THE PDPA: THE CHANGING LANDSCAPE OF COMPLIANCE IN THAILAND

6 NOVEMBER 2019 • ARTICLE

A NEW ERA FOR DATA PROTECTION IN THAILAND HAS BEGUN

The Personal Data Protection Act (PDPA) came into force on 28 May 2019. We look at the key differences between the PDPA and the GDPR and apply lessons from GDPR prosecutions to compliance with the PDPA.

This article should be read in conjunction with our previous articles on **"The GDPR AND PDPB: What do you need to know about data privacy and protection?**" and "**GDPR, PDPB and M&A transactions in Thailand**". Here, we consider the differences between the two pieces of legislation and the impact of the PDPA upon businesses operating in Thailand.

WHAT ARE THE KEY DIFFERENCES BETWEEN THE PDPA AND GDPR?

SUBJECT	GDPR	PDPA
1. Consent – Similarities	'Consent' of the data subject means any **freely given, specific, informed and unambiguous** indication of the data subject's wishes.	Consent must be **freely given** before or during the collection of personal data.
	Consent can be deemed as **not freely** given when entering into a contract is **conditional** on consent to the processing of personal data that is not necessary for the performance of that contract.	In entering into a contract, there must not be any **condition for consent** to be granted to collect, use or disclose personal information that is not necessary or relevant to entering into such contract.
	Consent is informed and specific when the subject is informed about the purpose of data collection, the controller's identity, use of data for automated decision-making and certain other information.	Specific objectives and other significant information related to processing must be communicated to the data subject.
	Personal data must be processed only where it is **necessary for the specified purposes.**	Personal data must be processed only where it is **necessary for the specified purposes.**

SUBJECT	GDPR	PDPA
	The request for consent must be presented in a manner that is clearly distinguishable from other matters, using **clear and plain language.**	Consent must be requested in a manner that is clearly distinguishable from other matters, using **clear and plain language.**
	The data subject must have the **right to withdraw consent** at any time and it should be easy to do so.	Likewise, the data subject must have the **right to withdraw consent** which was previously given.
	Exceptions to consent requirement: Contracts, legal obligations, vital interest of data subject, public interest and legitimate interest (Art. 6 GDPR).	**Exceptions** to consent requirements: Vital interest, public interest, legal obligations and legitimate interest.
Differences	**No specific form requirement**, but written consent recommended because data controller has burden of proof.	Request for consent must be in either **written or electronic form** unless that is impossible by its nature.
	Parental consent necessary for minors under **13-16 years**, depending on Member State implementation.	**Parental consent** necessary for minors under **10 years**.
	No grandfather provision (Art. 94 (1), 99 GDPR).	**Grandfather provision** for personal data collected prior to the PDPA coming into effect. Data collectors may continue to use this data for the original, intended purposes, without the need to obtain consent. However, data controllers must provide procedures that allow data owners to withdraw their consent when the data is no longer being used for the original purpose.
2. Extraterritoriality	Will apply to personal data collected, used or disclosed in the European Union (EU) or elsewhere, if the entity resides in the EU. Also applies to entities without an EU establishment if they process the data of EU nationals or residents where the processing is related to (i) the offering of **goods and services** to EU data subjects or (ii) to **monitoring of their behaviour**, such as by the use of website cookies.	Will apply to personal data collected, used or disclosed in Thailand and elsewhere, if the entity, domestic or foreign; (i) processes personal data of a data subject in Thailand during the course of activities related to the offering of **goods and services**; (ii) **monitors the behaviour** of the data subject in Thailand.
	Requirement for data controller to appoint a representative within the jurisdiction.	Requirement for data controller to appoint a representative in Thailand.

SUBJECT	GDPR	PDPA
3. Rights of Data Subjects	Broad protection is offered under the GDPR for data subjects in their dealings with data controllers and processors, including the right to information to access, to data portability, to withdraw consent, to rectification, to restriction of processing and to erasure/right to be forgotten.	The PDPA grants essentially the same rights, but some **rights differ in their scope.** Notably, the **right to erasure** only allows for data deletion if data controller is non-compliant or if it is no longer necessary for data controllers to retain personal data in accordance with the purpose of the collection, use or disclosure.
	In case of **withdrawal of consent, processing of collected data becomes unlawful** unless on other legal grounds.	In case of withdrawal of consent, **processing of collected data** remains **lawful**.
	Art. 22 (I) GDPR restricts decision-making that is solely based on **automated processes** and significantly affects the data subject, such as racial profiling or credit evaluation.	The PDPA does not contain such a provision.
4. Penalties	There are **two tiers of penalties**: Administrative fines of up to €10m (THB336.5 m) or 2% of annual global turnover in the preceding financial year (whichever is higher) can be issued for infringements of certain articles (8, 11, 25-39, 42, 43). Administrative fines of up to €20m (THB673m) or 4% of annual global turnover in the preceding financial year (whichever is higher) can be issued for infringements of articles of certain articles (5, 6, 7, 9, 12-22, 44-49).	Administrative fines can also be applied, **of up to THB5m** (€148,560).
	Right to compensation for tangible or intangible damages. The GDPR **does not limit the amount of compensation** for such damages.	Compensation for civil law liability may be granted at the court's discretion but **no more than twice the actual damages**, with claims potentially multiplied under Thai law as data subjects may bring class action lawsuits.
	Criminal liability depends on Member State implementation.	Criminal liability can **result in fines of up to THB1m** (€29,700) and/or possible **imprisonment** sentences of up to one year for directors and officers of the company.

