Legal 500
Country Comparative Guides 2025

Thailand

Data Protection & Cybersecurity

Contributor

Chandler Mori
Hamada Limited

Pranat Laohapairoj

Partner | pranat.l@morihamada.com

Suphakorn Chueabunchai

Senior Associate | suphakorn.c@morihamada.com

Pitchaya Roongroajsataporn

Associate | pitchaya.r@morihamada.com

Tatchai Luangphatarawong

Associate | tatchai.l@morihamada.com

Thanachart Osathanondh

Associate | thanachart.o@morihamada.com

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Thailand.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Thailand: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered; what sectors, activities or data do they regulate; and who enforces the relevant laws).

The Personal Data Protection Act, B.E. 2562 (2019) ("**PDPA**") outlines key protection frameworks for collection, use, and disclosure of any "**Personal Data**", which is defined as any data which, by itself or in combination with other data, can be used to trace back to an individual. In terms of application, the PDPA applies to both private and government sectors (except for certain organizations as specified in the PDPA.) The law has been fully enforceable since 1 June 2022.

In principle, the PDPA, which is mainly based on the General Data Protection Regulation of the European Union ("**GDPR**"), creates obligations on both private and government sectors if they are considered to fall under any of the two categories outlined below, in relation to collection, processing and treatment of Personal Data:

- any entity which has power to decide how to treat Personal Data ("**Controller**"); and
- any entity which treats Personal Data pursuant to instructions of a Controller ("**Processor**")

Both Controllers and Processors carry the burden of proof that they meet the requirements under the PDPA for all types of processing of Personal Data. In addition, the PDPA establishes a supervising authority (i.e., the Personal Data Protection Commission ("**PDPC**") and the Office of the PDPC ("**Office**")) to regulate operators.

Regulations under the PDPA can be broadly categorized into three areas as follows:

- Lawful basis:

Examples of commonly used bases for collection and processing of Personal Data are: (i) consent; (ii) contractual performance; (iii) legitimate interest; and (iv) legal obligations. However, processing of sensitive Personal Data is subject to a different set of bases. Please see further explanation in our response to Question No. 5.

- Rights of Data Subjects:

The PDPA provides an extensive list of rights of data subjects, many of which can be universally invoked while others can be used only under certain circumstances. Except for the right to withdraw any consent given by the data subject, rights of data subjects are not always absolute, as Controller may have certain grounds to argue against such requests, depending on specific facts of a case. Please see further explanation in our response to Question No. 39.

- Security measures:

The PDPA provides a blanket requirement to both Controllers and Processors to treat Personal Data in appropriate manners, which materially include well-organized safe keeping of data, safe storage (physical and electronic), automatic deletion of data, etc.

The PDPC Notification re: Security Safeguard Measures of the Personal Data Controller B.E. 2565 (2022) prescribes minimum data security standards (i.e., organizational, technical, and physical measures, access control, confidentiality) for Personal Data processed under the PDPA. Please see further explanation in our response to Question No. 33.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

Since the PDPA became enforceable, certain sets of subordinate laws under the PDPA (i.e., PDPC notification, PDPC regulation, and PDPC guidelines) have been officially enacted. However, there are certain provisions of the PDPA that still require enactment of subordinate laws to prescribe further or more detailed requirements, guidelines, or clarifications. Most recently, in April 2025, the Thai government introduced stricter penalties concerning Personal Data under the Royal Decree on Measures for the Prevention and Suppression of Technology-Related Crimes (No. 2), B.E. 2568 (2025). The decree imposes penalties on both data users and data collectors who process Personal Data in connection with

technology-related crimes or other criminal offenses. Offenders are subject to imprisonment for up to five years, a fine of up to 500,000 baht, or both. This amendment reflects the heightened focus on Personal Data security, particularly in response to the widespread rise of call center scams, which have affected a significant number of victims.

3. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

The PDPA and cybersecurity laws do not have any registration or licensing requirements for Controllers or Processors. However, with respect to the PDPA, certain subordinate laws impose registration requirements on institutions that act as certifying bodies for Data Protection Officers or those that issue certifications for data privacy standards. In addition, companies that appoint a Data Protection Officer ("**DPO**") must notify the Office of the details of such appointment.

4. How do the data protection laws in your jurisdiction define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data")? Do such laws include a specific definition for special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction (e.g., "controller", "processor", "data subject", etc.)?

