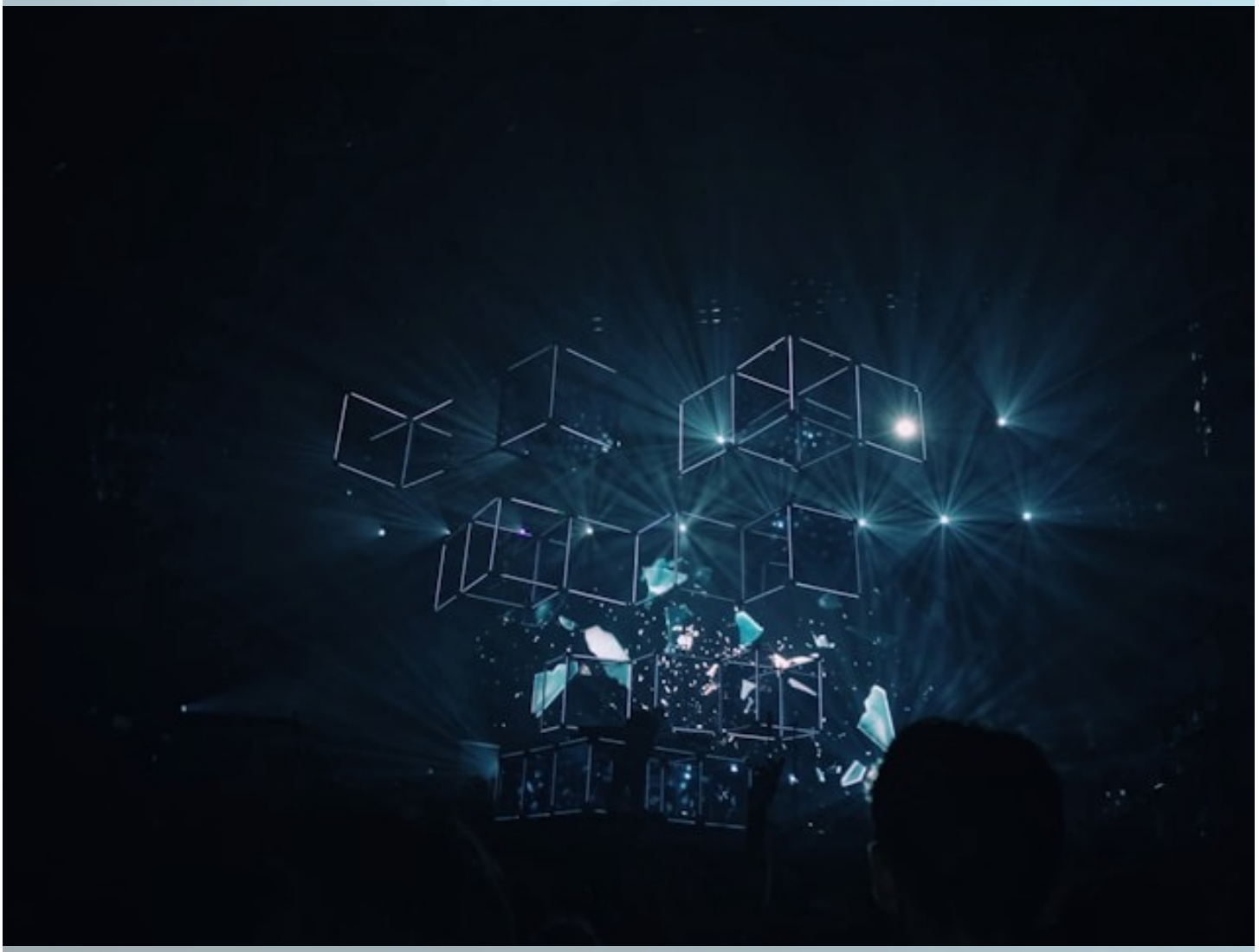
Overview of the Data Protection Act in Thailand

May 2023



IntelliSecure

Overview of the Data Protection Act in Thailand

This document provides a summary of the data protection legislation in Thailand, the Personal Data Protection Act (PDPA).

Background

Data privacy has become a critical issue for individuals and businesses worldwide as the digital age has made it increasingly easy to collect, store, and process personal data. Several countries have implemented comprehensive data protection laws in response to growing concerns over data protection and privacy.

