
Thailand's New Data Protection Act

June 2019

In the near future, processing, collecting or using personal data will be prohibited unless explicitly permitted by its owner.

Draft Thailand Data Protection Act (the "Act") was approved by the National Legislative Assembly on 28 February 2019. The draft Act is expected to come into force one year after its publication in the Royal Government Gazette.

The Act substantially adopted the principles set forth in the European Union's General Data Protection Regulation (the "GDPR"), which has become effective since 25 May 2018. The GDPR intends to protect the rights of individuals and prevent breach of their data privacy. Under the GDPR, those who control personal data (the "Data Controller") must obtain clear and affirmative consent from the owner of the personal data (the "Data Subject") for its collection, use or possession. The GDPR, applies extraterritorial jurisdiction, meaning, whoever collects, possesses or uses the personal data of an EU citizen is bound to comply with the GDPR regardless of their location. Moreover, the GDPR also requires third countries, to which personal data is transmitted, to protect that data according to GDPR standards.

Key details of the Act are as follows:

Parties

- Data Subject – the individual who owns, and can be identified by, the data.
- Data Controller – the individual or juristic person who determines how to process, use or collect the data.
- Data Processor – the individual or juristic person who processes the data at the instruction of the Data Controller.

It is important to note that Data Controller can be both Data Controller and Data Processor.

Definition of Personal Data

Data that could, directly or indirectly, identify an individual, e.g. their name, email address, physical address, work history, health records, or biometric or criminal records.

Consent

In order for the personal data to be collected, used, processed or disclosed, the Data Controller must seek and obtain clear consent from Data Subject.

Request for consent must be explicit, obvious and must not mislead or deceive the Data Subject. Consent must be made in writing or via an electronic system.

Rights of Data Subject

- Right to be informed of the purpose of the data collection and use of the data and period of storage;
- Right to be informed of a breach of data privacy;
- Right to withdraw consent at any time; and
- Right to access to the data.

Responsibilities of Data Controller

- Obtain consent from Data Subject and inform the Data Subject purpose of the data collection and use of the data and period of storage;
- Appoint a qualified person to audit data protection compliance (so-called the "Data Protection Officer");
- Implement proper data protection measures;
- Inform Data Subject about the use or disclosure of personal data; and
- Inform Data Subject of any breach of the data.

Responsibilities of Data Processor

- Process, use, collect, store or disclose personal data according to the agreement between the Data Controller and Data Processor (The agreement must stipulate the rights and duties of the Data Processor);
- Procure a secured processing system;
- Appoint Data Protection Officer
- Inform the Data Controller of breach of the data

Transfer of Data to Third Country

The Data Controller can transfer personal data to a third country or an international organization, but such third country must adopt a sufficient level of data protection measures. Further, the personal data must be transferred in accordance with guidelines to be prescribed by the Personal Data Protection Committee.

Penalties

Violation of the Act could lead to:

- Civil penalties – compensation for damage to the Data Subject;
- Criminal penalties – fines up to Baht 1,000,000 or imprisonment up to 1 year or both
- Administrative penalties – fines of up to Baht 5,000,000

Long Arm of the Act

This Act will also apply to Data Controllers or Data Processors residing outside Thailand who collect, keep, use, process or disclose personal data of an individual who resides in Thailand. Meaning, those individuals or organizations who violate the Act outside Thailand will be subject to penalties under the Act.

Author's Note:



A company doing business in Thailand or a company located outside Thailand, and other organizations, that collect, possess or use personal data of individuals residing in Thailand must obtain the appropriate consent from the owners of the data.

Further, complying with GDPR alone is not sufficient, even though the Act has adopted key concepts from GDPR. The Act and the GDPR may slightly differ.

Your company or organization, whether located in or outside Thailand, that either does business or has a commercial interest in the Kingdom, should stay aware of this upcoming Act and should install sufficient data protection measures to avoid violations.

**By Mr. Piyasak Chotipruk, Partner and Ms. Kanyapatch Chankitvuth, Associate
Dherakupt International Law Office Ltd.*