The term "Personal Data" is defined under the PDPA as any information relating to a natural person that enables identification of such natural person, whether directly or indirectly, but not including information of deceased persons. Sensitive Personal Data includes Personal Data relating to ethnicity, race, philosophical beliefs, religious beliefs, socio-political beliefs and affiliations, relationships with labour unions, criminal records, diseases and medical conditions, biometrics and DNA, and sexual preference. In any event, the PDPC may add other types of data into this category.

For the definitions of "Controller" and "Processor", please refer to Question No. 1.

5. What principles apply to the processing of personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

Under the PDPA, all Controllers must establish a legal basis for each process of collection, use, or disclosure of Personal Data. Bases differ between ordinary Personal Data and sensitive Personal Data.

Bases for ordinary Personal Data are as follow:

1. via consent of a data subject, prior to or during collection or processing;
2. for achievement of purposes relating to preparation of historical documents or archives for public interest or relating to study, research, or statistics for which an appropriate protection standard is used to protect rights and liberties of data subjects as prescribed and announced by the PDPC (i.e., historical, research or statistical purposes);
3. for prevention or suppression of a danger to life, body, or health of a person (i.e., vital interest);
4. for performance under a contract to which a data subject is a party, or for proceedings with a data subject's request before entering into a contract (i.e., contractual performance);
5. for performance of a Controller's duty for public interest or as required by the state (i.e., public interest);
6. under a legitimate interest of a Controller or another person or juristic person, unless such interest is less important than basic rights in Personal Data of relevant data subject (i.e., legitimate interest); and
7. for a Controller's compliance with the law (i.e., legal obligations).

The bases for sensitive Personal Data are as follow:

1. via consent of a data subject, prior to or during collection or processing of Personal Data;
2. for prevention or suppression of a danger to life, body, or health of a person, where the data subject is incapable of giving consent for whatever reason;
3. for legitimate activities with appropriate safeguards by foundations, associations, or any other not-for-profit bodies for a purpose of their members, former members, or regular-contacted persons under the organization's objectives, without disclosing sensitive Personal Data to external parties;
4. sensitive Personal Data has already been disclosed to

the public with explicit consent of data subjects;
5. for establishment, compliance, exercise, or defence of legal claims; and
6. for compliance with specific laws with a purpose relating to preventive medicine, public health, labour protection, research, or any other purpose for public interest.

Furthermore, the PDPA requires Controllers to provide clear and detailed privacy notices at or before the time of data collection. The notice must include:

- The purpose of the data processing, including the lawful basis;
- The circumstances under which data subjects must provide their Personal Data to comply with legal or contractual obligations, or for the purpose of entering into a contract, including the potential consequences of failing to provide such Personal Data;
- The categories of Personal Data collected;
- The retention period;
- The categories of individuals or entities to whom the Personal Data may be disclosed.
- The contact details of the Controller, its representative, and DPO.
- The rights of data subjects

Last but not least, Controllers are obligated to retain Personal Data only for as long as necessary to fulfil the purposes for which the data was collected, used, or disclosed, unless otherwise required by applicable laws or regulations. Once the retention period has expired, or the data is no longer necessary, Controllers must take appropriate steps to securely delete, destroy, or anonymize the Personal Data to prevent unauthorized access, use, or disclosure.

6. Are there any circumstances for which consent is required or typically obtained in connection with the processing of personal data? What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

There are no categorical prescriptions where consent is strictly required. General principles apply to all circumstances, whereby consent is required if a non-consent basis cannot be established for processing Personal Data. Therefore, consent is typically required when processing activities go beyond what is necessary for contractual or legal obligations, or the legitimate interests—such as for marketing, data analytics, or profiling. In such cases, the Controller must obtain clear, informed, and specific consent from the data subject prior to initiating any processing. Consent must be given voluntarily and must not be obtained through coercion or made a condition for accessing unrelated services.

The PDPA sets out strict requirements for the form in which consent must be obtained. It must be presented in a manner that is clearly distinguishable from other matters, meaning it cannot be bundled with, or embedded within, broader documents such as terms of service, or combined with unrelated consents. Consent must be purpose-specific, allowing individuals to selectively agree to certain processing activities while declining others. Data subjects must also be informed of their right to withdraw consent at any time, and the process for doing so must be as simple as the process for giving it.

7. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

Please see the response for Question No. 5 regarding bases for sensitive Personal Data.

