THAILAND

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 for another one year – until 1 June 2021.

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 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 resident 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 2021 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 Regulator to provide further guidance on this in due course.

NATIONAL DATA PROTECTION AUTHORITY

The Personal Data Protection Committee ("Regulator") is in the process of being 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.

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 others 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 Regulator is expected to provide guidance on the scope of consent and exemptions once established.

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.

Data subjects 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.
**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.

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 must be approved by the Regulator.

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, misuse, alteration, edit or disclosure by means of unlawful access. Such security measures must be subject to periodic review.

Nevertheless, whilst there is no penalty being enforced at this stage, all Data Controllers (and Data Processors) are now required to have in place personal data security measures in accordance with the standard prescribed by the Ministry of Digital Economy and Society set out under the Notification of the Ministry of Digital Economy and Society Re: Personal Data Security Standards B.E. 2563 (2020) ("Notification") which was released by the Thai Ministry of Digital Economy for Society and became effective on 18 July 2020.

The Notification sets out minimum standards for the personal data security measures covering administrative safeguard measures, technical safeguard measures, and physical safeguard measures in respect of the access to, or controlling the use of, Personal Data ("Measures"). Examples of Measures include access control of Personal Data, as well as the procurement of equipment used for the collection; and processing of Personal Data needs to take into consideration usage, safety and security. User access management protocols must be put in place to control and limit the access of Personal Data to only permitted personnel.

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

**BREACH NOTIFICATION**

In the event of a data breach, Data Controllers must report the breach to the Regulator without undue delay, and in any event 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.

**ENFORCEMENT**

It is expected that, prior to 1 June 2021, the Regulator will issue guidelines to assist Data Controllers’ compliance plans. In the meantime, to ensure compliance with the data protection law, public organisations and business operators should start to comply with the PDPA by evaluating the level of data protection measures adopted by its organisation against the standards of the PDPA, and ensure that the necessary documentation required by the PDPA are prepared.

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.

**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

Nahsinee Luengrattanakorn  
Associate  
T +66 2 686 8534  
nahsinee.luengrattanakorn@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.
Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2021 DLA Piper. All rights reserved.