SUBJECT	GDPR	PDPA
		Where a company has committed an offence, its directors are liable if the offence was a result of an act or the direction of the director, or if the director has a duty to direct or act and fails to do so.
5. Data Protection Officer ("DPO")	The GDPR provides that a DPO is needed if you meet one of the following criteria: (i) Public authority — the processing of personal data is done by a public body or public authorities, with exemptions granted to courts and other independent judicial authorities; (ii) Large scale, regular monitoring — the processing of personal data is the core activity of an organization which regularly and systematically observes its "data subjects" on a large scale; and (iii) Large-scale special data categories — the processing of specific "special" data categories as defined by the GDPR is part of an organization's core activity and is done on a large scale.	The PDPA provides that a DPO be designated for only two types of activities: (i) Activities which require regular, large-scale monitoring of personal data; and (ii) Core activities which encompass processing of sensitive information.
6. Data Protection & Security	The GDPR contains detailed obligations requiring data protection by design and by default. The GDPR enshrines the requirement of security of processing, covering encryption, confidentiality and system checks.	The PDPA does not have equivalent provisions detailing the means by which data protection or security of processing must be ensured.

"It is unclear whether the Thai government will seek designation for Thailand under the 'Adequacy Decision' power in Article 45 of the GDPR to allow for personal data to be sent to Thailand without further approval. "

A TALE OF TWO REGIMES

Although the PDPA closely resembles and is based on the GDPR in spirit and substance, companies in Thailand will need to comply with both regimes. It is unclear whether the Thai government will seek designation for Thailand under the 'Adequacy Decision' power in Article 45 of the GDPR to allow for personal data to be sent to Thailand without further approval. More significantly, this would indicate that Thailand's data privacy and protection regime meets international standards. The differences between the PDPA and GDPR may make this more challenging.

Hindsight – what can we learn from GDPR prosecutions and looking back on the first six months of the PDPA

Employees play a critical role in data privacy and protection and can be the weakest link in data privacy and protection systems, policies and procedures.

Defects and weakness in data storage, processing and security systems provide ready and regular opportunities for the theft and misuse of personal data.

Updated and documented policies, procedures and systems play a central role in a company's response to claims or investigation of a breach.

Enforcement against companies operating outside the jurisdiction of the EU remains uncertain and reputational damage may be a greater deterrent.

It is unclear how authorities should deal with a situation where a company complies with its local data privacy and protection laws and regulations but is in breach of the GDPR or PDPA, particularly where the requirements and standards diverge or where compliance with the laws and regulations of one jurisdiction could be in breach of the laws and regulations of another jurisdiction.

"Employees play a critical role in data privacy and protection and can be the weakest link in data privacy and protection systems, policies and procedures."

It is unclear how authorities should deal with a situation where a company complies with its local data privacy and protection laws and regulations but is in breach of the GDPR or PDPA, particularly where the requirements and standards diverge or where compliance with the laws and regulations of one jurisdiction could be in breach of the laws and regulations of another jurisdiction.

GDPR: HALFWAY TO COMPLIANCE?

To comply with the PDPA and/or GDPR requires companies to ensure that their systems, policies and procedures meet the requirements of the legislation and that employees, directors and management understand the data privacy and protection regime and their role in compliance with the regulations.

Below are some suggested key issues and steps:

1. Review existing **data protection procedures and policies**. These should be critically reviewed on a regular basis to ensure that they reflect the operation of data privacy and protection policies and procedures and to test if the necessary systems, procedures and policies are in place;
2. Apply the outcomes of **convictions and prosecutions** to data privacy and protection policies, procedures and training;
3. Ensure that changes to data privacy and protection policies and procedures are reflected in other documents, particularly **employment contracts and supplier, contractor and other commercial contracts**;

4. Regular briefings and training for **directors, managers and other officers**, particularly in relation to their roles in compliance with the legislation and the financial penalties for breaches of GDPR and the criminal penalties for a breach of the PDPA;
5. Ensure that there are **suitable and compliant systems, policies and procedures to protect personal data** to categorise and distinguish between types of personal data required for legitimate business purposes, sensitive data relevant to employee profiles and personal data provided directly and indirectly by the data subject;
6. The procedures allowing employees to bring **claims of breaches** to the Personal Data Collection Commission ("PDCC") should be regularly reviewed and modified based on actual complaints;
7. Provide regular personal **data handling and protection training to employees**, informing them of the scope and limits of their rights as data subjects, as well as their power to grant or withdraw consent;
8. Where **employee personal data has been collected prior to the PDPA coming into force**, consider informing employees that this data will continue to be used for the original, intended purpose/s and that any change in use to be notified to the employees, at which time they may consent or deny its continued use; and
9. **Regular training for the DPO** and monitoring of feedback and outcomes of data processing activities of the data processor/controller in large scale uses of personal data or sensitive information.Should you like to discuss any of the matters raised in this article, please contact Alan Polivnick.

Should you like to discuss any of the matters raised in this article, please contact Alan Polivnick.

KEY CONTACT

ALAN POLIVNICK
PARTNER • SYDNEY

T: +61 2 9276 7607

apolivnick@wfw.com