Note that there is no category of the sensitive Personal Data whose collection is prohibited.

For the processing of children's data, consent shall be required subject to the following additional requirements:

- For minors under the age of 10, consent must be obtained from a legal guardian.
- For minors aged between 11 and 20, consent must also be obtained from a legal guardian, except in certain cases where the minor is permitted to unilaterally and independently provide consent (i.e., acts that grant rights or benefits without imposing duties or obligations, acts that are strictly personal to the minor, and acts which are appropriate to the minor's status in life and necessary for his or her reasonable needs.)

The above requirements apply *mutatis mutandis* to the withdrawal of consent, the provision of notices to data subjects, the exercise of data subject rights, the filing complaints by data subjects, and all other acts under the

PDPA involving a minor as a data subject.

8. Do the data protection laws in your jurisdiction include any derogations, exemptions, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

Please see the key points mentioned under our responses to the Questions Nos. 3-7.

9. Does your jurisdiction require or recommend risk or impact assessments in connection with personal data processing activities and, if so, under what circumstances? How are these assessments typically carried out?

The PDPA does not specifically outline this topic in detail. However, the PDPC's guideline on notification of purposes recommends that a Data Protection Impact Assessment ("**DPIA**") should be conducted to identify and mitigate risks associated with the processing of Personal Data, particularly where the data subject has neither provided consent nor been informed, before a Controller processes personal data obtained from sources other than the data subject directly. It is important to note that the PDPA itself does not provide specific requirements or detailed procedures for conducting a DPIA. Nonetheless, in the past, a draft subordinate regulation (i.e., the draft PDPC Notification regarding DPIA) has previously been introduced to address this area more comprehensively.

Under the draft notification, Controllers must carry out DPIA when conducting any processing activity that produces high risks to rights and freedoms of data subjects. Such processing activities are as follows:

- extensive processing of Personal Data based on automated processing, including profiling on which decisions are based and whereby such decisions create legal effects concerning a person;
- processing on a large scale of sensitive Personal Data, taking into account number of relevant persons, amount of relevant information, diversity of relevant information, duration of processing, ;
- systematic monitoring of a publicly accessible area on a large scale; and
- a list of activities prescribed by the PDPC, namely:
  - use of innovative technology;
  - profiling of a special category of Personal Data to decide on access to services;
  - profiling of individuals on a large scale;
  - processing of biometric data;
  - processing of genetic data;
  - matching of data or combining datasets from different sources;
  - collecting Personal Data from a source other than data subjects themselves without providing them with a privacy notice;
  - tracking individuals' locations or behaviour;
  - profiling minors or vulnerable individuals or target-marketing or providing online services to them; and
  - processing of Personal Data that might endanger a data subject's physical health or safety in an event of a security breach.

Furthermore, the assessment should contain at least:

- necessity for undertaking the DPIA;
- descriptions of processing and records of each step;
- results of hearings conducted for stakeholders;
- proportionality of processing;
- assessment of physical, mental, and material risks;
- mitigation of risks; and
- monitoring measures.

In compliance with carrying out a DPIA when required, a Controller is assumed to have conducted the relevant risk assessments and provided appropriate measures under the PDPA.

10. Are there any specific codes of practice applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

The PDPC has issued three key guidelines, as follows:

1. **Guideline on Notification of Purposes** – outlining the required information that must be provided to data subjects regarding data processing activities, including procedures for collecting Personal Data from sources other than the data subject
2. **Guideline on Consent** – providing detailed requirements for obtaining valid consent, including form, content, and conditions to ensure that consent is freely given, specific, informed, and unambiguous.
3. **Guideline on Compliance with State Information and Personal Data** – clarifying the distinction between state information and Personal Data, and providing guidance on how to handle such information appropriately and in accordance with the PDPA.

In addition to the above guidelines, regulatory authorities

or industry associations in specific sectors may issue their own guidelines or codes of conduct to support compliance with the PDPA among business operators within their respective areas. Examples include the Personal Data Protection Guideline for the Non-Life Insurance Industry issued by the Thai General Insurance Association with support from the Office of Insurance Commission, and the Guideline on Personal Data Protection for Thai Banks issued by the Thai Bankers' Association.

