Luther.

Memo: Personal Data Protection in Thailand

November 2025

unyer GLOBAL ADVISORS

Content

A. Introduction

On 27 May 2019, the Personal Data Protection Act, B.E. 2562 (2019) ("**PDPA**") was published in the Thai Government Gazette. Thailand's first consolidated data protection law, which is largely based on the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"), was initially planned to come into effect on 27 May 2020. Due to the COVID-19 pandemic and resulting economic challenges, it only became fully enforceable in June 2022.

Since 2022, the Personal Data Protection Committee ("**PDPC**") has issued several notifications and guidelines related to security measures, maintenance of records, complaints, fines, consent, data breach notification, appointment of a Data Protection Officer ("**DPO**"), cross-border transfer, and data deletion or destruction.

The PDPA aims to guarantee protection for individuals and their personal data, and imposes a number of obligations on businesses when processing personal data.

The first part of this brochure (B.) is to provide you with an overview on the Thai data protection regime. It may serve as an initial check-up for whether your organisation has implemented the necessary rules and policies to comply with the legislation on personal data protection. In the second part (c.) we will explain in more detail how Luther Law Firm (Thailand) Ltd can assist you in complying with your PDPA related obligations.

Nevertheless, there are some key differences between the PDPA and the GDPR. In particular, unlike the GDPR, the PDPA does not apply to certain public authorities, and the definition of "personal data" in the GDPR is much more detailed, as it specifically includes IP addresses and cookie identifiers, whilst there is no mention of these in the PDPA.

B. The Personal Data Protection Act

The PDPA applies to all organisations carrying out activities involving personal data in Thailand, irrespective of whether being registered in Thailand or not. Where personal data is collected overseas and subsequently transferred into Thailand, the provisions of the PDPA will apply in respect of the activities involving personal data in Thailand.

1. Scope

The PDPA protects (living) natural persons within Thailand with regard to the collection, use, or disclosure (collectively, "**processing**") of their personal data and applies to both Data Controllers and Data Processors. It makes no explicit reference to nationality or place of residence in relation to the processing of personal data.

The PDPA applies to the processing of personal data by organisations that are in Thailand regardless of whether the processing of personal data takes place in Thailand or not. It also applies to Data Controllers and Data Processors that are outside of Thailand if their processing of personal data involves data subjects who are in Thailand. This includes cases where their activities relate to the offering of goods or services to data subjects in Thailand, regardless of whether payment is required, or where the data subject's behaviour is being monitored in Thailand[1].

The PDPA does not apply to :

- the processing of personal data by a person who collects such personal data for personal benefit or household activity of such person only;
- the operations of public authorities having the duties to maintain state security, including financial security, security of the state or public safety, including the duties with respect to the prevention and suppression of money laundering, forensic science or cybersecurity;
- a person or a juristic person who uses or discloses personal data that is collected only for the activities of mass media, fine arts, or literature, which are only in accordance with professional ethics or for public interest;
- the operations of a credit bureau company and its members according to the law governing the operations of a credit bureau business; and
- Thai legislative bodies, specific government institutions and judiciary authorities[2].

1 Sec. 5 PDPA
2 Sec. 4 PDPA

2. Definitions

- The PDPA defines Personal Data as *"any information relating to a person, which enables the identification of such person, whether directly or indirectly, but not including information of the deceased persons."* Unlike the GDPR, the PDPA does not define special categories of personal data. But it however requires that explicit consent be obtained for the collection of *"personal data pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner, as prescribed by the Committee."*[3]

The PDPA defines a Data Controller as *"a person or a juristic person who has the power and duties to make decisions regarding the collection, use, or disclosure of Personal Data."*

- A Data Processor is *"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."*[4]

The PDPC defines a Small Organization as:

- Small or medium enterprises according to the law on small and medium-sized enterprise promotion;
- Community enterprises and networks of community enterprises registered under the community enterprise promotion law;
- Social enterprises and social enterprise groups registered under the social enterprise promotion law;
- Cooperatives, cooperative federations, or a farmer's groups under the cooperatives law;
- Foundations, associations, religious or non-profit organizations;
- Condominium associations under the law governing condominiums or housing estate entities under the law governing housing estates;
- Family businesses or other similar businesses;
- Sole businesses operated by individual Data Controllers and Data Processors[5].

3 Sec. 26 PDPA
4 Sec. 6 PDPA
5 Notification: PDPC re Exemption to the Record of Processing Activities Requirement for Data Controllers that Are Small Businesses B.E. 2567 (8 January 2025) and Notification: PDPC re Exemption to the Record of Processing Activities Requirement for Data Processors that Are Small Businesses B.E. 2567 (8 January 2025)

3. Regulatory authority

The PDPC is the government agency responsible for overseeing and enforcing the PDPA, as well as drafting and issuing future sub-regulations and guidelines under the PDPA.

The PDPC can set up expert committees to receive and investigate complaints and settle disputes. The PDPC can issue orders to Data Controllers and Data Processors.

4. Collection, use and disclosure of personal data

The PDPA also provides that the collection of personal data shall be limited to the extent necessary in relation to the lawful purpose of the Data Controller.[6]

The Data Controller shall not process Personal Data without an appropriate legal basis. For processing Personal Data, the PDPA requires one of the following as a legal basis:[7].