In Thailand, the Personal Data Protection Act (PDPA) was enacted in 2019 and has been fully enforceable since June 2022.[ii]

The Personal Data Protection Committee (PDPC) is the regulatory authority responsible for regulating personal data and enforcing the PDPA.

Overview of the PDPA

The PDPA, Thailand's first comprehensive data protection legislation, is largely influenced by the European Union's General Data Protection Regulation (GDPR).

The PDPA's primary goal is to protect the personal data of individuals (referred to as “data subjects”) by regulating the collection, use, disclosure, and transfer (collectively, the “processing”) of personal data.

Further, “with the PDPA in place, Thai businesses can satisfy the EU’s strict requirements on data export measures under the Thailand-EU FTA,”[iii] thus expanding the reach of their businesses to Europe and beyond.

Currently, the PDPA does not have an official English translation.

Definitions

Nine (9) definitions are set out in the PDPA; these are listed in the table below.

Term	Definition
Personal data	"Any information relating to a Person that enables the identification of such Person, whether directly or indirectly, but not including the information of the deceased Persons in particular."[v]
Data Controller	"A Person or a juristic person having the power and duties to make decisions regarding the collection, use, or disclosure of the Personal Data."[vi]
Data Processor	"A Person or a juristic person who operates in relation to the collection, use, or disclosure of the Personal Data pursuant to the orders given by or on behalf of a Data Controller, whereby such Person or juristic person is not the Data Controller."[vii]
Person	"A natural person."[viii]
Committee	"The Personal Data Protection Committee (PDPC)."[ix]
Competent Official	"Any person appointed by the Minister to perform acts under this Act."[x]
Office	"Office of the Personal Data Protection Committee."[xi]
Secretary-General	"Secretary-General of the Personal Data Protection Committee."[xii]
Minister	"The Minster who is in charge under this act."[xiii]

Principles Relating to Use of Personal Data

There are several principles upon which the PDPA is based. These dictate that personal data must be:

1) accurate and up-to-date;

2) used or disclosed only when used for the purposes that have been stated by the company as consented by the data subject;

3) protected with the implementation of reasonable security arrangements that prevent risk and loss of data and

4) disposed of/deleted once: (a) data is no longer considered necessary for legal/business purposes, or (b) at the request of the data subject.

In addition, the Data Controller shall be responsible for and able to demonstrate compliance with the PDPA. The Data Controller holds the greatest responsibility for ensuring compliance with the PDPA.

Obligations of Data Controllers, Data Protection Officers, and Data Processors under the PDPA

Data Controller[xiv]

The Data Controller is responsible for the following activities:

1) provision and upkeep of appropriate security measures;

2) ensuring that personal data is handled lawfully;

3) establishing systems to handle personal data upon end of retention period or when personal data is irrelevant or redundant; and

4) notifying the PDPC regarding a personal data breach without delay, and within 72 hours.

Obligations of Data Controllers, Data Protection Officers, and Data Processors under the PDPA (cont.)

Data Protection Officer (DPO)

A DPO is required in the following circumstances:

1) a public authority carries out the processing of data;

2) the activities of the Data Controller or Data Processor require regular monitoring of the personal data or the system due to the large quantity of personal data and

3) the core activities of the Data Controller or the Data Processor is the collection, use, or disclosure of personal data according to section 26.[xv]

The DPO is responsible for the following activities:

1) to advise the Data Controller or the Data Processor on how to comply with the PDPA;

2) to review whether the processing of personal data by the Data Controller or the Data Processor complies with the PDPA;

3) to cooperate with the Office of the PDPC when there is any issue regarding the processing of personal data undertaken by the Data Controller or Data Processor and

4) to keep the confidentiality of personal data that becomes known or is received during his duties.

The DPO can either be an in-house resource or outsourced to an appropriate service provider.[xvi]

Obligations of Data Controllers, Data Protection Officers, and Data Processors under the PDPA (cont.)

Data Processor[xvii]

The Data Processor is responsible for the following activities:

1) carrying out activities according to the instructions given by the Data Controller;

2) providing appropriate security measures and notifying the Data Controller of any breach incidents; and

3) preparing and maintaining records of personal data processing activities according to the rules and methods set by the Committee.