11. Are organisations required to maintain any records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

Yes. Controllers must maintain records of processing activities consisting of at least following information in a written or electronic form for the purpose of audits by data subjects or the Office:

1. collected Personal Data;
2. purpose of collection for each type of Personal Data;
3. details of Controller;
4. retention period of Personal Data;
5. rights and methods for access to Personal Data;
6. use or disclosure of Personal Data which is acquired under bases other than consent;
7. Controller's rejection of request or objection from a data subject; and
8. details of security measures applied to Personal Data.

Similar to Controllers, Processors must also maintain records of processing activities whose minimum requirements are stated in the PDPC notification re: rules and procedures for preparation and storage of record of processing activities for Processors B.E. 2565 (2022). The minimum requirements are as follows:

1. name and information of the Processor and its agent (if any);
2. name and information of Controller, whereby the Processor proceeds under its order or on its behalf, and name and information of the agent of the Controller (if any);
3. name and information of the data protection officer ("**DPO**") including the contact address and means of contact in case the Processor appoints a DPO;
4. type or manner of collection, use or disclosure of Personal Data by the Processor under the order or on behalf of the Controller, including the Personal Data and purpose of collection, use or disclosure of personal data as designated by the Controller;
5. type of persons or agencies receiving the Personal Data in case the Personal Data is transmitted or transferred to a foreign country; and
6. explanation relating to the security safeguard measures.

Currently, there are 2 PDPC notifications regarding the requirement to maintain records of data processing activities for small organizations. Under these notifications, an organization that meets any of the following criteria is considered a small business enterprise and is exempt from the abovementioned obligations (subject to certain conditions).

1. A small or medium-sized enterprise under the law on the promotion of medium and small-sized enterprises;
2. A community enterprise or its network under the law on community enterprise promotion;
3. A social enterprise or a social business group under the law on social enterprise promotion;
4. A cooperative, federation of cooperatives, or farmers' group under the law on cooperatives;
5. A foundation, association, religious organization or a non-profit organization
6. A condominium juristic person under the laws governing condominiums, and a housing estate juristic person under the laws on land allocation;
7. A family business or other business with similar characteristics; or
8. A business operated by a natural person.

12. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

There is no explicit requirement to have data retention and disposal policies and procedures (except in the case of criminal records, which should not be retained for more than 6 months). However, Controllers must, under the PDPA, implement whatever systems necessary to ensure erasure and destruction of Personal Data upon one of following occurrences:

- when its prescribed retention period ends;
- when it becomes irrelevant, or its retention is beyond purpose for which it has been collected; or
- when a data subject has requested for the erasure or destruction or when a data subject withdraws consent.

The above requirement is not applicable for retention of Personal Data under several purposes (e.g., exercise of

freedom of speech, performance of a Controller's duty for public interest or as required by the state, or establishment, compliance, or exercise of rights under the law, etc.)

13. Under what circumstances is it required or recommended to consult with the applicable data protection regulator(s)?

There is no explicit requirement for consultation with the PDPC or the Office.

14. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, what are their legal responsibilities?

Under the PDPA, Controllers and Processors shall designate a data protection officer ("**DPO**") in the following circumstances:

1. Controllers and Processors is a public authority as announced by the PDPC;
2. the activities of Controllers and Processors in the processing of Personal Data require regular monitoring of Personal Data or system, by reason of having a large number of Personal Data as announced by the PDPC; or
3. the core activity of Controllers and Processors is the processing of sensitive Personal Data.

In 2023, the Notification re: The Appointment of DPO under Section 41(2) of the PDPA B.E. 2566 (2023) was introduced by the PDPC. This notification sets out the key criteria for the circumstance stated in (2) above that Controllers and Processors shall appoint a DPO where their core activities consist of processing operations which require regular or systematic monitoring of Personal Data on a large scale.

- Regular or systematic monitoring of Personal Data: If any core activities involve tracking, monitoring, analyzing, or profiling that generally processes Personal Data regularly or systematically, they will be deemed as processing activities requiring regular or systematic monitoring of Personal Data. The notification further prescribes some specific cases that are deemed as regular or systematic monitoring e.g., processing of data of membership cards, public transportation cards, and electronic cards, activities involving credit scoring or fraud prevention, and behavioral advertising.
- On a large scale: The notification provides some specific cases deemed as large-scale processing, as follows:
    - processing as a part of core activities with 100,000 or more data subjects;
    - processing for behavioral advertising through widely used search engines or online social media platforms;
    - processing of customers' or service users' Personal Data in the usual operations of the companies dealing with life insurance, non-life insurance, and financial institution businesses, excluding operations of the credit bureau and its members as defined by credit information business laws; or
    - processing of customers' or service users' Personal Data by licensees of the Telecommunications Business Operators Type 3 according to the telecommunication business operation laws.