- Prior consent[8];
- When processing is necessary for the performance of a contract[9];
- Necessary for compliance with a law to which the Data Controller is subjected[10];
- For supressing danger to a data subject's life[11];
- For the performance of a task carried out in the public interest by the Data Controller or in the exercise of official authority vested in the Data Controller[12];
- For the achievement of the purpose relating to historical documents or archives for public interest, or for the purpose relating to research and statistics[13]; or
- For the legitimate interest of the Data Controller where such interest does not override those of the data subject[14]

The PDPA recognises consent as a legal basis to process personal data, and includes specific information on how consent can be obtained and withdrawn.

The PDPA states that any collection of special categories personal data relating to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic information, biometric data, or any data which may affect the data subject in the same manner is prohibited without explicit consent of the data subject, except where one of the following exemptions applies:[15]

- Vital interests of the data subjects who are unable to provide consent;
- Non-profit organizations;
- Personal data was made public by the data subject;
- Legal claims or judicial acts;
- For legal compliance in the areas of (1) preventive or occupational medicine, (2) public interest in public health, (3) employment protection, social security, national health security, and social health welfare, (4) the scientific, historical, or statistics research, and (5) substantial public interests.

The PDPA imposes that the collection of personal data must be limited to the extend necessary in relation with one of the above purpose[16].

5. Rights of data subjects

The PDPA provides for the following rights of the data subjects:

5.1. A. Right to erasure

Unless exceptions apply, the PDPA allows data subjects to request for their personal information to be deleted[17]. This right to erasure applies where the consent of a data subject is withdrawn and the Data Controller has no legal ground to process the personal data, or the personal data is no longer necessary for the purpose of which it was collected.

The right can be exercised free of charge. The Data Controller must be responsible for all costs.

The Data Controller must inform data subjects of the right to request for their personal data to be deleted[18].

Exceptions to the right of erasure include:

- Freedom of expression and freedom of expressing opinion;
- Complying with legal obligations to achieve a purpose of public interest in the areas of public health or preventive or occupational medicine;

6 Sec. 22 PDPA
7 Sec. 24 PDPA
8 Sec. 24 PDPA
9 Sec. 24 (3) PDPA
10 Sec. 24 (6) PDPA
11 Sec. 24 (2) PDPA
12 Sec. 24 (4) PDPA
13 Sec. 24 (1) PDPA
14 Sec. 24 (5) PDPA
15 Sec. 26 PDPA
16 Sec. 22 PDPA
17 Sec. 33 PDPA
18 Sec. 23 PDPA

- The data processing for the purpose of preparation of historical archives, or educational research and statistics, subject to sufficient protective measures to protect personal data;
- Establishment, exercise, compliance with, or defence of, legal claims; and
- Complying with legal obligations for a public interest purpose.

The Data Controller must process the data subject's request within 90 days from the date of receipt. The data deletion or destruction must also include any copies or backups of personal data. If the Data Controller cannot fulfill the request within the 90-day period, it must take measures to ensure that the personal data is made difficult to process until the personal data can be deleted, destroyed, or de-identified. In such cases, appropriate organizational, technical, and physical measures must be implemented to protect the data, meeting the criteria set forth by the PDPC[19]. In addition, the PDPA gives data subjects the right to lodge a complaint with the relevant authority if the data controller fails to respond to the request for deletion.

5.2. B. Right to be informed

The PDPA recognise the transparency principle. It imposes an obligation on a Data Controller to inform data subjects of specific information relating to the collection and processing of personal data. However, the PDPA does not explicitly specify in what form the right can be exercised.

Data subjects must be provided with information relating to the processing of personal data in order to validate their consent.

The PDPA states that information that must be provided to data subjects includes:

- details of personal data to be collected, used or disclosed;
- purposes of collection for use or disclosure of the personal data, including the legal basis for the collection (no consent required);
- data subjects' rights (e.g., the right to erasure, right to object, right of withdrawal, etc.);
- data retention period;
- categories or entities, either as an individual or organisation, that the personal data will be disclosed to; and
- contact details of the Data Controller or its representative and the DPO.[20]

A Data Controller is obligated to inform data subjects of the possible consequences of the withdrawal of consent.[21]

Data subjects must be informed of the purpose of the processing of their personal data in an easily accessible form with clear and plain language, which can be in writing or electronic format, to obtain the data subjects' consent.[22]

Such notification may be provided in writing, such as by letter, SMS, email, or MMS, or may be delivered via a URL link or a QR code.[23]

Data subject(s) must be informed of any change to the original processing purpose.[24]

A Data Controller must inform data subjects of inadequate privacy safeguards of a third country or international organisation to which their personal data will be transferred to for their consent to the proposed transfer.[25]

The PDPA prescribes that a Data Controller must provide specific information to data subjects when their personal data is collected from a third party, which includes the source from which the data was collected for their consent.

In the case of indirect collection. The Data Controller must provide information relating to such collection to data subjects within a reasonable period, but at the latest within 30 days from the date of collection, or at the time of the first communication with the data subject, or when personal data are is first disclosed to the recipient.[26]

The PDPA does not provide examples of legitimate interest circumstances.

19 Notification: PDPC re the Criteria for Data Deletion, Destruction, or Anonymisation B.E. 2567 (13 August 2024)

20 Sec. 29 PDPA
21 Sec. 19 PDPA
22 Sec. 19 PDPA
23 Guidelines on Procedures for Notifying the Purpose and Details relating to the Collection of Personal Data from Data Subjects under the Personal Data Protection Act. 2562
24 Sec. 21 PDPA
25 Sec. 28 PDPA
26 Sec. 25 PDPA

5.3. C. Right to object

The PDPA guarantees the right for data subjects to object[27] to the processing of their personal data as well as to withdraw their consent to the processing at any time.

