DATA PROTECTION LAWS OF THE WORLD

Thailand

THAILAND

Last modified 5 January 2024

LAW

On 28 May 2019, the Personal Data Protection Act ("**PDPA**") became law in Thailand. There was an original one–year grace period for the formation of the Personal Data Protection Committee and the issuance of subordinate regulations, as well as for organisations to become compliant with the PDPA. However, on 21 May 2020, the Royal Decree Establishing Organisations and Businesses that the Personal Data Controllers are Exempted from the Applicability of the PDPA B.E. 2563 (2020) ("**Royal Decree**") was published in the Royal Gazette, which effectively extended the implementation of the key provisions of the PDPA until 31 May 2021. On 8 May 2021, an amendment to the Royal Decree was published in the Royal Gazette (Royal Decree No. 2), which postpone the full enforcement of the PDPA for another year. The PDPA then came into full force on 1 June 2022.

In January 2022, the Personal Data Protection Committee was established. Various public hearings on the subordinate regulations have been held. A few of these subordinate regulations have been published, while some are undergoing a public hearing process.

Key principles under the PDPA are highly influenced by the EU General Data Protection Regulation (often referred to as GDPR) regime, but with some key local differences. The PDPA acknowledges individual data subjects' right to control how their personal data is collected, stored, processed, and disseminated by data controllers, provides lawful bases for the processing of personal data, as well as prescribes the duties and responsibilities of data controllers and processors. Whilst Thailand has adapted several concepts from the GDPR, there are still some unique national perspectives in the provisions of privacy notice and data subject rights, notably as regards consent. The data protection obligations under the PDPA generally apply to all organisations that collect, use, or disclose personal data in Thailand or of Thai residents, regardless of whether they are formed or recognised under Thai law, and whether they are residents or have a business presence in Thailand. This extraterritorial scope of the PDPA represents a significant expansion of Thailand's data protection obligations to cover all processing activities relating to Thailand–based data subjects.

Data controllers are permitted to continue to process personal data collected before 1 June 2022 if the purpose for which the personal data was collected remains the same. However, data controllers must publicise a consent withdrawal method and notify the data subjects of the same so that data subjects have the option to withdraw their consent / opt–out. However, if a data controller uses or discloses personal data beyond the original purpose for which the data subjects had previously given consent, further specific consent is required for each separate purpose.

DEFINITIONS

Data Controller is defined as "*a person or juristic person who determines the purposes for which and the manner in which any personal data are, or are to be processed.*" Data Controllers have primary responsibility for ensuring that processing activities are compliant with the PDPA.

Data Processor is defined as "*a person or an entity that collects, uses, or discloses personal data on behalf of, or in accordance with, the instructions of a Data Controller.*" Data Processors have direct liability under the PDPA in areas such as (this is not exhaustive) data security, data transfer and record keeping.

Personal Data is defined as "*any data pertaining to a person that enables the identification of that person, whether directly or indirectly, but specifically excluding data of the deceased*."

Sensitive Personal Data is defined as "*personal data relating to a person’s race, ethnicity, political opinion, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health, disability, labour union, genetics, biometric or any data which may affect the data subject in the same way as prescribed by the Regulator*." The PDPA requires Sensitive Personal Data to be handled carefully. We expect the Personal Data Protection Committee to provide further guidance on this in due course.

Personal Data Breach is defined as “*a breach of security measures which causes loss, accessibility, usage, alteration, modification, or disclosure of personal data without authorization or unlawfully, whether or not by intention, deliberation, negligence, unauthorized or unlawful acts, a commission of computer offenses, cyber threats, errors or accidents, or any other causes*.”

NATIONAL DATA PROTECTION AUTHORITY

The Personal Data Protection Committee ("**Regulator**") has been established to supervise compliance with the PDPA, under the supervision of the Minister of Digital Economy and Society.

REGISTRATION

The PDPA does not require any registration of Data Controllers, Data Processors or data processing activities. This may change when subordinate laws are enacted.

