Data. Protection. Adding Value.

Data Protection Laws - Thailand

Legislation

Thailand's **Personal Data Protection Act B.E. 2562 (2019)** ("**PDPA**") sets out comprehensive rules governing the collection, use, and disclosure of personal data within the country, and introduces specific conditions for the international transfer of such data. PDPA came into effect on 1 June 2022. From this date, all businesses and organisations operating in Thailand will be required to comply with its requirements.

Risk Level: High

Scope: The PDPA has both territorial and extraterritorial jurisdiction. This means that the PDPA not only applies to business operators established in Thailand, but also to business operators established overseas when they offer products or services to data subjects in Thailand with or without any payment or monitoring of the data subjects' behaviour in Thailand.

Exemptions: PDPA shall not be applied, such as an activity for personal or family affairs or activities operated by the relevant authorities for national security or financial security, mass media or public interest, etc. PDPA also rules that some organisations may be exempt from certain obligations under the PDPA by promulgation in the form of a royal decree.

Enforcement

Civil Penalty: Under Thailand's PDPA, a data subject harmed by a wilful or negligent breach may claim actual compensation unless the damage was caused by force majeure, the data subject's own actions, or lawful official orders.

The court has discretion to sentence the data controller or data processor to pay punitive damages to the data subjects in addition to the actual compensation.

Criminal Penalty: Unauthorised use or disclosure of personal data can result in up to 6 months' imprisonment or a fine of up to 500,000 Baht, or both. If done for personal gain, penalties increase to up to 1 year's imprisonment or a fine of up to 1,000,000 Baht, or both.

Administrative Penalty: It may apply to the data controller or data processor violating the PDPA's provisions. Administrative penalty can be in a form of a monetary fine up to 5 million Baht.

Data Processing

For each personal data processing activity (e.g. collection, use, disclosure), the data controller must have a lawful basis. The below common lawful bases are categorised by type of personal data.

General personal data

- Legal obligations;
- Contract;
- Legitimate interests; or
- Consent

Sensitive personal data

- Legal obligations for the purpose of preventive medicine, occupational medicine, public health, labour protection, social security, research, or vital public interest, by providing the suitable measures to secure fundamental rights;
- Establishing legal claims;
- Explicit consent; or
- Vital interests

Other restrictions on processing: For processing the personal data of minors under 10 years old, parental consent is always required. For minors aged 10 to under 20, parental consent is generally not required in all cases, but is necessary if the minor is not legally sui juris (for example, not married or lacking legal capacity).

Supervisory Authority

Supervisory Authority: The Personal Data Protection Committee (the "PDPC") is the main supervisory authority that enforces the PDPA. The PDPC's main responsibility and authority is to issue subordinate regulations under the PDPA. This includes inspections and monitoring all businesses and organizations by issuing the announcements and orders in compliance with the PDPA.

Registration/Approval Requirements: No, data controller and data processor are not required to register or notify the PDPC for processing of personal data. However, the data controller has the duty to notify the PDPC of any personal data breach without delay within 72 hours of becoming aware of the breach.

Principles

PDPA is founded on several key principles designed to protect the rights and privacy of data subjects regarding their personal data. The main principles include:

Lawful, Fair, and Transparent Processing
Data subjects must be informed about how their data will be processed and for what purposes.

Purpose Limitation
Data controller must limit its personal data collection to the extent necessary for lawful purposes.

Data Minimisation
Only the personal data that is necessary for the intended purpose should be collected and processed.

Accuracy
Personal data must be accurate, complete, and kept up to date.

Storage Limitation
Personal data should not be kept for longer than is necessary for the purposes for which it was collected.

Integrity and Confidentiality
Appropriate security measures must be in place to protect personal data against unauthorised or unlawful processing, loss, destruction, or damage.

Accountability
Data controllers are responsible for ensuring compliance with the PDPA and must be able to demonstrate such compliance.