A Data Controller can make an objection to the request of data subjects, and continue to collect, use, and disclose their personal data based on two grounds:

- the controller can demonstrate that the collection, use, and disclosure of personal data is based on a legitimate ground that overrides the data subjects' interests; or
- the collection, use, and disclosure of personal data has the purpose of establishing, exercising, or defending against a legal claim.[28]

The PDPA does not explicitly specify whether a Data Controller has an obligation to provide information to data subjects on how to exercise the right.

The PDPA does not specify a timeline for a Data Controller to respond to a request to restrict the processing of personal data. However, the PDPA provides a right to data subjects to make a complaint to a relevant authority in case the Data Controller fails to respond to the request of objection

5.4. D. Right to access

Under the PDPA, data subjects have the right to request access and obtain a copy of their personal data that is processed by a data controller.[29]

Under the PDPA, the right to access personal data and request a copy of such data must not adversely affect the rights or freedoms of others. The PDPA does not prescribe what needs to be included in responding to an access request.

A Data Controller is allowed to refuse a request to access personal data, including obtaining a copy and/or source of personal data, only in the case where the refusal complies with law or a court order. Under the PDPA, there is no exception for those related to trade secrets.

A Data Controller must respond to the request without undue delay, and within a maximum of 30 days upon the receipt of the request with no extension period.

27 Sec. 32 PDPA
28 Sec. 32 (1) PDPA
29 Sec. 30 PDPA

The copy of the personal data must be provided to the data subject in a format which is readable and commonly used.[30]

Notification(s) from the relevant authority relating to the exercise of rights as well as an extension period may be published in the future.[31]

The PDPA does not specify whether the exercise of this right is free of charge.

The PDPA does not address the means for data subjects to make a request to access their personal data.

5.5. E. Right to data portability

The PDPA recognises the right to data portability. Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format as well as to transmit such data to other third parties.[32]

The Data Controller has an obligation to record the ground of objection to a data portability request for the verification of data subjects and the competent authority.

5.6. F. Right to file a complaint

Data subjects lodge a complaint with the PDPC if Data Controllers or Data Processors, including their employees or service providers violate or fail to comply with the PDPA.

6. Obligations of Data Controllers and Data Processors

The PDPA sets out a number of responsibilities for Data Controllers and Data Processors, including definitions and obligations relating to compliance with data subjects' rights, breach notification, record keeping, security measures and the appointment of a DPO. Data Controllers must ensure that personal data remains accurate, up-to-date, complete, and not misleading[33]. Data Controllers must implement appropriate security measures and notify supervisory authorities of data breaches.[34] The PDPA does not specifically provide for Data Protection Impact Assessments ("**DPIAs**") in certain circumstances, but outlines that Data Controllers have a duty to provide appropriate security measures and review them

30 Sec. 31 PDPA
31 Sec. 30 PDPA
32 Sec. 31 PDPA
33 Sec. 35 PDPA
34 Sec. 37 PDPA

when it is necessary, or when the technology has changed in order to effectively maintain the appropriate security and safety standards.[35]

Data Controllers based outside Thailand and involved in certain forms of data processing, are obliged to designate a representative based within Thailand in writing.[36]

The PDPA requires Data Controllers and Data Processors to keep records of processing activities and provides an exemption from this requirement for small organisations[37]. It also provides for the appointment of DPOs by Data Controllers or Data Processors.

The PDPA provides that where "is to be provided to other Persons or legal persons, apart from the Data Controller, the Data Controller shall take action to prevent such person from using or disclosing such Personal Data unlawfully or without authorization".[38]

Data Controllers are obliged to set up a system of checks for erasure or destruction of personal data when necessary to comply with retention periods, when the data subject withdraws consent, etc.[39]

6.1. Data transfers

The PDPA allows the transfer of personal data outside Thailand only by the following legal mechanisms:

1. If the recipient country or international organisation has adequate standards of protection for personal data and the transfer is in accordance with the rules prescribed by the PDPC.[40]
2. These include the existence of legal measures aligned with Thailand's data protection laws, obligations on data controllers regarding security and data subjects' rights, and the existence of a regulatory authority. The Office of the PDPC has the power to refer cases for adjudication, and the PDPC has the discretion to make decisions on a case-by-case basis or to establish a list of countries with adequate data protection standards.[41]
3. In the absence of the PDPC decisions or the list of countries, cross-border transfer is permitted under the following legal grounds:

   - where the consent of the data subject has been obtained;
   - it is necessary to perform an obligation under a contract where the data subject is the contracting party or the transfer is at the request of a data subject;
   - it is necessary to perform an obligation under a contract between the Data Controller and other persons for the interests of the data subjects;
   - it is performed for significant public interest;
   - the transfer is pursuant to the law; and
   - where it 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 their consent.[42]

4. For cross-border transfer to a company that is within the same affiliated business or in the same group of undertakings, the data transferor must prepare establish the binding corporate rules (the "**BCR**") as approved by the PDPC[43]. The BCR must adhere to the following minimum standards:

   - The BCR must be legally binding on, apply to, and be enforced by every member concerned of the same affiliated business or within the same group of undertakings, whether a juristic person or a natural person, including the data processor, the data transferor, and the data transferee, as well as their employees, staff, or persons involved in the transfer or receipt of personal data within the group;
   - The BCR must contain a clause concerning the data subject's rights and complaints for the cross-border transfer;
   - The BCR must contain measures for personal data protection and the minimum standards of the security measures.[44]

