DATA PROTECTION LAW OF THAILAND: INTRODUCTION

OVERVIEW

The Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**") of Thailand came into force on the 28th of May 2019. It establishes a framework of principles, rules and bodies which protects an individual's personal data whilst also enabling businesses to continue to derive economic value from the exploitation of personal data. A one-year grace period is currently in place to give organizations time to be prepared to comply with the provisions of the PDPA. It ends on the 28th of May 2020.

KEY PRINCIPLES

The PDPA has the following key principles:

- **Organizations must appoint a Data Protection Officer** ("**DPO**") if an organization's 'core activities' involve the collection use and disclosure of personal data or if the regulator mandates it.
- **Extra-territorial application** to Processors and Controllers both in and outside of Thailand provided that the Processor or Controller is collecting, using or disclosing the personal data of a data owner ("**Data Subject**") in Thailand.
- Data breaches must be notified to the regulator within **72 hours** of the discovery of a breach.
- **Criminal, civil and administrative** sanctions are available.

KEY DEFINITIONS

Personal data is any data which relates to a living individual which enables either direct or indirect identification of said individual.

Personal Data Controllers ("Controllers") are persons (real or juristic), who have the power and duty to decide on the collection, use or disclosure of personal data.

Personal Data Processors ("Processors") are a person (real or juristic) who collects uses or discloses personal data on behalf of a Controller.

ENFORCEMENT BODIES

The PDPA establishes the Personal Data Protection Commission ("**PDPC**"). Its main function is to act as the sector's enforcer, publish implementing laws and establish "Expert Committees" which act as specialist tribunals which handle disputes and complaints under the PDPA.

KEY PROVISIONS

Notice & Consent: Individuals must provide consent to a Controller prior to or at the time of any collection, use or disclosure of information. However, for an individual to give valid consent, they must be notified of the purpose of the data collection, retention periods, information about the controller, the Data Subject's rights, etc.

Limitations: There are five types of limitations on Controllers: purpose, proportionality, source, retention and transfer. **Purpose limitation** refers to the inability of a Controller to collect, use or disclose personal data for any purpose other than that which was notified and consented to prior to or at the time of collection. **Proportionality** refers to the prohibition of a Controller to collect, use or disclose more personal data than is necessary to achieve the original objective that the personal data was collected for. **Source limitation** refers to the general principle that personal data may only be collected directly from the Data Subject. **Retention limitation** refers to the inability of a Controller to keep personal data for longer

than is required in order to achieve the original objective of the collection of personal data. **Transfer limitations** refer to a prohibition on cross-border transfers of personal data where the destination has an inadequate level of data protection.

Access, Correction and Portability: Controllers have an obligation to ensure that personal data is up to date, accurate and not misleading. To complement this, Data Subjects have the ability to request that Controllers correct their personal data and that Controllers grant them access to their own data. Additionally, Controllers are required to ensure that Data Subjects are able to obtain their data in a format which can then be reused by other online service providers with ease. This involves storing and disclosing data in a format which is interoperable with the systems of other Controllers.

Security: The PDPA mandates that all Controllers provide appropriate security measures to prevent the loss, access, use, modification and disclosure of personal data without authorization.

Openness: The Openness principle mandates that Controllers be transparent with Data Subjects and disclose key pieces of Information for examination by Data Subjects to verify.

PENALTIES

The PDPC may impose administrative fines of up to THB5,000,000. Criminal breaches of the PDPA may carry up to a year of imprisonment or a fine of up to THB1,000,000. Aggrieved Data Subjects may file civil lawsuits and the court has the power to award up to twice actual damages against a Controller or Processor.

NEXT STEPS FOR ORGANIZATIONS

The PDPA poses a fundamental challenge to organizations of all sectors. Accordingly, LawPlus Ltd. recommends that organizations review their personal data protection policies and practices and undertake the following to prepare themselves for the end of the Grace Period on the 28th of May 2020:

(1) Review privacy policies and notices
(2) Review/create data breach notification procedures
(3) Review data transfer policies
(4) Identify Controllers and Processors
(5) Review data security measures, both online and offline
(6) Appoint DPOs

ABOUT THE SERIES

This is the first article of a series on Data Protection law in Thailand. Subsequent articles will cover each of the key principles in greater depth and will even cover specific sectors and special topics. The next article will focus on the Notice and Consent principles of the PDPA.

To find out more about how LawPlus Ltd. can help you and your organization comply and navigate Thai data-protection and cyber-security law, feel free to get in contact with us.

Revised: October 2019

Kowit Somwaiya
Managing Partner
kowit.somwaiya@lawplusltd.com

Jia Xiang Ang
Coordinator
jiaxiangang@lawplusltd.com