Innovation Driven by Trust: Thailand's Personal Data Protection and Cyber Security Acts

As a country thought to be stuck in the “Middle Income Trap”, Thailand is innovating its way out. The kingdom is shifting away from a manufacturing based economy into one driven by innovation and technology through the Government’s ‘Thailand 4.0’ initiative. A cornerstone of Thailand 4.0 is the need to cultivate trust in consumers and investors about the stability, sustainability and safety of Thailand’s booming digital economy. To this end, the Personal Data Protection Act B.E. 2562 (“**PDPA**”) and Cyber Security Act B.E. 2562 (“**CSA**”) have been enacted and are effective (in full for the CSA and in part for the PDPA) as of 28 May 2019.

The CSA aims to secure national security in cyber-space through the protection of Information Infrastructures (“**II**”) which the CSA deems critical or important such as public/private databases, computer systems and networks. Where the CSA applies to the safety of the underlying infrastructure of the Digital Economy, the PDPA concerns itself with the rights and protection of data subjects. It mandates that the explicit consent of a data subject must be sought by those collecting personal data prior to collection, use or disclosure.

Cyber Security Act

The CSA establishes a number of bodies which discharge the duties under this law. In particular the National Cyber Security Committee (“**NCSC**”), the Cyber Security Governance Committee (“**NSGC**”), the Executive Committee of the Office of the Cyber Security Committee and the Office of the National Cyber Security Committee (“**ONCSC**”).

The CSA’s main impact is its focus on protecting the kingdom’s II from cyber security threats, thus ensuring the country’s economy is well protected from highly disruptive cyber-attacks. It accomplishes this by empowering the above mentioned Committees to perform key responsibilities such as drafting and enforcing standards frameworks, codes of conduct and risk assessment measures to ensure that Information Infrastructure Authorities (“**IIA**”), which manage IIs are adequately protected from any cyber security threats; and analyzing cyber security related situations and assess their impacts in order to prevent, handle and mitigate cyber security threats in the future.

The CSA defines II as any computer, or computer system used by either government of private entities for operations which are related to national security, safety, economic stability or are public interest infrastructures. This includes, but is not limited to, the provision of information infrastructure services in the following sectors: banking, IT/telecoms, energy and public utilities, transportation/logistics, and public health. For example, a cloud provider whose server hosts important financial information from the banking sector on their servers or hosts highly sensitive patient records must comply with the Kingdom’s new cyber security laws.

IIAs must comply with the four key requirements under the CSA as follows:

1. conduct cyber security risk assessments at least once a year and send a summary of said report to the ONCSC within 30 days of completion;

2. create and implement sector specific mechanisms, procedures and codes of conduct which must at least adhere to the codes of conduct issued by the CSGC to monitor cyber security threats and solve cyber security issues;

3. notify the ONCSC of the names and contact information of owners, possessors of the computer and the computer system's administrators; and

4. report cyber security threats to the ONCSC where cyber security threats occur (failure to do so may result in a fine of up to THB 200,000).

Personal Data Protection Act

The PDPA establishes a Personal Data Protection Commission ("**PDPC**") and the Office of the PDPC ("**OPDPC**") to ensure that Personal Data Controllers ("**Controllers**") (those who have the power to control the collection, use or disclosure of collected personal data) and Personal Data Processors ("**Processors**") (those who collect, use or discloses of personal data on behalf of a Personal Data Controller) comply with the PDPA. The PDPA is extra-territorial and applies to Controllers and Processors both within Thailand and abroad where the data collected, used or disclosed is of a data subject within Thailand.

Controllers and Processors must be aware of the following key principles of the PDPA:

1. explicit consent to collection, use or disclosure of personal data must be obtained from data subjects, by Controllers and Processors, subject to certain exceptions;

2. personal data may only be collected, used or disclosed for lawful purposes which have been notified to the data subject and no more;

3. Controllers must also inform data subjects of the types of persons or authorities which the collected personal data will be disclosed to, information about said Controller and the rights of a data subject (e.g. the right to access, make copies of, raise objections, request destruction of data or revoke consent for the use of their personal data);

4. Data Protection Officers must be appointed by Controllers where required;

5. Controllers and Processors must provide appropriate measures to protect and secure collected personal data; and

6. transfer of personal data to a foreign country or an international organization may only occur if such country or organization has a sufficient standard of personal data protection.

The PDPA also imports and adapts some concepts from the European Union's General Data Protection Regulation 2016/679 ("**GDPR**"). This includes concepts of data retention periods and data portability.

While the PDPA is now effective in part, its key provisions on data collection, use and disclosure, etc. are exempt from being effective until the 28th of May 2020 to allow businesses sufficient time to be fully prepared to comply with the PDPA. Prior to the 28th of May 2020, the PDPC will issue rules to implement the PDPA. Businesses in Thailand and abroad will need to monitor such rules and prepare themselves to fully comply with the PDPA and its implementation rules.

Download PDF

AUTHOR

Kowit Somwaiya
Managing Partner | **Bangkok**
kowit.somwaiya@lawplusltd.com

Jia Xiang Ang
Coordinator | **Bangkok**
jiaxiangang@lawplusltd.com

LawPlus Ltd.
Unit 1401, 14th Floor, Abdulrahim Place 990
Rama IV Road, Bangkok 10500, Thailand
Tel: +662 636 0662
Fax: +662 636 0663

LawPlus Myanmar Ltd.
Unit No. 520, 5th Floor, Hledan Centre
Corner of Pyay Road and Hledan Road, Kamayut Township,
Yangon, Myanmar

Tel: +95 (0)92 6111 7006
and +95 (0)92 6098 9752