MARSH JLT SPECIALTY

Client Alert

JULY 2019

The Thailand Personal Data Protection Act (PDPA) 2019

The Personal Data Protection Act (PDPA) 2019 was published on May 27, 2019. The provisions relating to the establishment of the Personal Data Protection Committee ("PDPC") became effective the day after the publication in the Royal Gazette, i.e. May 28, 2019. Other provisions of the PDPA, which include the provisions on collecting consent, use, and disclosure of personal data, rights of data subjects, liabilities, and penalties, will become effective on May 27, 2020. Businesses have started preparing themselves to ensure that they comply with the provisions of the PDPA once it comes into full force.

The PDPA protects the personal data of data subjects in Thailand, but this is not limited to Thai nationals.

In conjunction with Tilleke & Gibbins International Ltd, we have outlined the key points in the Act. We have also highlighted the key protection available under a Cyber Security insurance policy as well as the coverage implications as a result of this new law.

TO WHOM DOES THE PDPA APPLY?

Generally, the PDPA is applicable to persons and entities that collect, process, or transfer personal data – unless otherwise exempted (e.g. certain governmental bodies).

There are two key roles, as defined in the PDPA: (i) a data controller; and (ii) a data processor. A controller means a person/entity with the power to make decisions regarding the collection, use, and disclosure of personal data (as defined below), while a processor merely collects, uses, or discloses personal data in accordance with the instructions of, or on behalf of, the controller. Controllers generally have more obligations than processors.

MARSH

The PDPA has extraterritorial jurisdiction, and thus, overseas controllers/processors could still be subject to the PDPA, if the processing of personal data undertaken relates to any of the following:

- The offering of goods or services to individuals in Thailand, regardless of whether any payment will be made by the data subject.
- The monitoring of an individual's behaviour in Thailand.

WHAT RESPONSIBILITIES WILL COMPANIES HAVE UNDER THIS NEW REGULATION?

Almost all types of business operators are identified as a controller and/or a processor, depending on the purpose of possessing the data, and the nature and amount of personal data.

In general, a controller must:

- Obtain consent from the data subject before, or at the time of, collecting personal data.
- Implement suitable measures for preventing unauthorized access (the detailed standards for suitable measures will be further prescribed by the PDPC).
- Implement a system to delete personal data when the retention period expires, when it is no longer necessary, or when consent is withdrawn by the data subject.
- Maintain written records relating to the processing activities, and have such records available for inspection by the data subject and the PDPC.
- Assess and appoint a data protection officer (DPO), if required.
- Notify the PDPC of any data breach, without delay, and within 72 hours. If the breach has a high risk of affecting the data subject, each impacted data subject must also be notified, and remedial action must be undertaken without delay.

A processor must:

- Follow the lawful instructions of the controller when processing personal data.
- Implement suitable measures for preventing unauthorized access.
- Assess and appoint a data protection officer (DPO), if required.
- Maintain records of the processing activities, in accordance with the criteria and procedures to be prescribed by the PDPC.

WHAT KIND OF INFORMATION DOES THE PDPA APPLY TO?

The PDPA defines "personal data" as any data pertaining to an individual which enables the identification of such individual, whether directly or indirectly, but not including the data of the deceased specifically.

This means that any information could be subject to the provisions of PDPA, if such information belongs to a person, and it can be used to identify that person. This includes, for example, the name, surname, photograph, identification card number, and passport number, etc.

WHAT WILL THE PENALTIES BE FOR FAILING TO COMPLY WITH THE PDPA?

Failure to comply with the provisions of the PDPA could lead to the following penalties:

- Civil Liabilities: The court may order punitive damages of up to twice the value of the actual damage.
- Administrative fines ranging from THB 500,000 to THB 5,000,000.
- Criminal Penalties: Imprisonment for a term not exceeding 1 year, and/or a fine not exceeding THB 1,000,000.

ARE THE FINES INSURABLE BY LAW?

Civil liabilities are generally insurable under Thai law. However, this does not apply to criminal penalties. In relation to civil administrative fines, a few insurance companies do offer coverage for civil administrative fines, where insurable by law, in their Cyber Security insurance policies.

WE OUTSOURCE THE PROCESSING OF THE DATA - DO WE STILL HAVE TO COMPLY WITH THE PDPA?

If you have the power or duty to make decisions relating to collection, use, and/or disclosure of the personal data, you would be regarded as the controller. Therefore, most of the time, you would have to comply with the PDPA.

WHAT IS CYBER SECURITY INSURANCE?

Cyber Security insurance is an integral part of a risk transfer strategy for any company reliant on an operational technology or information technology dependent infrastructure. Cyber Security insurance can fill the gaps in traditional insurance, as well as provide direct loss and liability protection for risks created by the use of technology and data in an organization's day-to-day operations. These insurance policies are flexible, allowing a customized programme to provide protection for the key exposures.

Please contact your Marsh broker to examine your organization's unique risks and concerns, and for further information on available solutions that can be tailored towards them.

BOARD GOVERNANCE MUST INCLUDE CYBER SECURITY RISK MANAGEMENT

Cybersecurity risks and evolving cyber regulation are dominating boardroom conversations. Board Directors and Senior Executives have come to the realisation that the potential liabilities arising from such risks for themselves, as well as their organisation, are nearly unlimited. Increasingly, regulators and shareholders will hold management accountable for poor risk management and cyber governance.

SUMMARY

The change in legislation may require immediate action from organisations to ensure the ability to comply with the new requirements. Compliance with the requirements following a breach could be costly – all affected organisations need to assess and understand the risk of these potential costs and to consider how best to manage and transfer them.

Please feel free to contact your Marsh broker for further advice.

Contacts:

THEERAYA PHONGPOOL
+66 2626 5670
theeraya.phongpool@mmc.com

KUNDIS SETHAPONGKUL
+66 2626 5633
kundis.sethapongkul@mmc.com

ARATI VARMA
+65 6922 8028
arati.varma@marsh.com