DATA PROTECTION OFFICERS

Data Controllers and Data Processors are only required to appoint a data protection officer (DPO) if it qualifies as any of the following:

- is a public authority as prescribed and announced by the Regulator;
- requires regular monitoring of Personal Data or system due to the collection, use or disclosure of large amount of Personal Data as prescribed by the Regulator; or
- the core activity of the Data Controller or the Data Processor involves the collection, use, or disclosure of Sensitive Personal Data.

The relevant subordinate regulation was issued on 14 September 2023. It sets out criteria of the core activities of Data Controllers and Data Processors that require ‘regular monitoring’ and indicates factors to be considered in determining a ‘large amount’ of Personal Data. For example, if the core activities consist of tracking, monitoring, analysing, or profiling of personal behaviour or characteristics, and generally involve the processing of Personal Data in a systematic manner and on a regular basis, such core activities require ‘regular monitoring’. If the processing of Personal Data is of 100,000 data subjects or more, or for behavioural advertising purpose via search engine or social media, or by insurance company, financial institution, or licensed telecommunications operator, such processing is considered the processing of ‘large amount’ of Personal Data.

COLLECTION & PROCESSING

Legal bases for collection and processing

The collection, use or disclosure of Personal Data requires consent of the data subject unless other legal bases for processing apply. These include, among other things, the performance of contract or legal obligations, or by legitimate interest of the Data Controller. The legal bases of processing Personal Data and Sensitive Personal Data are different. Due to the sensitive nature of Sensitive Personal Data, explicit consent is required for its collection, use and disclosure without relying on the other legal bases set out in the PDPA (such as vital interest, public health interest and preventive medicine where consent cannot be obtained).

The request for consent must be: (i) explicitly made in writing or via electronic means; (ii) clearly separated from other messages; (iii) delivered in a format which is easily accessible and understandable using language that is easy to understand; and (iv) the message should not be misleading or cause data subjects to misunderstand the purpose of collection. The Data Controller

must also ensure that the consent is freely given and not conditional on entering into a contract. The Regulator can "*require the Data Controllers to request consent from the data subject in accordance with the form and statement prescribed by the Committee*". However, in practice, requiring compliance through a prescribed form may prove challenging, given that Data Controllers may develop their own mechanisms for gaining and assessing consent.

In addition to the above consent requirement, the official guideline on data subject consent issued by the Regulator further prescribed that the consent given by the data subject must indicate a clear affirmative action that the data subject consents to the specific purposes. The examples given under the guideline include data subjects clicking the checkbox, double clicking screen, or screen swiping to affirm their intention to give consent.

Data subjects also have the right to refuse to consent, and the right to withdraw any consent they have given, at any time. Following any such refusal or withdrawal of consent, Data Controllers should be wary of proceeding with the proposed data processing activity.

Notice

Data Controllers must give notice to the data subjects that Personal Data or Sensitive Personal Data is being collected, prior to or at the time of collection, regardless of whether consent or other legal bases of processing apply. The privacy notice must contain particulars prescribed by the PDPA, including categories of persons or entities to whom the collected Personal Data may be disclosed to and the purpose of collection.

The official guideline on privacy notice issued by the Regulator further prescribes that the privacy notice may be given by electronic means, such as a URL link or QR code, and that the language used in a privacy notice should be clear and easily understandable.

TRANSFER

The Data Controller may not use or disclose Personal Data without consent unless it has been exempted from the consent requirement (i.e. on the grounds of other legal bases of processing). The recipient of the Personal Data must not disclose the Personal Data for any other purposes other than as previously notified to the Data Controller when requesting for the Personal Data.

In the event that the Data Controller uses or discloses Personal Data which is exempt from the consent requirement (i.e. other legal basis of processing), the Data Controller must maintain a record of such use or disclosure in the manner prescribed under the PDPA, for example the record must be kept in a written or electronic format.

Processing between Data Controllers and Data Processors

As the Data Processor will be carrying out activities only pursuant to the instructions given by the Data Controller, the PDPA imposes an obligation on the Data Controller to ensure that there is a data processing agreement in place between the Data Controller and Data Processor governing the activities of the Data Processor.

