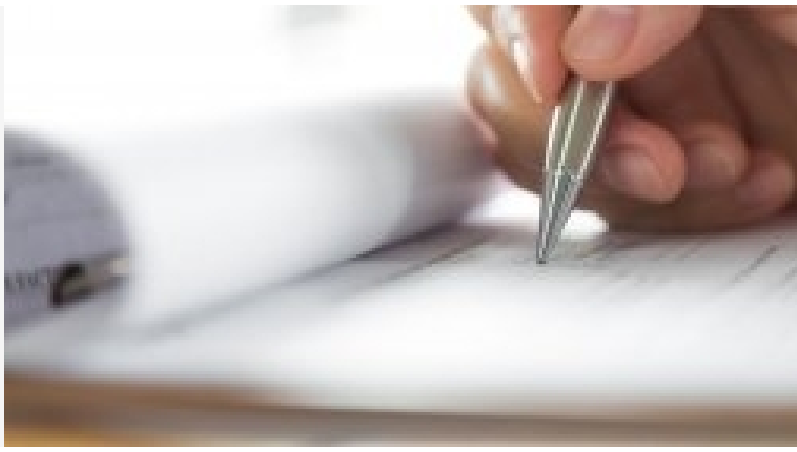
THAILAND'S PERSONAL DATA PROTECTION ACT: A BUSINESS CHECKLIST

15 APRIL 2020 • ARTICLE



The Personal Data Protection Act B.E. 2562 (2019) ("PDPA") will come fully into force on 27 May 2020 and represents Thailand's first comprehensive regulatory framework for the protection of personal information. This article outlines the key points of the PDPA and important recommendations for business when preparing a final checklist of what needs to be done to get ready for the implementation of the PDPA.

"Similar to the EU's General Data Protection Regulations ("GDPR"), the PDPA seeks to ensure that the processing of personal data has a legal basis."

KEY POINTS OF THE PDPA

The PDPA governs how the personal data of individuals is processed (i.e. collected, used, disclosed and transferred). If an entity located in Thailand acts as a data controller or processor, the PDPA applies regardless of whether the processing of personal data takes place inside or outside Thailand or if the data being processed is for Thai or non-Thai residents. Entities located outside Thailand will still be required to comply with the PDPA if they offer goods or services to residents of Thailand or observe the behaviour of individuals in Thailand and process their personal data.

Similar to the European Union's General Data Protection Regulations ("GDPR"), the PDPA seeks to ensure that the processing of personal data has a legal basis. Consent is only one of the legal bases for processing personal data, and other legal bases for data processing under the PDPA include:

- the preparation of historical, archival, research- or statistics-related documents (the "research basis");
- the prevention or suppression of dangers to a person's life, body or health (the "vital interest basis");
- where the processing is necessary for the performance of a contract to which the data subject is a party or for a precontractual request of the data subject (the "contract basis");
- where the processing is necessary for the data controller's mission carried out for the public interest or for the exercise of public powers granted to the data controller (the "public task basis");
- where the processing is necessary for the legitimate interests of the data controller or another person, which do not override the data subject's fundamental rights in the personal data (the "legitimate interest basis"); and
- the compliance with the data controller's legal obligations (the "legal obligations basis").

Another key aspect under the PDPA is the requirement to inform the data subject of (i) how their personal data will be used by the data controller, (ii) whether personal data will be disclosed to a third party and (iii) of the data subject's rights to their personal data. This must be done at the time the personal data is being collected from the data subject.

In relation to cross-border data transfers, the PDPA also regulates the transfer of personal data from Thailand to other countries and imposes obligations on the data controller and data processor to ensure that security measures are in place to protect personal data.

"Our experience is that even the most highly developed GDPR policies will require a degree of localisation to comply with the PDPA."

The PDPA introduces a range of new obligations on businesses and a new regime of how to treat personal data. Some of these obligations will apply with immediate effect on 27 May 2020, while other details are still pending subordinate legislation which will not be enacted until the formation of the Personal Data Protection Commission, the regulator under the PDPA which will develop subordinate regulations and enforce the PDPA. The absence of a Personal Data Protection Commission will not prevent data subjects commencing proceedings directly against data controllers or processors in the event of a breach of the PDPA.

For personal data obtained prior to 27 May 2020, the PDPA permits the continued use of the personal data but only for the purposes for which they were originally obtained, and provided that the procedure for revoking the consent to the use of this personal data is put in place and facilitated by the data controller. Therefore, businesses that intend to rely on this legacy exemption should understand its limitations and must inform their data subjects how to revoke the consent to use the personal data.

European business operators will recognise similarities between GDPR and the PDPA, but our experience is that even the most highly developed GDPR policies will require a degree of localisation to comply with the PDPA. In light of this new legal landscape, we recommend that all businesses that retain personal data comply with these seven preliminary steps to prepare for the PDPA's full effect.

Step 1 – Review the personal data required for your business

As the PDPA requires the data controller to have a legal basis for the processing of personal data, businesses should review which personal data is necessary for their operations. There may be different legal bases for different types of data, such as personal data required to provide services to customers, and personal data required for the company's internal operations, such as the day-to-day relationship with the company's employees and suppliers and vendors.

The review should focus on identifying the relevant actions and processes for each type of personal data, the personnel and the risks involved in the processing of personal data in order to design the measures suitable for the legal basis of collecting the personal data and protection of the personal data.

Step 2 – Identify the legal basis for the processing of personal data

In addition to consent, there are six legal bases for the processing of personal data. While consent is the legal basis most frequently used in past practice of data collection, consent may not be the most suitable or convenient legal basis in most cases as consent can always be revoked by the data subject, thereby preventing the use of the collected personal data.