Rights of Data Subjects Under the PDPA

The data subject has eight (8) rights that must be supported appropriately to ensure the required action is taken within the timescales as stated in the PDPA.

Eight Rights of Data Subjects		
Rights	Explanation	Timescale
Right to be informed[xviii]	The data subject has the right to be informed by the Data Controller regarding how their personal data is being collected and used.	Without undue delay
Right of Access[xix]	The data subject has the right to access data kept by the Data Controller and can request access to their personal data and to obtain a copy of it.	Within 30 days
Right to rectification[xx]	The Data Controller shall ensure that the personal data remains accurate, up-to-date, complete, and not misleading.	Without undue delay

Rights of Data Subjects Under the PDPA (cont.)

Eight Rights of Data Subjects (cont.)		
Rights	**Explanation**	**Timescale**
Right to erasure[xxi]	The data subject has the right to request the Data Controller to erase or destroy the personal data or anonymise the personal data such that the data subject is not identifiable under certain conditions.[xxii]	Undefined
Right to restrict processing[xxiii]	The data subject has the right to request for restriction of Data Controller's usage of personal data under certain conditions.[xxiv]	Undefined
Right to data portability[xxv]	The data subject has the right to obtain their personal data from the Data Controller in a format which is readable or commonly used by automated tools or equipment and could be used or disclosed via automatic means.	Undefined
Right to object[xxvi]	The data subject has the right to object to the usage of their personal data during certain circumstances.[xxvii]	Without undue delay upon successful objection request granted by the company
Right to complain to the Expert Committee[xxviii]	The data subject has the right to complain to the expert committee to order the Data Controller to take action.	Undefined

Consent[xxix]

Consent must be obtained from a data subject to collect and process their data.

In case of minors, the following requirements apply:

- Age 0 to <10 – parental consent is always required.
- Age 10 to <20 – parental consent is required if the minor is not competent to give consent.

Transfer of Personal Data

The PDPA requires Data Controllers to provide personal data to data subjects in a format that is (a) readable or usable by machines or equipment and (b) can be used or disclosed via automatic means.

Data subjects also have the right to (a) request the Data Controller to send or transfer his/her personal data to other Data Controllers and (b) obtain personal data in the same format sent by the Data Controller to other Data Controllers, except where it is not possible to do so for a technical reason.[xxx]

Transfers of personal data outside of Thailand must be carefully reviewed before the transfer takes place to ensure that they fall within the limits imposed by the PDPA – i.e., whether the receiving organisation can retain the same level of security as stated in the PDPA.[xxxi]



Breach Notification[xxxii]

Notification to the PDPC

Where a breach is known to have occurred, the PDPC is to be informed without delay and within 72 hours from the time that the Data Controller becomes aware of the breach, irrespective of the level of risk.

Notification to the PDPC is to be performed in writing or via electronic means as prescribed by the PDPC.[xxxiii]

Details to be provided within the notification to the PDPC must include the following:

1) brief information regarding the nature of the personal data breach, the data subjects affected, or the characteristics and records of personal data related to the data breach incident;

2) contact details of the DPO or the person coordinating the notification;

3) the possible impacts caused by the data breach, and

4) how will the Data Controller work to prevent, cease, or rectify the data breach or remedy the damage?[xxxiv]

Notification to the Affected Data Subjects

If the breach is likely to result in high risks to the rights and freedoms of the affected data subjects, they must be notified regarding the breach and remedial measures without undue delay.

Notification to the data subjects must be performed in writing or via electronic means addressed to each data subject. If not possible, a Data Controller may notify a group of data subjects (if not individually identifiable), via public media, social media, or any other means accessible to the data subjects.[xxxv]

Breach Notification (cont.)

Notification to the Affected Data Subjects (cont.)

