DATA PROTECTION LAW OF THAILAND: NOTICE & CONSENT

Adherence to the notice and consent principles of the Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**") is vital to any PDPA compliance regime. Notice and consent are two separate matters but are inextricably linked pre-requisites of any collection, use or disclosure of personal data.

NOTICE REQUIREMENT

The PDPA requires that Controllers notify data subjects of the purpose of any collection, use or disclosure of personal data prior to or at the time of a collection. The underlying purpose of this requirement is to ensure that data subjects are made aware of how their data will be used and for what purpose it serves. It enables an individual to make an informed decision when giving consent to Controllers to collect use or disclose their personal data. Examples of information which must be notified to the Data Subject include the following:

- Purpose of data collection
- Consequences of not providing data
- Rights of Data Subjects
- Retention periods
- Types of data to be collected
- Information about the Controller

EXCEPTIONS TO NOTICE

While the requirement of consent contains many exemptions, the requirement of notice is almost never exempted, save for situations where: (1) it can be proven that notification would defeat the purpose of collection use or disclosure and (2) in urgent situations where collection, use or disclosure is vitally important and required by the law to protect the legitimate interests of an employer.

CONSENT REQUIREMENT

Personal data is owned by the individual it pertains to, therefore, prior to any collection use or disclosure of personal data, a Data Subject must consent to it, and may at any time revoke its consent unless unable to do so for contractual reasons. Consent may be given either in writing or electronically unless it is by nature, impossible. To validly request consent, a request must meet certain requirements under the PDPA, some of which overlap with the requirement of notice. This includes: (1) notification of the purpose of the collection, use or disclosure; (2) requests for consent must be clearly distinguishable from other matters; and (3) requests must be made using clear and plain language that is easy to understand and is not misleading to a data subject.

EXCEPTIONS TO CONSENT

There are three categories of consent exceptions under the PDPA which include: (1) exemptions for collections of normal personal data; (2) exemptions for the collection of personal data from sources other than the Data Subjects; and (3) exemptions for collections of sensitive personal data. Despite having three categories of consent exceptions under the PDPA, significant overlap exists between them and their relevant grounds of exemption. The following are the main purposes for any collection use and disclosure of persona data without the consent of a data subject under the PDPA:

(1) To prevent harm to life, or the health of an individual.
(2) To be used for the lawful activities of non-profit organizations.
(3) To prepare historical or statistical documents for the public benefit.
(4) To carry out duties to benefit of the public or to perform functions as allocated by the state.
(5) To comply with contractual obligations.

(6) To establish, enforce and uphold legal claims.
(7) To comply with the PDPA, other laws and public policy objectives (health and research).
(8) To protect the legitimate interests of the employer.

RISKS

In addition to the criminal, civil and administrative penalties, a failure to collect personal data in an adequate manner would result in the Controller being unable to collect use or disclose the personal data already collected and would have to delete such data. This may be dangerous for companies whose business models revolve around the use of insights derived from processing personal data. More critically however, such a failure may cause serious reputational harms to the company and may ultimately lead to economic losses. Listed companies may see large (possibly long term) negative fluctuations in their stock price, banks and fin-tech companies may lose the trust (and thus patronage) of their customers and users of social media platforms may migrate to other platforms.

NEXT STEPS FOR ORGANIZATIONS

Given that there is less than a year before the grace period ends on the 28th of May 2020, LawPlus Ltd. recommends that organizations do the following:

For the Requirement of Notice

- Compile information on how your organization collects uses and discloses personal data, specifically with respect to the information which must be noticed.
- Determine the impact on the service provided if consent is withdrawn.
- Determine a data retention policy for the various types of personal data that the organization collects.
- Draft a privacy policy in line with the requirement of notice.

For the Requirement of Consent

- Draft and design a consent notice which considers the capacity of a given data subject to give consent and is context sensitive.
- Identify situations where consent is required and where exemptions may apply.
- Conduct a review of consent request webpages and physical forms to ensure PDPA compliance and to ensure that data subjects are able to withdraw consent as easily as they give it.

ABOUT THE SERIES

To read our first article "Data Protection Law of Thailand: Introduction" simply click on the link. Stay tuned for our next article on the various limitations imposed on the collection, use and disclosure of personal data under the PDPA.

Revised: October 2019

Kowit Somwaiya
Managing Partner
kowit.somwaiya@lawplusltd.com

Jia Xiang Ang
Coordinator
jiaxiangang@lawplusltd.com

LawPlus Ltd.
Unit 1401, 14th Fl., Abdulrahim Place, 990 Rama IV Road, Bangkok 10500, Thailand
Tel. +66 (0)2 636 0662 Fax. +66 (0)2 636 0663
www.lawplusltd.com