In many cases, the contract basis and the legitimate interest basis could be relied on by businesses for collecting and processing personal data, but for the legitimate interest basis, the data controller must also ensure that the processing activities do not harm the rights of the data subject.

Step 3 – If consent is needed, review the consent request language

Consent has been the means used by businesses to ensure that their use of personal data would not be disputed even before the PDPA was enacted. However, the PDPA imposes a number of requirements on how consent is obtained from the data subject to ensure that individuals are well-informed, and that the consent is freely given.

Consent requests are now required to be separate from other matters and must be presented in clear and plain language. This means consent requests can no longer be in small print or lumped together with other terms and conditions. If consent wording is in one language only, there is a real risk that consent could be challenged by native speakers of other languages as not having been requested in accordance with the PDPA. Multi-language support is therefore likely to form a significant part of the localisation process.

CONSENT REQUESTS CAN NO LONGER BE IN SMALL PRINT OR LUMPED TOGETHER WITH OTHER TERMS AND CONDITIONS.

Another key requirement is that consent for the processing of personal data must not be used as a condition to the data subject's use of the data controller's services unless the personal data is necessary for the provision of the services. This means that the current common practice of requiring customers to consent to a catch-all terms and conditions on the use of personal data, including the use for direct marketing or sharing with affiliate companies for marketing purposes, before they can use the services, is not permitted under the PDPA.

The PDPA also has a more stringent consent requirement for sensitive personal data which relate to race, ethnicity, political opinions, sectarian, religious or philosophical beliefs, sexuality, criminal records, health data, disability, trade union information, genetic data, biometric data and other personal data prescribed by the Personal Data Protection Commission. The consent for the processing of these sensitive classes of personal data must be explicit and must be separate from a consent request for processing other general personal data.

Step 4 – Prepare and implement privacy notice and privacy policy

The PDPA requires the data controller to inform the data subject of the details on how their personal data will be used, the relevant legal bases for data processing, the persons to whom their personal data may be disclosed, the retention period for personal data, contact details of the data controller and the data protection officer (if applicable), and the rights of the data subject.

"The PDPA requires the data controller to inform the data subject of the details on how their personal data will be used."

This information can be placed in the form of a "Privacy Notice" to be presented to each data subject prior to the collection of their personal data. The Privacy Notice can be short and simplified so that it can be easily understood, with a link to more comprehensive details contained in the "Privacy Policy" which sets out in detail the reasons for the processing as well as the manner of processing and the procedure for the data subject to exercise their rights under the PDPA.

Step 5 – Prepare a data processing agreement with data processors

If any of the processing of personal data is not done in-house, the PDPA requires the data controller and the data processor to enter into a data processing agreement. "Processing" activities cover many day-to-day or back-office activities, including data storage, whether offline or cloud-based. Therefore, it is likely that most businesses will be required to enter into a data processing agreement with a service provider.

In the data processing agreement, both parties should ensure proper allocation of their responsibilities as the PDPA imposes civil, administrative and criminal liabilities, and permits the data subject to claim for punitive damages in the event of a data breach.

Step 6 – Consider whether to appoint a Data Protection Officer

Similar to the GDPR, the PDPA also requires the data controller and the data processor in the private sector to appoint a data protection officer ("DPO") if their activities require regular and systemic monitoring of personal data due to a large volume of personal data or if their activities involve the processing of sensitive personal data.

However, the criteria of what is considered as "regular and systemic monitoring of personal data due to a large volume of personal data" are yet to be determined Personal Data Protection Commission. While this point remains unclear, it is likely that many large businesses and larger SMEs will be required to appoint a DPO.

The DPO's functions are to give advice on the compliance with the PDPA, audit the processing of personal data by the company and its employees and coordinate with the Personal Data Protection Commission Office in case of issues of compliance with the PDPA.

The failure to appoint a DPO when required can result in non-compliance with the PDPA even if the company's collection and processing of personal data otherwise complies with the PDPA.

Step 7 – Prepare inter-group policy on data transfer if you share personal data with an affiliate in another country

"The scope of obligations under the PDPA will increase once the Personal Data Protection Commission Office becomes operational."

The PDPA regulates cross-border transfers of personal data with a mechanism similar to the adequacy decision under the GDPR. However, as the details of which countries are considered as having "adequate privacy safeguards" have not yet been prescribed, data controllers may rely on other grounds for cross-border transfers which are: compliance with legal obligations, the contract basis, compliance with contractual obligations of the data controller with a third party for the benefit of the data subject, the vital interest basis, and the carrying out of an important task of public interest.

For companies which share personal data with their affiliates outside Thailand, the PDPA has mechanism similar to the GDPR's binding corporate rules. This permits cross-border transfers of personal data if the data controller or the data processor has an internal policy with safeguards for cross-border transfer of personal data to its foreign affiliate, provided that this internal policy has been approved by the Personal Data Protection Commission Office.

Although the Personal Data Protection Commission Office's criteria for the inter-group policy for cross-border transfer has not been prescribed, businesses may start making preparations for inter-group data privacy measures.

This is the PDPA in a nutshell. The scope of obligations under the PDPA will increase once the Personal Data Protection Commission Office becomes operational. If you have any questions or require further advice or assistance in relation to the preparation of your business for the PDPA, please do not hesitate to contact us.

KEY CONTACTS

NATTANIT BOONRUANG
ASSOCIATE • BANGKOK

T: +66 2 665 7848

nboonruang@wfw.com