royal Decrees were announced in 2021 to postpone the enforcement of the main provisions in

PDPA for the Personal Data Controllers in certain business industries and organizations, the PDPA's effectiveness for Personal Data Controllers are still in force. Personal Data Controllers are required to provide data security measures as prescribed by the Ministry of Digital Economy and Society (the "**MDES**") (i.e., access control measure) during the postponement period. Under the PDPA, several subordinate laws are being prepared although none has been issued by the time of this book's publication.

On February and June 2021, the Office of the PDPC arranged unofficial public hearing sessions for subordinate laws, including rules and procedures for obtaining consent from data subjects, appropriate measures for the processing of sensitive data, rules and protective policies for the transfer of personal data outside of Thailand, preparation of records for processing personal data, security measures for processing of personal data, criteria regarding the type or size of Personal Data Controllers or amount of data processed that is required to appoint a data protection officer, the qualifications of data protection officers, etc.

A. Applicability

As a general principle, the PDPA will apply to both the private and government sectors (except for certain organizations specified in the PDPA) that deal in any way with data of natural persons. The PDPA, however, will not apply to six types of data treatment, as follows:

(i) collection, use, or disclosure of personal data of persons who collect personal data for personal benefits or for their family activities;
(ii) operations of government agencies having a duty to preserve state security, including fiscal security or public security, as well as duties relating to anti-money laundering, forensic science, or cyber security;
(iii) actions of persons or juristic persons who use or disclose personal data collected specifically for mass communications activities, artwork, or literary work in accordance with the professional code of conduct or for the public interest;
(iv) actions of the House of Representatives, the Senate, and the Parliament, including commissions appointed by these bodies, which collect, use, or disclose personal data for the purpose of making deliberations under their duties and powers;
(v) consideration of the courts and performance by officers in legal proceedings, legal execution, and deposits of property, including implementation of the criminal judicial processes; and
(vi) actions of the National Credit Bureau Company Limited and its members under the law on operation of credit information businesses.

B. Regulations

Broadly speaking, the PDPA provides for three main areas of regulations: (i) the basis under which personal data is processed and treated; (ii) rights of a data subject; and (iii) security measures.

Under the PDPA, there are three main definitions, as follows:

- "**Personal Data**" means any data which, by itself or in combination with other data, can be used to trace back to an individual, meaning virtually all and each piece of personal data is "Personal Data" as recognized by the PDPA;
- "**Personal Data Controller**" means any entity which has the power to decide how to treat Personal Data; and
- "**Personal Data Processor**" means any entity which treats Personal Data pursuant to instructions of the Personal Data Controller.

(i) Basis of Treatment

The PDPA dissects Personal Data into two types: (i) ordinary data (such as names, addresses, phone numbers, email addresses, etc.); and (ii) sensitive data (ethnicity, race, philosophical beliefs, religious beliefs, socio-political beliefs and affiliations, relationships with labor unions, criminal records, diseases and medical conditions, biometrics and DNA, sexual preference, etc.), both of which may be treated under different sets of bases.

Like other data protection regulations in other countries, the PDPA provides for a set of lawful bases under which treatment of ordinary data can occur, which are as follows:

1) via consent of the data subjects;
2) for the achievement of purposes relating to preparation of historical documents or archives in the public interest or relating to study, research, or statistics for which an appropriate protection standard is used to protect the rights and liberties of the data subjects as prescribed and announced by the PDPC;
3) for prevention of danger to life, body, or health of persons;
4) for performance under a contract to which the data subject is a party, or for proceedings with the data subject's request before entering into such contracts;
5) for performance of a Personal Data Controller's duty for the public interest or as required by the state;
6) under a legitimate interest of a Personal Data Controller, another person or juristic person, unless such interest is less important than the basic rights in the Personal Data of the data subject; and
7) for Personal Data Controller's compliance with law.

From the list, the four most important and often used lawful bases to process personal data are: (i) consent; (ii) contractual performance; (iii) legitimate interests; and (iv) compliance with laws. Additional explanations for items (i) – (iii) are as follows:

a. Consent

Consent in general must be clear and in written, electronic, or other unequivocal manners, and different objectives should be separated to ease understanding of the data subjects. Consent must also provide other information to allow the data subjects to carefully consider whether their consent should be given to the Personal Data Controller, such as rights of data subjects, contact information, retention period, etc. Note that consent must not be lumped in with information gathered via a contractual performance basis.

b. Contractual Performance / Entering into a Contract

The most important principle to remember is that all items of Personal Data given under this basis must be absolutely necessary for the performance of a contract / entering into a contract. If a piece of data is not needed for performance of / entering into a contract, then it cannot be lumped into this basis and must, by itself, find its own basis.

c. Legitimate Interests

Legitimate interests of the Personal Data Controller must always be weighed against fundamental rights of the data subjects over such Personal Data. There is no official guideline under the PDPA as to a mechanism for weighing such interests, or to what extent

a Personal Data Controller can trust their own judgment. Therefore, it is recommended that the surrounding circumstances for a single use of data under this basis be thoroughly considered before an operator decides to proceed with this treatment. Any miscalculation will mean treatment of data without a proper lawful basis, rendering the operator liable to penalties under the PDPA.

Like other data protection regulations in other countries, the PDPA provides for a set of bases under which treatment of sensitive data can occur. These bases, although different from bases for ordinary data, have, in large part, been derived from the same fundamentals. The bases are as follows:

1) via express consent of the data subjects;
2) for prevention of danger to life, body or health of persons, for which the data subject cannot give his/her consent;
3) for conducting legitimate activities with appropriate protections by a foundation, association, or non-profit organization having a purpose relating to politics, religion, philosophy or a labor union for its members, former members, or persons with regular contact with the entity, without disclosure of such Personal Data outside the entity;
4) if sensitive data has already been disclosed to the public with the express consent of the data subject;
5) under necessity to establish a right of claim under law, comply with or exercise a legal right of claim, or raise as defense for a legal right of claim; and
6) under necessity to comply with laws to ensure achievement of the purposes relating to public health, occupational health, social security, scientific study, etc.