Cross-Border Transfer

Personal Data may not be transferred outside of Thailand, unless the recipient country or international organisation has adequate personal data protection standards in the Regulator’s view and the transfer is in accordance with the rules prescribed by the Regulator. Exemptions may apply such as in the following cases:

- the data subject has given consent and proper notification has been given by the Data Controller;
- the transfer is necessary for the performance of a contract between the Data Controller and data subject; or
- the transfer is necessary in order to protect the vital interests of the data subject.

According to the subordinate regulation regarding the criteria for protecting Personal Data sent or transferred abroad issued on 25 December 2023, the cross-border transfer rules do not apply to the sending and receiving of Personal Data as an intermediary for data transit or data storage that has technical measures to protect unauthorized access from third parties, such as cloud computing services.

As the relevant subordinate regulations have already been issued, the Regulator may soon issue the list of destination or data receiving countries which are considered to have adequate personal data protection standards pursuant to the PDPA.

Transfer between group companies may be exempt from the above requirement if the international transfer is to an organisation within the same group / affiliated business and such transfer is for joint business operations. Nevertheless, the personal data protection policy of such group companies or so called the binding corporate rules (BCR) must be approved by the Regulator. The relevant Data Controller or Data Processor may submit the BCR to the Regulator for approval via post or electronic channel as prescribed by the Regulator.

However, in the absence of a BCR or a decision on the adequate personal data protection standards of the destination country, the Data Controller or Data Processor may transfer Personal Data to another country if it provides appropriate measures as prescribed by the subordinate regulation. Such measures must, for instance, be legally enforceable and binding on all relevant parties, uphold the data subject rights and complaint, and implement the security measures as prescribed by the PDPA.

The subordinate regulation further prescribes that the appropriate measures may be in the form of contract, certification, or provisions in the bill, or binding agreement between Thai and international governmental bodies.

In addition, the subordinate regulation stipulates that the appropriate measure in a form of contract must have either of the following characters:

1. the contract must rely on the international form of contract i.e. ASEAN Model Contractual Clauses for Cross Border Data Flow, Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to the European Union regulation or GDPR, or the standard contractual clauses for sending or transferring of Personal Data of other international organisation as prescribed by the Regulator; or
2. the contract must contain some provisions as prescribed by the Regulator. For example, in case of contract between the Data Controller and Data Controller, the receiving party must inform the transferring party of data breach incident within 72 hours upon becoming aware; or in case of contract between the Data Controller and Data Processor, the receiving party must contact the transferring party if there is any data subject’s right request, and it must delete the Personal Data obtained as requested by the transferring party.

The transfer requirements may have an impact on multinational organisations that routinely transfer data cross border. However, given that many organisations in Europe will already comply with similar (and likely more stringent) data protection laws, the impact of the PDPA may be limited regarding cross–border transfer of data.

SECURITY

Under the PDPA, Data Controllers are required to have appropriate security measures to protect the stored Personal Data against loss, unauthorized and unlawful access, use, alteration, edit or disclosure. Such security measures must be subject to periodic review.

Notification of the Regulator on Security Measures of Data Controller B.E. 2565 (2022), a subordinate regulation under the PDPA, further prescribed that those appropriate security measures shall include organizational measures, technical measures, and physical measures. Examples of security measures include access controls, user access management, user responsibilities, and audit traits.

Data Controllers (and Data Processors) under the PDPA are also now required under the said subordinate regulation to notify staff, employees and / or any relevant persons of the security measures in order to raise awareness of the importance of personal data protection and encourage strict compliance.

BREACH NOTIFICATION

General provisions of the PDPA provide that, in the event of a Personal Data Breach, Data Controllers must report the breach to the Regulator without undue delay, and in any event, if feasible, within 72 hours of becoming aware of it. Data Controllers also have an obligation to notify the data subjects of the breach and the remedial measures if the breach is likely to result in high risks to the rights and freedoms of individuals.

