PERSONAL DATA PROTECTION LAW OF THAILAND
Data Transfer Limitation, Data Retention Limitation and Data Security Requirements

The Personal Data Protection Act B.E. 2562 ("**PDPA**") requires Data Controllers (**"Controllers"**) to comply with the personal data transfer limitation, have appropriate data security measures and comply with the limitation on personal data retention.

Transfer Limitation

Under Section 28 of the PDPA, Controllers are prohibited from transferring personal data to countries or international organizations which do not have adequate personal data protection standards, except for the transfers under 6 general exemptions and the inter-group transfer exemption. The general exemptions consist of the cross-border transfers: (1) for legal compliance; (2) with consent of the data subject; (3) as necessity for the data subject to comply with contractual obligations; (4) for compliance with contractual obligations of the Controller with other parties for the interest of the data subject; (5) to prevent harm to life, and (6) for major public interest.

The Inter-group transfer exemption is a situation where Controllers can transfer personal data to countries without adequate data protection standards if the data transfer policies of the Controllers have been reviewed and certified by the Personal Data Protection Committee (**"PDPC"**) or if Controllers have established appropriate measures for enforcing rights of data subjects with efficient remedial measures (Section 29 of the PDPA).

Security Requirements

Under Section 37(1) of the PDPA, Controllers are required to provide appropriate security measures against any unauthorized or unlawful loss, accession, use, alteration, correction or disclosure of personal data and review them when necessary. Such measures must meet the minimum requirements to be specified by the PDPC.

The PDPA does not define the "appropriate security measures" and the time for them to be reviewed. The size of the dataset, the sensitivity of data and the vulnerability of data subjects could be the key considerations. For example, intensive security measures could be deemed appropriate in a situation where the Controller collects, uses and discloses an extremely large amount of sensitive personal data such as political opinions, genetic data and criminal records.

Retention Limitation

Under Section 37(3) of the PDPA, Controllers cannot retain personal data forever. They must implement a system for personal data destruction when:

(1) the data retention period has expired;

(2) the data is no longer relevant;

(3) the data is in excess of the necessity pursuant its collection objectives;

(4) the data subject requests its destruction; or

(5) the data subject revokes his consent to the use or disclosure of his personal data.

The data retention limitation, however, does not apply if the data is retained for the public interest, public health, establishment/defense of legal claims and legal compliance. The PDPA links the retention limitation to the notice requirement, requiring Controllers to notify data subjects of the retention period when or before their personal data is collected. The PDPA does not prescribe any retention period for personal data, nor does it provide guidelines on when data is in "excess of the necessity" or when it becomes no longer relevant. Such guidelines will be given when the PDPA implementing regulations are enacted.

Risks of Non-Compliance

Violations against the transfer limitation can land the violator under an imprisonment term of up to 1 year and/or a fine not exceeding THB1,000,000 (Section 79 of the PDPA) and an administrative fine of up to THB5,000,000 (Sections 83 and 84 of the PDPA). Violations against the retention limitation and the security requirements are subject to an administrative fine of up to THB3,000,000 (Section 83 of the PDPA). In addition to these legal penalties, the violators could also suffer a severe reputational risk.

Measures to Mitigate Risks

To mitigate risks related to violations of Sections 28, 37(1) and 37(3) of the PDPA, businesses can:

(1) develop a system whereby personal data is destroyed when any of the events listed under Section 37(3) has occurred;

(2) ensure that all the data privacy notices specify a data retention period and conduct periodical data audits to ensure that personal data which is no longer necessary for its collection objective is destroyed;

(3) anonymize and aggregate personal data to keep the relevant insights without the associated personal data protection risks;

(4) if international transfers of personal data are to be made, seek expert legal advice on international data transfers;

(5) implement the minimum standards prescribed by the PDPC for personal data protection;

(6) have in place incident response plans, written information security programs and cyber security insurance.

Kowit Somwaiya
Managing Partner
kowit.somwaiya@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