5. In the absence of a certified BCR, the data transferor must provide appropriate safeguards that enable the enforcement of the data subject's rights, including effective legal remedial measures according to the regulations issued by the PDPC. The appropriate safeguards must adhere to the

35 Sec. 37 (1) PDPA
36 Sec. 37 (5) PDPA
37 Sec. 39 and 40 (3) PDPA
38 Sec. 37 (2) PDPA
39 Sec. 37 (3) PDPA
40 Sec. 28 PDPA
41 Clause 6 of Notification : PDPC re the Criteria on the Protection of Personal Data transferred to Foreign Countries pursuant to Section 28 of the PDPA B.E. 2566 (25 December 2023)
42 Sec. 28 (1) – (6) PDPA
43 Sec. 29 PDPA
44 Clause 7 of Notification : PDPC re the Criteria on the Protection of Personal Data transferred to Foreign Countries pursuant to Section 29 of the PDPA B.E. 2566 (25 December 2023)

same minimum standards as the BCR. The appropriate safeguards may be in one of the following forms:

- The standard contractual clauses (the "**SCC**") regarding data protection in relation to the cross-border transfer or the transfer of personal data between countries, as specified by the PDPC for the data transferor and data transferee to define the duties and conditions of the contractual parties, to ensure appropriate measures for the protection of personal data;
- Certification regarding the collection, use, and disclosure of personal data by the data controller or data processor in relation to the cross-border transfer of personal data or transfer of personal data between countries. This certification confirms the presence of appropriate measures for the protection of personal data, in accordance with recognized standards;
- Statutes or agreements that are legally binding and enforceable between the government agencies of Thailand and other countries in the case of the transfer of personal data between each other[45].

6.2. Data processing records

Both the GDPR and the PDPA have imposed an obligation on Data Controllers and Data Processors to record their processing activities. In both laws, this obligation also applies to the representative of a Data Controller and the lists of information that must be retained bear many similarities.

Data Controllers and Data Processors are required to maintain a record of their personal data processing activities.

The PDPA prescribes the specific information that a Data Controller must record for the verification of data subjects and the competent authority, which includes[46]:

- the information of the data controller;
- the purposes of the collection;
- the collected personal data;
- the rights and means to access the data subjects' personal data, including conditions of access and person(s) authorised to access such data;
- the retention period of the personal data;
- use and disclosure of personal data collected without the consent of the data subject under sec. 27;
- the rejections or objections to the requests of the data subjects rights; and
- the details of the security measures.[47]

The processing of information of a Data Controller can be recorded in **writing or electronic form**.[48]

Data Controllers located outside Thailand and involved in certain forms of data processing are required to designate in writing a representative located in Thailand. The local representative of the Data Controller is required to carry out activities on behalf of the Data Controller, including recording its processing activities in the same manner as the Data Controller.

The data processing records requirements do not apply to a Small Organisation unless the processing is:

- is likely to result in a risk to the rights and freedoms of data subjects;
- is not occasional; or
- involves special categories of data in Section 26 (e.g. data concerning religious beliefs, ethnic origin, data necessary for the establishment, exercise or defence of legal claims, etc.).

The PDPA does not specifically provide for Data Protection Impact Assessments ("**DPIAs**") in certain circumstances, but outlines that Data Controllers have a duty to provide appropriate security measures and review them when it is necessary, or when the technology has changed in order to effectively maintain the appropriate security and safety standards[49].

6.3. Appointment of a DPO

The PDPA requires Data Controllers and Data Processors, including their representatives, to designate a DPO in the following circumstance[50]:

- the Data Controller or the Data Processor is a public authority or body as prescribed by the PDPA;
- the activities of a Data Controller or Data Processor relating to a data processing that require regular monitoring of the personal data or the system due to the large number of personal data collected; or

45 Clause 8 of Notification : PDPC re the Criteria on the Protection of Personal Data transferred to Foreign Countries pursuant to Section 29 of the PDPA B.E. 2566 (25 December 2023)
46 Sec. 39 PDPA
47 Sec. 39 PDPA
48 Sec. 39 (1) PDPA
49 Sec. 37 (1) PDPA
50 Sec. 41 PDPA

- the core activities of a Data Controller or Data Processor relate to the processing of certain categories of data in Section 26 of the PDPA (e.g. racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner, as prescribed by the PDPC).

Where a Data Controller and a Data Processor are part of the same company, a single DPO may be appointed, provided that the DPO is easily accessible to both the Data Controller and the Data Processor. The appointment of a single DPO is also permitted for public authorities or bodies (which are the Data Controllers or Data Processors) that have a large organisational structure or several establishments.

The scope of the DPO's duties are[51]:

- to inform and advise the data controller, and the data processor, their employees and service providers on obligations under the PDPA;
- to monitor the performance of the Data Controller or the Data Processor including their employees or service providers, with respect to the collection, use or disclosure of personal data;
- to act as a contact point for Data Controllers and Data Processors; and
- to keep all personal data known or acquired in the course of its performance confidential.

The appointment of the DPO must be considered based on expert knowledge and expertise in personal data protection, which may be further specified by the PDPC.

An employee of a Data Controller or Data Processor or a contractor may be appointed as the DPO.

Data subjects and the PDPC must be informed of the contact details of the DPO.

Data subjects may contact the DPO with regard to the processing of personal data, including the exercise of their rights.

The Data Controller and Data Processor must provide the necessary resources as well as aid in the facilitation of the DPO's tasks under the PDPA.