Treatment of sensitive Personal Data by commercial operators will most likely come via express consent, with that basis being the most common in day-to-day operations.

(ii) Rights of Data Subjects

The PDPA provides for an extensive list of rights of data subjects, many of which can be universally invoked while others can be used under certain circumstances. The rights are as follows:

1) to have access to the stored Personal Data;
2) to ask for usable copies of the Personal Data;
3) to ask for disclosure of how Personal Data has come to be collected;
4) to object to the collection, use, and disclosure of Personal Data;
5) to request for the deletion or destruction of Personal Data in storage of the Personal Data Controller;
6) to ask for suspension of the collection, use, and disclosure of Personal Data; and
7) to revoke any consent previously given to the Personal Data Controller.

The rights outlined above are not always absolute, as the Personal Data Controller may have ability to argue against such requests, depending on specific facts of such case, such as:

1) there is on-going contractual performance, and such request may obstruct such performance;
2) the law stipulates otherwise, that the Personal Data Controller must continue such treatment of data; and

3) the Personal Data Controller has legitimate interests that outweighs the fundamental rights of the data subjects over such Personal Data.

(iii) Security Measures

The PDPA provides a blanket requirement to both Personal Data Controllers and Personal Data Processors to treat Personal Data in appropriate manners, which materially include well-organized safe keeping of data, safe storage (physical and electronic), automatic deletion of data, etc. Although safety is of the utmost concern, the PDPA itself does not provide any specific guidelines, and currently there are no details of what characteristics safe storage must have. However, based on discussions within the industry, operators must abide by at least the prevailing industrial standards used by most entities in the industry, such standards must be appropriate in terms of cost and utility and fit the type of data the operator is possessing, and the operator's general and financial position and threat of loss and leakage of data in its possession. It has also been suggested that pseudonymization and anonymization will, in any case, afford additional protection against and safety from unintended and intentional leakage.

After the Royal Decree came to force, the MDES issued a notification in the Government Gazette prescribing minimum data security standards (i.e., administrative safeguards, technical safeguards, and physical safeguards for access control) for personal data under the PDPA. The notification is effective during the extended transition period (i.e., within 31 May 2022). The summary of data security standards under this notification are as follows:

1) access control must be implemented over personal data, and devices for processing personal data;
2) the operator must provide a system for designation of permission and access rights over personal data;
3) user access management must be in place to control access to personal data, thus it can be accessed by authorized persons only;
4) there must be a system for designation of user responsibilities to prevent unauthorized data processing activities; and
5) the monitoring records relating to past access, alteration, deletion, or transfer of personal data should be implemented.

In addition, Personal Data Controllers must communicate with their personnel, employees, and relevant persons about the above security measures and build awareness of the necessity of personal data protection.

(3) Penalties for Violations under the PDPA

A. Civil Breach

A damaged data subject may bring a civil suit against a Personal Data Controller and/or Personal Data Processor who has/have wronged him/her. The PDPA expressly allows the court to award punitive damages, which is generally rare in Thailand, and which shall not exceed two times the actual damages, in case the court believes the breach is severe.

B. Criminal Breach

Regardless of the civil case as outlined above, the authority may pursue a criminal case against any commercial operator who has breached the PDPA.

Any use or disclosure of sensitive data without consent and which has caused damage to the data subject carries penalties of imprisonment of up to six months or a fine of up to Baht 500,000, or both. However, any use or disclosure, if undertaken for undue benefit of the commercial operator, will double the above-stated maximum imprisonment duration and fine amount.

C. Administrative Breach

Regardless of a civil case as outlined above, the authority may pursue an administrative case against any commercial operator who has undertaken a wrongful act under the PDPA. Besides the criminal provisions as outlined above, any other breach of the PDPA will bring penalties in term of administrative fines of up to Baht 5,000,000 for the most serious of the breaches.

(4) Data Protection Officer

The PDPA recognizes that there may be a need for many organizations to have a data protection officer, or multiple in the case of high complexity or a large volume of work. This position, although existing under the PDPA, is not yet mandatory as there is no supplementary regulation to provide guidelines as to what kind of commercial operators (or other types of entities) need to have a data protection officer. The supplementary regulation is expected that possession of certain characteristics may require organizations to have a data protection officer, such as routine dealing with sensitive data, and dealing with large-scale processing of Personal Data. According to an unofficial public hearing on the first set of supplementary regulations under the PDPA held by the Office of the Permanent Secretary of the Ministry of Digital Economy and Society during 15 – 18 February 2021, large-scale processing may include the processing of Personal Data of 50,000 data subjects or sensitive data of 5,000 data subjects during any 12-month period.

In line with other jurisdictions, data protection officers must be independent and will report directly to the top of the management in each organization, thus reducing structural inefficiencies that may result in mistreatment of or delayed performance over personal data. The data protection officer is also at the front line to deal with any leakage or mistreatment, complaints from data subjects, and liaise with the state officers.

Co-authors:
Jutharat Anuktanakul, Partner – jutharat.a@mhm-global.com
Koonlacha Charungkit-anant, Partner – koonlacha.c@mhm-global.com
Pranat Laohapairoj, Partner – pranat.l@mhm-global.com
Suphakorn Chueabunchai, Associate – suphakorn.c@mhm-global.com
Theerapat Sombatsatapornkul, Associate – theerapat.s@mhm-global.com