DRKILAW TALKS 188

Dherakupt International Law Office Ltd.
900 Tonson Tower, 12F/L, Ploenchit Road, Lumpini,
Patumwan, Bangkok 10330

PDPA Compliance Guide for Businesses

January 2021

There is a 5-month countdown until 1 June 2021, the date Thailand's Personal Data Protection Act ("PDPA") becomes effective. Government will actively enforce this law. Every business must be ready to comply. We provide a PDPA checklist to help readers assess their readiness for the PDPA.

Thailand's PDPA

The PDPA sets out to protect the personal data of individuals. Every business, as a "data controller" must comply with the PDPA during its collection, use, and disclosure (a/k/a "processing") of "personal data" of "data subject(s)," all of which are defined under this new law.

Below are minimum PDPA requirements for businesses, as data controllers, in the form of a summary checklist.

PDPA Checklist for Businesses

1. Prepare & Implement Privacy Polices

Businesses must determine the types of personal data they collect, period of storage, and purposes of collection. Businesses must inform the data subject of, among other things, data processing activities, and rights of the data subject.

The data subject must be informed of processing activities before or at the time of businesses collect their personal data.

2. Prepare Requests for Consent

The business must acquire clear consent and/or explicit consent for sensitive data from the data subject in order to process its personal data (unless the data is processed according to lawful bases, e.g. contractual obligation, legitimate Interest, vital Interest, etc.)

The consent request form must be clear and truthful, and must not be intended to mislead or deceive. The business can provide the form wither in writing or via electronic/digital channels.

3. Prepare Requests for Consent from Data Subjects under 10 Years of Age

If a business processes personal data of minors under 10 years old, it must obtain consent, from the adult with parental authority over the minor, to process such data.

4. Prepare Data Processing Agreement

If the business hires service providers who process personal data according to the instruction of the business, it must enter into a data processing agreement with the service provider as it is a data processor. This agreement must stipulate the clear rights and duties of the service provider, and govern the relationship between the business and the service provider to secure the personal data.

5. Prepare Cross Border Transfer Assurances

If the business transfers personal data to foreign countries, it must ensure that the recipient country has adequate personal data protection standards, or ensure that it meets other legal criteria to lawfully cross-border transfer personal data.

6. Appoint Data Protection Officer

The business may appoint a Data Protection Officer ("DPO") to monitor and audit its compliance with the PDPA where its data processing activities require regular monitoring of personal data because of the large volumes of personal data, or its core activity is the processing of sensitive data.

7. Implement Proper Personal Data Security

The PDPA requires that businesses procure appropriate data protection security measures to prevent unlawful of unauthorized access to, and loss use, alteration, correction or disclosure of, personal data. The data security measures must also include minimum administrative, technical and physical safeguards.

8. Define Period of Storage

Businesses can no longer store personal data of its customers and employees for an unlimited periods of time. The business, must, under the PDPA, specify periods of personal data storage and inform the data subject accordingly.

9. Prepare Personal Data Processing Records

Business must, according to the PDPA, prepare processing records accessible to data subjects and the Office of the Personal Data Protection Committee upon lawful request. Processing records must include all details required by the PDPA.

Processing can be made in written or electronic form.

Criminal, Civil, and Administrative Penalties

Violation of the PDPA or personal data breaches could lead to:

- Civil penalties – actual compensation to the data subject for damage and punitive damages (up to 200% of actual compensation) and;
- Criminal penalties – fines up to Baht 1 million or imprisonment up to one year, or both; and
- Administrative penalties – fines of up to Baht 5 million

The PDPA also prescribes penalties for directors, managers, or any responsible person involved in the violation or data breach. Businesses are liable for violations or breaches committed by employees.

Author's Note:

The PDPA which was initially due to take effect on 27 May 2020. Government postponed enforcement until 1 June 2021 as the COVID-19 pandemic negatively affected Thailand's business sector. There is currently no indication government will postpone enforcement for a second time.

Government, by all current indications, is committed to protecting the safety and integrity of personal data processed in Thailand, particularly since it will be held to a nearly equal standards among peer countries with which it transacts and interacts. As such, businesses can enforcement at both the private and public levels. However, businesses can spin their compliance efforts into a positive public relations to garner trust among customers, stakeholders and employees.

Every business in, or with a commercial nexus to, Thailand that collects, uses, or discloses (a/k/a/ processes) personal data of individuals in Thailand must implement necessary compliance measures. Compliance can be very costly, if done in excess. Insufficient compliance, on the other hand, may expose the business to significant risks and penalties.

By Anuphan Kitnitchiva Ph.D., Senior Partner and Anchalee Klinkesorn, Associate Director Dherakupt International Law Office Ltd.