The PDPA does not explicitly comment on the independence of DPOs, but the Data Controller or the Data Processor should not terminate the employment of the DPO by the reason that it performs its duties under the PDPA. The DPO must be able to report directly to the highest level of management of the Data Controller or data processor.

6.4. Data security and data breaches

The PDPA requires Data Controllers and Data Processors to implement security measures in order to prevent the loss, access, use, change, revision, or disclosure of personal data without authorisation.[52]

In addition, the PDPA imposes an obligation on Data Controllers to notify the PDPC of any personal data breaches, without undue delay and, where feasible, no later than 72 hours after having become aware of the breach.[53] The information that must notify the PDPC is the following:

- details about the personal data breach;
- contact details of the Data Protection Officer (DPO) or a person designated by the Data Controller;
- likely consequences of the personal data breach; and
- preventive or corrective measures for the personal data breach, preliminary remedies for damages in terms of personnel, process, technology, or any other appropriate measures.

A breach is the unauthorised access, loss, use, modification or disclosure of personal data through intentional, wilful, negligent, accidental, unauthorised or unlawful acts.[54]

Under the PDPA, if a personal data breach is likely to result in a high risk to data subjects' rights and freedoms, the Data Controller must notify the breach to data subjects.[55]

51 Sec. 42 PDPA

52 Sec 37 (1)
53 Sec. 37 (4)
54 Clause 3 of Notification: PDPC re Security Standard of Personal Data of the Personal Data Controller (20 June 2022)
55 Sec 37 (4)

7. Sanctions and penalties

7.1. Civil liability

Data subjects lodge a complaint with the PDPC if Data Controllers or Data Processors, including their employees or service providers violate or fail to comply with the PDPA.

In the event that the operations of a Data Controller or a Data Processor violate or fail to comply with the PDPA and cause damages to a data subject, the Data Controller or the Data Processor should compensate such damages, regardless of whether such operation is performed intentionally or negligently, except where the Data Controller or the Data Processor can prove that such operation was a result of:

- a force majeure, or the data subject's own act or omission to act; or
- an action taken in compliance with an order of a government official exercising its duties and power under the law.

Compensation should include all necessary expenses incurred by the data subject to prevent the damage likely to occur or to remedy the damage that has occurred.

In addition, the civil court may order data controllers and data processors to pay punitive damages not exceeding twice the amount of compensation.

Claims for damages for breach of the PDPA are subject to a limitation period of 3 years from the date on which the data subject becomes aware of the damage and the identity of the Data Controller or Data Processor to be held liable, or 10 years from the date on which the unlawful act in respect of the personal data took place.

7.2. Administrative liability

The PDPC and its expert committee(s) have investigative and corrective powers.

The expert committee(s) have authority to:

- order Data Controller or Data Processor to comply with their obligations under the PDPA within a prescribed period;
- to prevent Data Controller or Data Processor from carrying out activities that cause harm to data subjects within a prescribed period;
- request documents or information relating to data protection under the PDPA; and
- make an application to the competent court for an order authorising the competent officer to enter the premises of the Data Controller or any person involved in the offence, to investigate and gather facts and to seize documents, evidence or other items relating to the offence.

The PDPA provides that the expert committee(s) may issue a warning before imposing a fine, and in determining whether to impose an administrative fine, the expert committee shall take into account the seriousness of the circumstances of the offence, the size of the organisation, and any other circumstances prescribed by the PDPC.

The PDPA does not expressly provide the expert committee(s) with the authority to conduct data protection audits, review issued certifications, or notify the controller or processor of an alleged breach under the PDPA.

The PDPA does not explicitly address whether a supervisory authority must act in complete independence in carrying out its duties.

Depending on the offence, administrative fines under the PDPA range from a maximum of THB 500,000 to a maximum of THB 5 million.

7.3. Criminal liability

If a Data Controller violates the provisions of Sections 27 (disclosure without a legal basis) or 28 (cross-data transfer) of the PDPA with respect to special categories of data listed under Section 26 (e.g., data concerning religious beliefs, ethnic origin, data necessary for the establishment, exercise or defence of legal claims, etc.) and in a manner that is likely to cause harm to another person, to impair his or her reputation, or to expose him or her to hatred, contempt or degradation, the Data Controller may be punished with imprisonment for a term not exceeding 6 months, or a fine not exceeding THB 500,000, or both.

If a Data Controller violates the provisions of Sections 27 (disclosure without a legal basis) or 28 (cross-data transfer) of the PDPA with respect to special categories of data listed under Section 26 (e.g., data concerning religious beliefs, ethnic origin, data necessary for the establishment, exercise or defence of legal claims, etc.) in order to unlawfully benefit himself or herself or another person, he or she shall be punished with imprisonment for a term not exceeding 1 year, or a fine not exceeding THB 1 million, or both.

Any person who comes to know the personal data of another person as a result of performing duties under the PDPA and discloses it to another person shall be punished with imprisonment for a term not exceeding 6 months, or a fine not exceeding THB 500,000, or both, unless the disclosure happened:

- in the performance duty;
- to the benefit of an investigation or legal proceeding;
- to a domestic or foreign government agency authorized by law;
- where the data subject's written consent has been obtained for that specific occasion; or
- in connection with legal proceedings disclosed to the public.

In the event that the Data Controller is a juristic person, and the offence is committed as a result of the instructions given by or the act of a director, manager or person responsible for the act of the juristic person, or if such a person has a duty to give an instruction or carry out an act but fails to give such an instruction or carry out such an act until the legal person has committed the offence, such a person shall also be punished with the penalty prescribed for such an offence.