Details to be provided within the notification to data subjects must include the following information:

1) brief information regarding the personal data breach;

2) information regarding the DPO or the person coordinating the notification;

3) the possible impacts the data breach may cause to the data subject;

4) approach taken to remedy any damages incurred by the data subject and measures to be taken by the Data Controller regarding the personal data breach.[xxxvi]

Fines

Under the PDPA, the Office of the PDPC can impose a range of fines of up to THB 3,000,000 upon failure to comply with the personal data breach notification.[xxxvii]

Assessment of Risk of the Personal Data Breach[xxxviii]

For an assessment of the risk that the Personal Data Breach poses in relation to the degree of impact on the rights and freedom of a person, the Data Controller may consider the following factors:

1) characteristics and category of the Personal Data Breach;

2) characteristics or category of personal data relating to the breach;

3) volume of personal data related to the breach, which may be considered from the number of data subjects or records of personal data relating to the breach;

Breach Notification (cont.)

Assessment of Risk of the Personal Data Breach (cont.)

4) characteristics, category, or status of the affected data subjects, as well as the fact whether or not the affected data subjects, including minors, disabled persons, incompetent persons, quasi-incompetent persons, or vulnerable persons, cannot protect the rights and benefits of themselves due to their limitations;

5) severity of the impact and damage that occurred or may occur to the data subject due to the Personal Data Breach, and the effectiveness of the measures that the Data Controller has taken or will take to prevent, cease, or rectify the Personal Data Breach, or remedy the damage, to alleviate the impact and damage that occurred or may occur to the data subject;

6) wide-ranging effects on the business or the operation of the Data Controller or the public due to the Personal Data Breach;

7) characteristics of the storage system of the personal data relating to the breach and relevant security measures of the Data Controller or the Data Processor, including organizational, technical, and physical measures; and

8) legal status of the Data Controller, such as whether it is a natural person or a juristic person, including the size and nature of the business of the Data Controller.[xxxix]

For further information, contact

Manish Chawda
contact@intellisecure.co

The material in this post represents general information only and should not be relied upon as legal advice. Nia Pte Ltd is not a law firm and may not act as an advocate or solicitor for purposes of the Singapore Legal Profession Act.

[i] For the official legislation, see https://ratchakitcha.soc.go.th/documents/17082307.pdf. There is no official English translation of the PDPA.

[ii] See https://www.trade.gov/market-intelligence/thailand-personal-data-protection-act#:~:text=Thailand%27s%20Personal%20Data%20Protection%20Act,fully%20enforceable%20in%20June%202022.

[iii] See https://www.aseanbriefing.com/news/thailand-issues-first-personal-data-protection-act/.

[iv] This document uses the following unofficial English translation: https://cyrilla.org/entity/sl9175g71u?file=15887704957529yl1t08r6ge.pdf&page=1.

[v] Local language definition: ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งท าให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ. See section 6 of the PDPA.

[vi] Local language definition provided here: "ผู้ควบคุมข้อมูลส่วนบุคคล" หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอ านาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล. See section 6 of the PDPA.

[vii] Local language definition: ผู้ประมวลผลข้อมูลส่วนบุคคล" หมายความว่า บุคคลหรือนิติบุคคลซึ่งด าเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามค าสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งด าเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล. See section 6 of the PDPA.

[viii] Local language definition: "บุคคล" หมายความว่า บุคคลธรรมดา. See section 6 of the PDPA.

[ix] Local language definition: "คณะกรรมการ" หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. See section 6 of the PDPA.

[x] Local language definition: "พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้. See section 6 of the PDPA.

[xi] Local language definition: "ส านักงาน" หมายความว่า ส านักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. See section 6 of the PDPA.

[xii] Local language definition: "พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้. See section 6 of the PDPA.

[xiii] Local language definition: "รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัติน. See section 6 of the PDPA.

[xiv] See section 37 of the PDPA.

[xv] See section 41of the PDPA.

[xvi] See section 42 of the PDPA.

[xvii] See section 40 of the PDPA.

[xviii] See section 23 of the PDPA.

[xix] See section 30 of the PDPA.

[xx] See section 35 of the PDPA.

[xxi] See section 33 of the PDPA.

[xxii] The conditions applicable for when data can be erased, destroyed or anonymised are:

(1) the personal data is no longer necessary in relation to the purposes for which it was collected, used or disclosed;

(2) the data subject withdraws consent on which the collection, use, or disclosure is based on, and where the Data Controller has no legal ground for such collection, use, or disclosure;

(3) the data subject objects to the collection, use, or disclosure of the personal data referred in Section 32 (1), and the Data Controller cannot reject to such request as referred in section 32 (1) (a) or (b), or where the data subject exercise his or her right to object as referred in section 32 (2);

(4) the personal data have been unlawfully collected, used, or disclosed under this Chapter. See section 33 of the PDPA.