Rights of Data Subjects
The PDPA grants data subjects various rights, including the right to access, correct, delete, and object to the processing of their personal data, as well as the right to withdraw consent at any time.

pwc

Transparency Requirements

The data controller is obliged to notify a data subject before or at the time that the data subject's personal data is collected. The notification provides data subjects with privacy information such as the data to be collected, purposes of processing, lawful basis of processing, retention periods, third parties to whom data may be disclosed, contact details of the data controller, and their rights under the PDPA.

Also, when collecting personal data from other sources, the data controller must provide data subjects with privacy information within a reasonable period (no more than 30 days) of obtaining the data.

Individual Rights

The PDPA provides legal rights for data subjects with regard to their personal data:

(1) Right to access and obtain copies of the data;
(2) Right to data portability;
(3) Right to object to processing;
(4) Right to erase the data;
(5) Right to restrict processing;
(6) Right to rectification;
(7) Right to lodge a complaint; and
(8) Right to withdraw consent.

However, it is noteworthy that not all data subject rights are sole and absolute as there are exceptions where a data controller may reject a data subject's request to exercise their rights.

Security & Data Breaches

Data security: According to the PDPA, data controller is required to implement suitable security measures to prevent the unauthorised or unlawful loss, access, use, modification, correction, or disclosure of personal data.

These security measures must be regularly reviewed and updated as necessary.

PDPA sets out the minimum standards for such security measures in detail. For instance, it includes requirements for controlling access to personal data and critical information systems, which involves verifying identities and authenticating users, granting access and usage rights appropriately, and ensuring that access is limited strictly to those who need it to perform their duties.

Data breach: The data controller must inform the PDPC of any personal data breach without undue delay and, where possible, within 72 hours of becoming aware of the incident, unless an exemption is applicable.

If the personal data breach is likely to pose a high risk to the rights and freedoms of the individual, the data controller must notify the data subject of the breach and the remedial actions taken without undue delay.

Other Business Obligations

Data Protection Officer (DPO): The data controller and the data processor are required to appoint a DPO to monitor internal compliance and provide advice regarding the PDPA where: (1) their activities require large scale, regular and systematic monitoring of personal data, or (2) their activities involve processing sensitive personal data. Employees or service contractors who have expertise in data protection laws, regulations and practices may be appointed as DPO.

Data processing records: The data controller and the data processor must arrange and maintain records of data processing activities for the data subjects. The data processing records must be done in writing. whether it be on hard copies or electronically, wherein the following details must be recorded:

(1) The collected personal data;
(2) The purpose of collection;
(3) The data controller's details;
(4) The retention period;
(5) The rights and means to access, including the conditions of person accessible and of access;
(6) The use or disclosure of personal data:
(7) The rejection of request or objection to the data subjects' rights;
(8) The description of personal data protection measures employed.

Cross-Border Transfers

Under the PDPA, cross-border transfers of personal data can be made through three main options:

(1) Whitelisted Countries (Adequate data protection standards): Transfers are allowed to countries or organisations recognised by the PDPC as having adequate data protection standards.
(2) Binding Corporate Rules (BCR): Multinational companies can use an agreement policy approved by the PDPC to transfer data within their group.
(3) Appropriate Safeguards: Appropriate safeguards may be in the one of the following forms: 1) Standard Contractual Clauses (SCCs) serve as foundational frameworks for legal agreements in cross-border data transfers. In Thailand, Asean Model Contractual Clauses and SCCs for the transfer of personal data to third countries under the GDPR are currently acceptable. 2) Certification which provides the appropriate safeguards in accordance with the recognized standards as prescribed by the PDPC. 3) Agreements that are legally binding and enforceable between the state agencies in Thailand and foreign state agencies that transfer personal data between each other.

Let's connect to discuss how we can help:

Vunnipa Ruamrangsri
Partner, PwC Legal Thailand

+66 02 844 1284
vunnipa.ruamrangsri@pwc.com