C. Our Services

We are able to assist in ensuring full compliance with the PDPA.

1. Audits

The first step of our comprehensive support and advice is a thorough two-stage audit of your organization. Such audit would provide us with a detailed picture of your organization's personal data portfolio. The audit will help to detect any gaps and lapses in the organization's data handling and it forms the basis for assessing the organization's specific needs in developing a comprehensive personal data protection framework.

Usually we would, as a first step, provide you with the necessary documents to establish where personal data exists and how it is handled. Based on your information following the pre-audit, we would then, in a second step, conduct the actual audit consisting of an exhaustive review of the information collected, identification of potential compliance failures as well as a final report proposing the necessary amendments to the organisation's personal data protection regime.

2. Policy Drafting

As mentioned, every organisation needs to have an adequate data protection policy in place. The policy needs to warrant the organisation complies with the PDPA requirements and especially safeguards the personal data in its possession.

3. Training

We further offer training sessions to provide your data handlers with training in order to raise awareness of personal data protection and avoid future non-compliance. Fees vary according to our work involved and therefore would be agreed on a case-by-case basis.

4. Data Protection Officer

As explained above, organisations need to have a DPO who is responsible for ensuring the organisation's compliance with the PDPA if:

- theirs activities of Data Controller or Data Processor relating to collection, use, or disclosure of personal data require regular monitoring of the personal data or the system due to the large number of personal data collected; or

- their core activities of Data Controller or Data Processor relate to the collection, use, or disclosure of certain categories of data.

As the DPO does not necessarily need to be an employee of the organisation, many organisations outsource the DPO function to PDPA specialists in order to ensure PDPA compliance as far as possible. The organisation thereby benefits from the knowledge and experience of the external DPO, enabling the organisations to have its own employees working on more business related matters.

Please note that comprehensive knowledge about the personal data being handled by an organisation is a necessary requirement in order for a DPO to discharge his/her duties properly. Therefore, we can only act as an organisation´s DPO where we have conducted the aforementioned audit and developed a policy prior to rendering our DPO services.

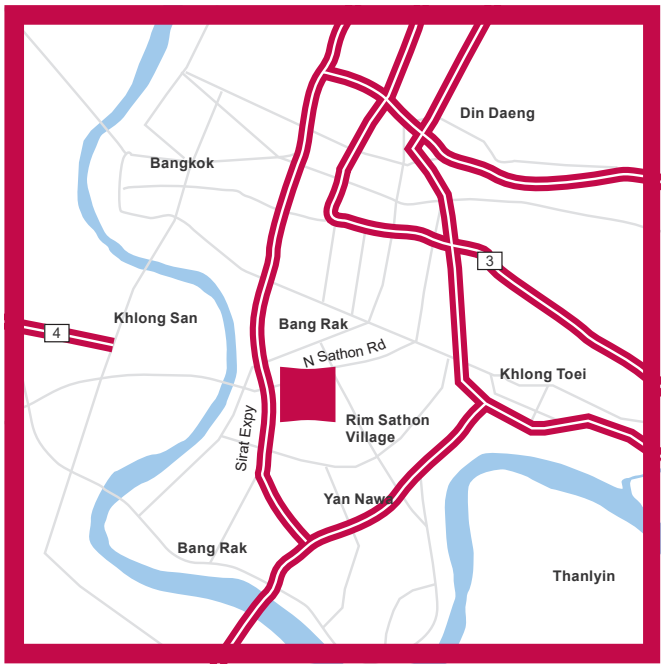
We can provide a DPO for your organisation, if required.

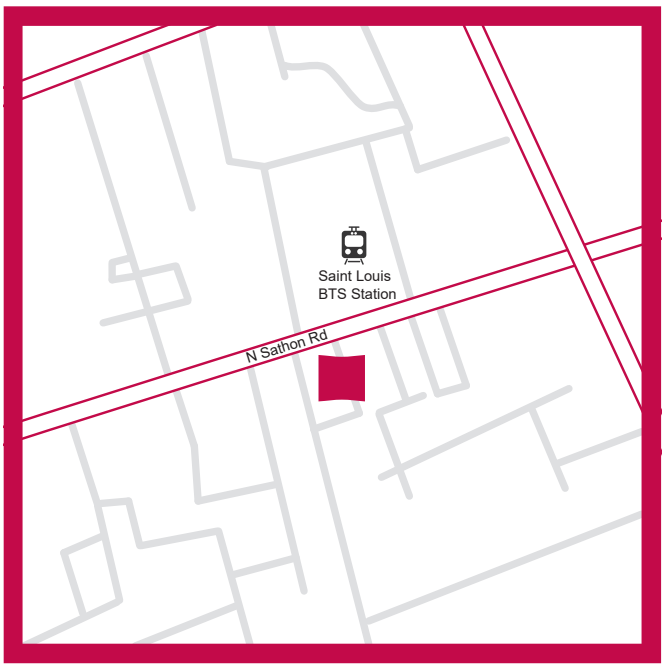
5. Legal Advice Regarding Data Transfer

If you wish to transfer personal data abroad, we offer services that ensure the organisation abroad provides a standard of protection that is commensurate with the requirements prescribed under the PDPA.

Please do not hesitate to contact us to discuss the needs of your organisation and for a customized fee quote.

