PwC Legal Insight # 05/2020
Legal update

Issued Date: 16 September 2020

Get ready to comply with the PDPA – effective 1 June 2021

The following report may be of interest to :

All clients

Summary :

The Personal Data Protection Act BE 2562 (2019) (PDPA) was legislated to give individuals more control over their personal data and stipulate new obligations of business operators on personal data protection and rules on how to process or treat the personal data. Under the PDPA, for example, data subjects have the right to withdraw their consent, at any time, to their personal data being collected, used or disclosed. They can also request the erasure, destruction or anonymisation of all of their collected personal data.

Business operators located in Thailand who collect, use or disclose personal data of data subjects, including employees, suppliers, vendors, distributors and customers, must comply with the PDPA, regardless of whether the personal data processing takes place inside or outside Thailand. Violating these legal requirements exposes business operators to civil, criminal and administrative penalties. Directors of limited companies may face criminal penalties for failure to comply with the requirements prescribed by the PDPA.

To prepare for PDPA compliance, business operators should take these key steps:

1) Review data

Review all existing data stored physically and virtually, identifying the type of data, source of data, the data subjects, the purpose and necessity of data processing, data retention period and the lawful basis of data processing.

Once the review is complete, create a data flow to map data usage – starting from the point of collection. This will help identify any areas of non-compliance or potential risks in the collection, use or disclosure of data, such as capturing personal data without a lawful basis e.g. consent, performance of a contract, legitimate interest, vital interest, legal requirement, public interest. The data review and risk assessment may be time-consuming, but it's essential.

2) Create documentations

Create required documentations to comply with the PDPA which may include privacy policy, privacy notice, consent form, data processing agreement, breach notification, consent withdrawal form, data inventory or the record of data processing activities. Business operators may separate the documents into two groups: (1) documentation for data subjects and (2) documentation for data processors.

For the first group of documents, business operators should create a standard consent form and privacy notice templates for the collection, use or disclosure of data subjects' personal data, and these templates must contain key elements to be valid under the PDPA. For example, (i) the consent form must contain an independent consent section and use an easily understandable term or language to prevent any ambiguity in the purposes of processing the personal data, (ii) the privacy notice must inform the data subjects of the collected persona data, the purpose of data processing, the data retention period, the type of third parties to whom the data may be disclosed, the contact details of business operators, and the data subjects' rights.

For the second group of documents, business operators should create a standard data processing agreement to be executed with data processors who collect, use or disclose personal data under the order or on behalf of the business operators. This is to stipulate data processors' duties and obligations to comply with the PDPA and ensure that the data processors will be liable or indemnify business operators for damage arising as a result of violation of the PDPA compliance.

3) Update existing procedures

The next step is to update current practices and procedures in line with the PDPA. These new practices and procedures must be set to support the created documentations. For example, business operators can prescribe procedures on how to collect data subjects' personal data on grounds of consent, how to process data subjects' requests with regards to their personal data, or what action to take in the situation where data breach occurs. Business operators should also consider appointing or assigning main contact person or responsible person who has sounded understanding of the PDPA to handle queries on personal data made against the business operators to manage the PDPA compliance risks and exposures. This person may be the data protection officer (DPO) whose qualification and duties must conform with the PDPA.

4) Train employees

Make sure all employees are up to speed on the requirements prescribed under the PDPA. This will help reduce exposure to the risk of non-compliance and the negative impact non-compliance will have on business operations. Ensuring that all employees are trained will also increase the chances of achieving full compliance with the law.

Despite PDPA enforcement being postponed to 1 June 2021, business operators should not ignore the importance of personal data protection and should start preparing for compliance now because it is time-consuming which may take 3 – 5 months to complete.

There are many steps that must be taken to make sure that a business operator and all of its employees, suppliers, vendors and distributors fully comply with the PDPA. If you're uncertain about how to proceed with any of these steps, you should consult a professional legal services team.

For further information, please contact:

- Ms. Vunnipa Ruamrangsri, Legal Partner, at vunnipa.ruamrangsri@pwc.com or +66 (0) 2844 1284
- Mr. Thanakorn Busarasopitkul, Senior Manager, at thanakorn.busarasopitkul@pwc.com or +66 (0) 2844 1293
- Mr. Korapat Sukhummek, Manager, at korapat.sukhummek@pwc.com or +66 (0) 2844 2015