Notification of the Regulator on Rules and Methods of Personal Data Breach Notification B.E. 2565 (2022), a subordinate regulation under the PDPA, prescribed a general procedure upon the Data Controller who is being informed, or becomes aware of actual or potential Personal Data Breach, which includes the following:

- To conduct an initial investigation concerning the Personal Data Breach, to confirm that there is actually a breach and assess the risk that may affect the rights and freedoms of individuals.
- If there is a high risk that the Personal Data Breach may affect the rights and freedoms of individuals, the Data Controller shall take action to prevent, suppress, or rectify in order to stop the breach from causing additional impacts.
- If there is reasonable ground to believe that there was a Personal Data Breach, the Data Controller shall notify the Regulator of the said breach without undue delay, and where feasible, within 72 hours of becoming aware of such breach.
- If Personal Data Breach has a high risk where it may affect the rights and freedoms of individuals, the Data Controller shall notify the affected data subject of the breach, together with the remedial measures taken. Such notification to the data subject shall be given without undue delay.
- Reviewing security measures or taking any other necessary and suitable measures to stop, respond, rectify, or rehabilitate the current situation, and prevent the impacts of a Personal Data Breach of the same nature from arising in the future.

The breach notification given to the Regulator shall be in written or electronic form (or other methods prescribed by the Regulator) and shall include details such as brief information regarding the nature and category of personal data involved in the Personal Data Breach, Data Controller or DPO contact information, information relating to the impacts that may arise, and measures that the Data Controller uses, or will use to prevent, stop, or rectify the Personal Data Breach.

Where the Data Controller fails to notify the Regulator within 72 hours, the Data Controller shall be subjected to an administrative fine (not exceeding THB 3 million). In this regard, the Data Controller may request to be exempted from the liability for the delayed notification of a Personal Data Breach, by clarifying the reasons and the showing that the delay was caused by unavoidable necessities. Such request must be made to the Regulator, not exceeding 15 days of becoming aware of the breach.

Additionally, if the Data Controller views that the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of individuals, the Data Controller may request to be exempted from the breach notification requirement (i.e. to be exempted from notifying the Regulator in accordance with the list of information). In doing so, the Data Controller must provide the Regulator with information, documents, or evidence to support such a request.

ENFORCEMENT

Since the PDPA has fully come into force, there has been approximately 354 cases of complaints and 382 reports of data breach incidents submitted to the Regulator. While 80 administrative orders have been issued, the details of the cases and orders are not publicly available.

There are three types of penalties under the PDPA — civil, criminal and administrative penalties. The amount of penalty will depend on the offence committed. The maximum administrative fine is THB 5,000,000. Punitive damages may also be awarded by the court but this is limited to twice the amount of actual compensation. In the event that the offender is a juristic person, the director, manager or the responsible person may also be criminally liable under the PDPA if the relevant offence(s) resulted from such person's order, action or omission. It is unclear at this early stage what direction the Regulator will take in terms of actual enforcement.

Data Processors who do not comply with their obligations are liable to an administrative fine under the PDPA. There may also be liability under tort law.

Additionally, the Regulator has issued a subordinate regulation under the PDPA, the Notification of the Regulator on the Criteria for Considering the Issuance of Administrative Fine Order by the Expert Committee B.E. 2565 (2022), under which the severity of the violation or failure to comply with the PDPA shall be determined based on the details of the offense (intentional or gross negligence), the size of the Data Controller or Data Processor’s business, the value of damage and severity caused by such wrongdoing, etc. Based on such severity, the expert committee may give notice and order amendment, or impose an administrative fine on the Data Controller or Data Processor.

Exemption from Enforcement of Certain Provisions of the PDPA

The Royal Decree issued on 17 August 2023 exempts certain obligations of Data Controllers under the PDPA in respect of the processing of Personal Data by the listed authorities, such as the National Anti-Corruption Commission, Department of Revenue, Customs Department, Excise Department. However, the exempted Data Controllers must still provide security measures as prescribed by the Regulator to ensure that the exemption does not unreasonably affect the personal data protection principle.

ELECTRONIC MARKETING

Under the PDPA, data subjects have the right to object to direct marketing (whether or not electronic). Therefore, Data Controllers must ensure that there is an opt–out function implemented throughout the entire processing period.

ONLINE PRIVACY

General rules of the PDPA apply to online privacy.

KEY CONTACTS

Samata Masagee
Partner
T +66 2 686 8520
samata.masagee@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.