Our office in Bangkok



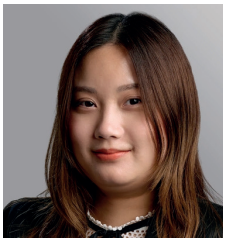


Our office in Bangkok

Luther Law Firm (Thailand) Co., Ltd.
AIA Sathorn Tower
Unit 2007-2008, 20th floor
11/1 S Sathon Rd, Yan Nawa, Sathon, Bangkok 10120
Phone: +66 2 2100 036
Email: Thailand@luther-services.com

Your contact persons

Fabian Lorenz, M.A.
Attorney-at-law (Germany), Location Head, Partner
T +66 61 420 4049
fabian.lorenz@luther-lawfirm.com



Natthamol Dechpokked
Associate
T +66 93 306 7581
natthamol.dechpokked@luther-lawfirm.com

Luther in Asia

Expertise

Our office works closely together with the other Luther offices in Asia and Europe. We take a holistic approach, dealing with Asia-wide compliance issues, assisting with the creation of international holding structures and ensuring tax-efficient repatriation of profits.

We provide the complete range of legal and tax advice to clients doing business in and from Asia. To offer a seamless service, we have teams in Europe as well as in Asia, led by partners with many years of experience on both continents. That way, we can immediately answer questions concerning investment decisions and provide our clients with an accurate assessment of the particularities of their projects, no matter where they are located.

Our lawyers unite substantial practical knowledge in important legal areas and cover the entire spectrum of law in Asia and beyond. We support foreign investors in the assessment of location and investment criteria, the structuring of investment projects, acquisitions and joint ventures. Finding and implementing solutions for sensitive areas like technology transfer and know-how protection also form part of our work. Alongside our clients we negotiate with future partners and local authorities and ensure the enforcement of their rights, in and out of court as well as in arbitration proceedings.

The services of our lawyers are complemented by our accountants, HR professionals and tax consultants offering all the services one would necessarily associate with a “one-stop shop” concept, from outsourced administration to accounting, payroll and tax compliance. Additionally, we provide corporate secretarial services, especially in Asian “common law” countries.

Collectively, our lawyers, tax consultants and professionals combine the competence and experience necessary to comprehensively assist comprehensively on all business matters in Asia. Our tax experts advise on individual and corporate tax compliance as well as on withholding tax issues, on Double Taxation Agreements and on complex international tax structures. Our accountants and professionals carry out the time-consuming administrative tasks of accounting and payroll functions a business must undertake, allowing our clients to concentrate on growing their business.

Singapore

Singapore is a leading international trade and financial hub. As such, it serves as Asian headquarters for many international companies operating within the Asia-Pacific region.

With a staff strength of more than 90, Luther is by far the largest continental European law firm in Singapore. More than 26 lawyers from Singapore, Germany, France and other jurisdictions cover the full range of corporate and commercial legal work as well as the structuring of investments within South and South East Asia.

Our team is supported by excellent local Singaporean lawyers, notary publics, tax advisors, accountants, corporate secretaries and other professionals.

Shanghai

Shanghai is the main hub for doing business in China, and with a team of more than 20 international lawyers, Luther is the largest German-speaking law firm in the city. Our China team consists of German and Chinese legal experts most of whom have over a decade of experience in developing and entering the Chinese market.

Luther Shanghai is fully authorised to offer legal services including litigation and provides advice on all questions of Chinese law. Our legal team is supported by Chinese tax advisors, accountants, corporate secretaries and other professionals.

Region

Our two principal Asian offices in Singapore and Shanghai are complemented by offices and teams in Yangon (Myanmar), Bangkok (Thailand), Delhi-Gurugram (India), Ho Chi Minh City (Vietnam), Kuala Lumpur (Malaysia) and Jakarta (Indonesia).

This network of Luther offices is further strengthened by the long-established business relationships that we have successfully developed both locally and with our regional partners in Australia, Hong Kong, Japan, New Zealand, the Philippines and South Korea.

Hits the mark. Luther.

Luther Rechtsanwaltsgesellschaft mbH is one of the leading corporate law firms in Germany. With some 420 lawyers and tax advisors, we can advise you in all fields of German and international corporate law. In addition to having offices in every economic centre throughout Germany, we are also present in 11 locations abroad: in Brussels, London and Luxembourg in Europe, and in Bangkok, Delhi-Gurugram, Ho Chi Minh City, Jakarta, Kuala Lumpur, Shanghai, Singapore and Yangon in Asia.

Our advisory services are tailored to our clients' corporate goals. We take a creative, dedicated approach to achieving the best possible economic outcome for each of our clients. The name "Luther" stands for expertise and commitment. With a passion for our profession, we dedicate all our efforts to solving your issues, always providing the best possible solution for our clients. Not too much and not too little – we always hit the mark.

We know how crucial it is to use resources efficiently and to plan ahead. We always have an eye on the economic impact of our advice. This is true in the case of strategic consulting as well as in legal disputes. We have complex projects on our agenda every day. At Luther, experienced and highly specialised advisors cooperate closely in order to offer our clients the best possible service. Thanks to our fast and efficient communication, permanent availability and flexibility, we are there for you whenever you need us.

Luther has been named "Law Firm of the Year: Germany 2024" by The Lawyer, one of the most well-known legal magazines worldwide.