[xxiii] See section 34 of the PDPA.

[xxiv] The conditions for when the data subject may exercise this right are:

(1) when the Data Controller is pending examination process in accordance with the data subject's request pursuant to section 36;

(2) when it is the personal data which shall be erased or destroyed pursuant to section 33 (4), but the data subject requests the restriction of the use of such personal data instead;

(3) when it is no longer necessary to retain such personal data for the purposes of such collection, but the data subject has necessity to request the retention for the purposes of the establishment, compliance, or exercise of legal claims, or the defence of legal claims;

(4) when the Data Controller is pending verification with regard to section 32 (1), or pending examination with regard to section 32 (3) in order to reject the objection request made by the data subject in accordance with section 32 paragraph three. See section 34 of the PDPA.

[xxv] See section 31 of the PDPA for more detail.

[xxvi] See section 32 of the PDPA.

[xxvii] These circumstances include:

(1) Where the personal data is collected with the exemption to consent requirements under section 24 (4) or (5), unless the Data Controller can prove that:

(a) the collection, use, or disclosure of such personal data can be demonstrated by the Data Controller that there is a compelling legitimate ground;

(b) the collection, use, or disclosure of such personal data is carried out for the establishment, compliance or exercise of legal claims, or defence of legal claims;

(2) the collection, use, or disclosure of such personal data is for the purpose of direct marketing;

(3) the collection, use, or disclosure of the personal data for the purpose of scientific, historical or statistic research, unless it is necessary to performance of a task carried out for reasons of public interest by the Data Controller. See section 32 of the PDPA.

[xxviii] See section 33 and section 34 of the PDPA.

[xxix] See section 20 of the PDPA.

[xxx] Organisations receiving personal data must have adequate data protection standard in accordance with the rules for the protection of personal data as prescribed by the Committee except if:

- Transfer is made pursuant to applicable laws;
- Data subject is informed of the inadequate personal data protection measures of the organisation but still provides consent;
- Transfer is necessary to complete the contract where the data subject is a party, or to complete tasks as requested by the data subject prior to entering a contract;
- Transfer is for compliance with a contract between the organisation and other persons for the interests of the data subject;
- Transfer is to prevent or suppress a danger to the life, body, or health of the data subject or other persons, when the data subject is incapable of giving the consent at such time; or
- Transfer is necessary for carrying out the activities in relation to substantial public interest.

[xxxi] See section 28 of the PDPA.

[xxxii] See https://ratchakitcha.soc.go.th/documents/17233460.pdf for the official legislation of the Notification on the Criteria and Procedures for Handling Personal Data Breaches (the 'Notification'). There is no official English translation.

For an unofficial English translation, see https://hsfnotes.com/data/2022/12/21/pdpa-update-thailands-new-legislation-on-personal-data-breach-notification/ and https://www.noandt.com/en/publications/publication20230203-1/.

[xxxiii] See clause 6 of the Notification.

[xxxiv] See clause 6 of the Notification.

[xxxv] See clause 11 of the Notification.

[xxxvi] Approach to remedy the damage incurred by the data subject and brief information related to measures taken or will be taken by the Data Controller to prevent, cease, or rectify the Personal Data Breach – measures in respect of personnel, processes, or technology, or any other measures, including recommendations related to measures that the data subject may additionally take to prevent, cease, or rectify the Personal Data Breach, or remedy the damage incurred. See clause 10 of the Notification.

[xxxvii] See section 83 of the PDPA.

[xxxviii] See https://www.dataguidance.com/sites/default/files/khuumuueaenwthaangkaarpraeminkhwaamesiiyngaelaaecchngehtukaarlaemidkhmuulswnbukhkhl_v-1-0.pdf for the official legislation of the Guidelines on Data Breach Assessments and Personal Data Breach Notifications ("Guidelines"). The first seven pages cover the standard required for a breach notification to be notifiable. There is no official English translation.

[xxxix] See clause 12 of the Notification.