If the core activities do not fall under above cases, the notification further provides four key factors which must be considered when determining whether the processing is carried out on a large scale: (1) the number of data subjects, (2) the volume of data, (3) the duration of processing and (4) the geographical extent of the processing activities.

For the legal responsibility of the appointed DPO, the PDPA stipulates that the DPO shall:

a. provide advice to Controllers or Processors, including their employees or service providers with respect to compliance with the PDPA;
b. investigate the performance of Controllers or Processors, including their employees or service providers with respect to the processing of Personal Data for compliance with the PDPA;
c. coordinate and cooperate with the Office in the circumstance where there are problems with respect to the processing of Personal Data undertaken by Controllers or Processors, including their employees or service providers with respect to the compliance with the PDPA; and
d. keep confidentiality of the Personal Data known or acquired in the course of his or her performance of duty under the PDPA.

15. Do the data protection laws in your jurisdiction require or recommend employee

training related to data protection? If so, please describe such training requirement(s) or recommendation(s).

There is no requirement or recommendation under the PDPA. However, in practice, employee training is recommended as part of the organization's security measures, particularly for those engaged in regular or large-scale processing of Personal Data.

16. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

Prior to or at time of collection of Personal Data, a Controller must give notice to data subject. Such notice must consist of following items, except if the data subject is already aware of such information:

- purpose of processing, including corresponding bases;
- notification of a case where a data subject must provide his or her Personal Data for compliance with law or a contract, or where it is necessary to provide Personal Data to enter into the contract, including notification of the possible effect of the data subject not providing such Personal Data;
- Personal Data to be collected and the retention period. If it is not possible to specify a retention period, then specifying an expected data retention period according to data retention standards;
- categories of persons or entities to whom collected Personal Data may be disclosed;
- information, address, and contact details of a Controller or data protection officer; and
- rights of data subject as prescribed under the PDPA.

However, there is no mandatory form of notice. It is advisable that Controllers act reasonably and utilize communication channels that afford ample opportunity to data subjects to be notified and learn of these details.

17. Do the data protection laws in your jurisdiction draw any distinction between the responsibility of controllers and the processors of personal data? If so, what are the implications?

There is a distinction under the PDPA as outlined previously, and position determines roles and authorities. Both positions have statutory obligations and liabilities irrespective of clarity of a contract between them.

18. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these or any similar terms defined?

The PDPA does not specifically outline such topics. All treatment processes, whether monitoring or automated decision-making, are deemed simply as processing of Personal Data. However, there is a draft subordinate law (i.e., draft PDPC notification regarding obligation of Controllers in facilitating a data subject's right to not be subject to a decision based solely on automated processing) which touches upon following topics:

Definition of “Profiling” and “Automated Decision-Making”

- “Profiling” means any form of automated processing of Personal Data consisting of use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.
- “Automated Decision-Making” means a process of making a decision by automated means without human involvement. These decisions are based on Personal Data acquired from a data subject or created by a Controller or Processor.

Key obligations of Controllers regarding the implementation Automated Decision-Making

- Controllers must prepare for decision-making by humans or with human involvement in case a data subject does not wish for the decision to be based solely on automated processing, including profiling. However, such obligations are under several conditional exemptions (e.g., the Automated Decision-Making is necessary for entering into or performance of a contract, authorized by laws, or the decision is based on the data subject's explicit consent).

There must not be any Automated Decision-Making for sensitive Personal Data, unless a data subject's explicit consent is obtained and appropriate measures to protect rights and freedoms of the data subject have been procured.

19. Please describe any restrictions on targeted advertising and/or behavioral advertising. How are these terms or any similar terms defined?

The PDPA does not explicitly define or regulate "targeted advertising" or "behavioral advertising" as standalone legal terms. However, such practices typically involve the processing of Personal Data—often through cookies, tracking technologies, or profiling—to deliver personalized content or advertisements. As such, they fall within the scope of the PDPA and are subject to its general requirements. In particular, Controllers must obtain valid consent from data subjects before collecting and processing Personal Data for advertising or marketing purposes, especially where such data is not necessary for the provision of a core service.