Lawyers and tax advisors

420

Locations

21

Long-standing connections to commercial law firms worldwide

Offices in international financial centres and investment locations

About unyer

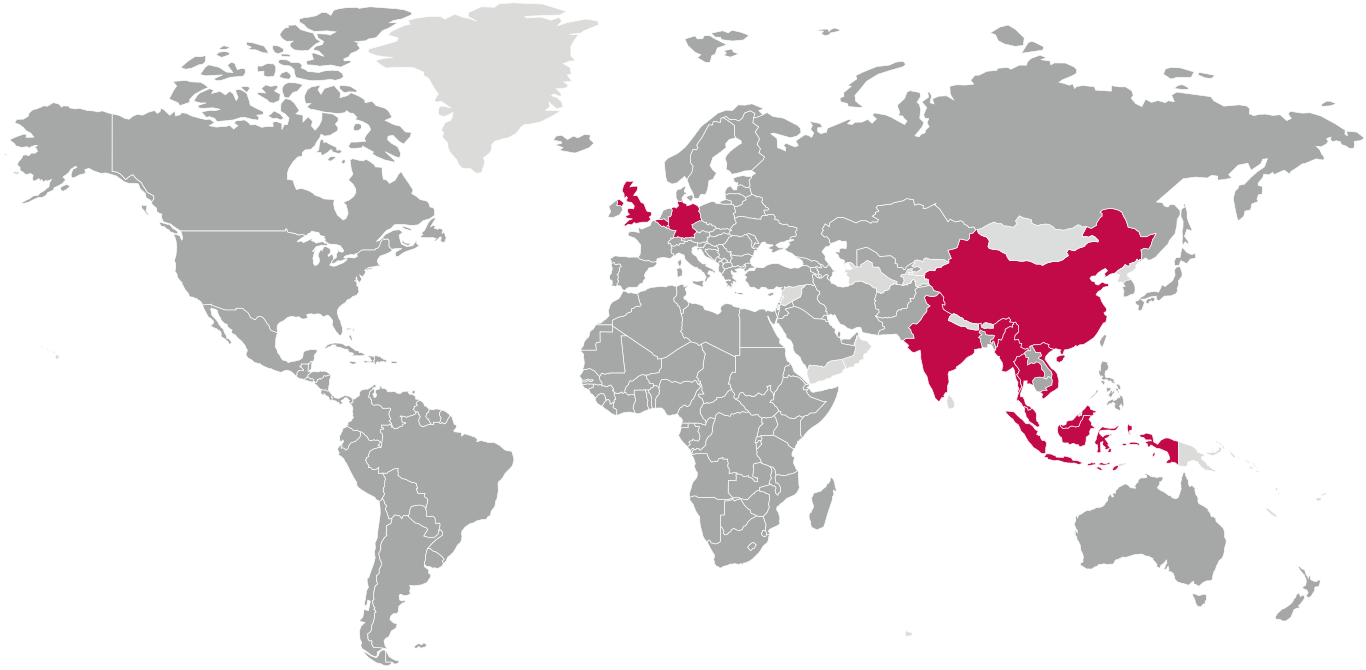
unyer is a global organisation of leading international professional services firms. Besides law firms, unyer is also open to other related professional services, especially from the legal tech sector. unyer is based in Zurich as a Swiss Verein. unyer is globally connected but has strong local roots in their respective markets.

unyer has an exclusive approach and only accepts one member firm from each market. unyer members offer its clients full services across all jurisdictions with a compelling industry focus. The organisation has an annual turnover of more than EUR 650 million and includes over 2,550 lawyers and advisors in more than 14 countries in Europe and Asia.
www.unyer.com

MEMBER OF unyer

Our locations

We have a global outlook, with international offices in key economic and financial centres in Europe and Asia. We also maintain close relationships with other commercial law firms in all relevant jurisdictions. Luther is a founding member of unyer (www.unyer.com), a global organisation of leading professional services firms that cooperate exclusively with each other. This way, we ensure a seamless service for our clients throughout their demanding international projects.



- Luther locations
- Best friends

Our locations

Bangkok
Berlin
Brussels
Cologne
Delhi-Gurugram
Dusseldorf
Essen
Frankfurt a.M.
Hamburg
Hanover
Ho Chi Minh City
Jakarta
Kuala Lumpur
Leipzig
London
Luxembourg
Munich
Shanghai
Singapore
Stuttgart
Yangon

Imprint

Luther Rechtsanwaltsgesellschaft mbH, Anna-Schneider-Steig 22, 50678 Cologne, Germany, Phone +49 221 9937 0, Fax +49 221 9937 110, contact@luther-lawfirm.com

Luther Law Firm (Thailand) Co., Ltd., AIA Sathorn Tower, Unit 2007-2008, 20th floor, 11/1 S Sathon Rd, Yan Nawa, Sathon, Bangkok 10120, Thailand, Phone +66 2 2100 036, thailand@luther-services.com

Disclaimer

Although every effort has been made to offer current and correct information, this publication has been prepared to provide information on recent regulatory and legal developments in Thailand only. It is not exhaustive and thus does not cover all topics with which it deals. It will not be updated and cannot substitute individual legal and/or tax advice. This publication is distributed with the understanding that Luther, the editors and authors cannot be held responsible for the results of any actions taken on the basis of information contained herein or omitted, nor for any errors or omissions in this regard.

Luther.

Bangkok, Berlin, Brussels, Cologne, Delhi-Gurugram, Dusseldorf, Essen, Frankfurt a.M., Hamburg, Hanover, Ho Chi Minh City, Jakarta, Kuala Lumpur, Leipzig, London, Luxembourg, Munich, Shanghai, Singapore, Stuttgart, Yangon

You can find further information at:
www.luther-lawfirm.com
www.luther-services.com

unyer GLOBAL ADVISORS