PwC Legal Insight # 06/2021
Legal update

Issued Date: 24 May 2021

# Catch up on the key points for Thailand's Personal Data Protection Act (PDPA)

## The following report may be of interest to:

All clients

## Summary:

Full enforcement of the Personal Data Protection Act B.E. 2562 (2019) (the PDPA) has been postponed for one more year due to the severe ongoing impact of the COVID-19 pandemic on both local and foreign businesses. On 8 May 2021, the Royal Decree postponing the PDPA's effective date from 27 May 2020 to 31 May 2022 was legislated and published in the Royal Thai Government Gazette. This means that the PDPA will now come into full effect from 1 June 2022.

This gives business operators a good opportunity to continue – or start – planning and implementing the fundamental steps necessary to be fully prepared for enforcement of the PDPA. To prepare for PDPA compliance, business operators who collect, use and disclose personal data need to be aware of these key points.

### 1. Jurisdiction

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.

### 2. Relevant parties

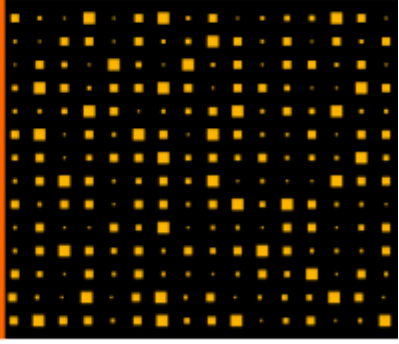
Three major players under the PDPA are:

- Data subject – an individual who can be identified directly or indirectly by the personal data, except for deceased and juristic persons.
- Data controller – an individual or juristic person having the power and duties to make decisions regarding the collection, use or disclosure of the personal data.
- Data processor – an individual or juristic person who collects, uses or discloses personal data on behalf of or as ordered by the data controller.

© 2021 PricewaterhouseCoopers Legal & Tax Consultants Ltd. All rights reserved. PwC refers to the Thailand member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 284,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.



Business operators can be identified as either the data controller or the data processor, with each role having different obligations and liabilities. Therefore, business operators need to be able to identify what their role is in each personal data processing activity.

**3. Personal data**

Personal data is information that can directly or indirectly identify or be traced back to the identity of a living individual. The PDPA stipulates two categories of personal data (general and sensitive personal data) for which different processing requirements and exemptions apply.

Sensitive personal data could create significant risks to the data subject's fundamental rights and freedoms. Examples of sensitive personal data are race, religion, health-related data, biometric data and criminal record. A data controller may only process sensitive personal data in limited circumstances and with a higher level of protection.

**4. Key lawful basis of data processing**

To collect, use and disclose a data subject's personal data, the data controller must have a valid legal basis. In business operations, the lawful bases frequently relied on include: (1) consent, (2) contract, (3) legitimate interest, and (4) legal obligation.

The data controller must identify the most appropriate lawful basis from the start and seek a new lawful basis whenever the purposes of processing change. We wish to highlight that consent is not always the most appropriate or easiest legal basis and it should only be treated as an alternative basis for data processing when no other lawful basis obviously applies. This is because consent can be revoked by the data subject at any time and the data controller is required to meet the consent requirements set out in the PDPA.

**5. Notification of data processing**

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.

**6. Cross-border transfers**

Under the PDPA, the data controller cannot transfer personal data to affiliates or third parties located in countries outside of Thailand with inadequate data protection standards as regulated by the soon to be constituted Personal Data Protection Committee (Committee). There are exceptions if the data transfer falls under any of the following circumstances: (1) compliance with the law, (2) obtaining consent from the data subject, (3) compliance with a contract between data controller and data subject, (4) compliance with a contract in the data subject's interest between the data controller and a third party, (5) protecting the data subject's vital interests, or (6) carrying out of an important task of public interest.

© 2021 PricewaterhouseCoopers Legal & Tax Consultants Ltd.. All rights reserved. PwC refers to the Thailand member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 284,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

**7. Data Protection Officer (DPO)**

The data controller and the data processor are required to appoint a Data Protection Officer (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.

**8. Record of processing activities (ROPA)**

The data controller and the data processor must prepare and maintain a written or electronic record of personal data processing activities (ROPA) for data subjects and the Committee to check and verify. The ROPA is important because not only is it a legal requirement, but it also helps business operators improve data governance and increase business efficiency.

**9. Rights of data subjects**

The PDPA provides legal rights for data subjects with regard to their personal data: (1) the right to access and obtain copies of the data, (2) the right to data portability, (3) the right to object to processing, (4) the right to erase the data, (5) the right to restrict processing, (6) the right to rectification, (7) the right to lodge a complaint, and (8) the right to withdraw consent. However, it's 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.

**10. Sanctions**

Failure to comply with the PDPA could result in civil liabilities including punitive damages with administrative fines of up to THB 5 million. Importantly, there are also criminal penalties which include imprisonment for up to one year or a fine of up to THB 1 million, or both. Any company directors, managers or other persons in a role of responsibility could be liable for the violation.

**11. The effect of PDPA postponement**

Although the data controllers are temporarily exempt from their obligations under the PDPA until 31 May 2022, they're still required to arrange and implement security measures for collected personal data at the acceptable standard set forth in the notification from the Ministry of Digital Economy and Society.

Data protection isn't just a legal requirement, it's an opportunity for business operators to build trust with customers, business partners, employees and investors. To ensure full compliance with the PDPA and mitigate any risks or exposure, business operators should seek professional legal consultation.

## For further information, please contact:


- Ms. Vunnipa Ruamrangsri, Partner, at vunnipa.ruamrangsri@pwc.com or +66 2 844 1284
- Mr. Thanakorn Busarasopitkul, Senior Manager, at thanakorn.busarasopitkul@pwc.com or +66 2 844 1293
- Mr. Korapat Sukhummek, Manager, at korapat.sukhummek@pwc.com or +66 2 844 2015
- Mr. Piniti Chomsavas, Manager, at piniti.chomsavas@pwc.com or +66 2 844 2032


© 2021 PricewaterhouseCoopers Legal & Tax Consultants Ltd. All rights reserved. PwC refers to the Thailand member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 284,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.