20. Please describe any data protection laws in your jurisdiction restricting the sale of personal data. How is the term "sale" or such related terms defined?

There is no definition of or a separate concept for the sale of Personal Data, nor are there any other related terms or any specific restrictions applicable to it. All general principles and concepts that broadly apply to the processing of Personal Data will apply, as applicable, to the sale and similar activities. However, the illegal sale of Personal Data may result in imprisonment of up to 5 years, a fine not exceeding 500,000 THB or both.

21. Please describe any data protection laws in your jurisdiction restricting telephone calls, text messaging, email communication, or direct marketing. How are these terms defined?

There is no definition of or a separate concept for these activities, nor are there any specific restrictions applicable to them. All general principles and concepts that broadly apply to the processing of Personal Data will apply, as applicable, to these and similar activities.

Nevertheless, use of Personal Data for direct marketing via profiling or target marketing towards minors or vulnerable individuals may obligate Controllers to carry out DPIA for such processing activity, according to the draft PDPC notification. Please refer to our response to the Question No. 19 for clarification regarding DPIA.

In addition to the PDPA, there are requirements relating to marketing communication in Thailand in accordance with the Commission of Computer-related Offences Act B.E. 2550 (the "CCA"). The CCA prohibits the sending of computer data or e-mails to other persons in any manner which disturbs the recipients.

There are certain exemptions prescribed by the sub-regulation (i.e. Notification of the Ministry of Digital Economy and Society re: Characteristics and Method of Sending, Characteristics and Size of Data, and Frequency and Method of Sending Without Disturbing the Recipient) to clarify the characteristics and method of sending data without disturbing the recipients; amongst others, the sending of computer data or e-mail to communicate or to be evidence of a contractual (transactional) relationship, which has been agreed upon by the sender and the recipient, including the sending of data relating to the legal relationship derived from the employment agreement, hire of work agreement, or any other benefits which are related to and agreed upon between the recipient and the sender, or the delivery of goods and services agreed upon between the sender and the recipient in advance, such as membership or subscription for becoming a user of any legitimate services.

From the above, the marketing communication should reasonably fall under the exemption of not disturbing the recipient if such sending has been agreed upon between sender and the recipient, i.e. to members, subscribers, or individuals who registered to receive such newsletter. If not, the opt-in consent from the recipient would be required.

Noted that in such opt-in consent, the CCA requires that a sender must include a message on an easy method to opt out which includes (i) any technical measure enabling the recipient to easily respond to the sender in order to terminate, refuse to receive the information, or decline to receive the information, such as to include an e-mail address, phone number, facsimile number, or contact address of the sender, in order to send to and cause the sender to stop sending computer data or electronic mail to the recipient; or (ii) any method of computer operation by providing the URL, a form, or any computer command for enabling the recipient to make a command to decline the receipt of such information or to promptly unsubscribe.

The provision of the CCA applies to the sending of marketing communication to general company email addresses which are not linked to a specific name of individuals.

22. Please describe any data protection laws in your jurisdiction addressing biometrics, such as

facial recognition. How are such terms defined?

"Biometric Data" is Personal Data resulting from use of technological processing relating to physical or behavioural characteristics of a natural person to confirm unique identification of a natural person, such as facial imaging data, dactyloscopy data, or iris recognition data.

As Biometric Data is categorized as sensitive Personal Data under the PDPA, bases for processing Biometric Data is outlined above in Question No. 5. In addition, there is a draft supplementary regulation (i.e., draft PDPC notification regarding appropriate protection measures for processing of sensitive Personal Data) prescribing additional obligations of Controllers for processing sensitive Personal Data (e.g., provision of appropriate protection measures for such processing, preparation of a sensitive Personal Data protection policy to be disclosed to data subjects, etc.)

23. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

The PDPA does not specifically outline such topic.

24. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

The PDPA does not prohibit the offshore transfer of Personal Data; however, it imposes additional obligations on transferors.

By default, Personal Data can only be transferred offshore to countries that have adequate Personal Data protection measures. Under the respective subordinate law, countries deemed adequate must have a data privacy law that is not less stringent than the PDPA and a regulatory entity in place. If it is uncertain whether the destination countries have sufficient Personal Data protection measures, the PDPC has the authority to consider and make the final decision. This decision, regarding the adequacy of a country's Personal Data protection measures, will be published. To date, there has been no such decision published by the PDPC.

If a particular destination lacks adequate Personal Data protection measures, transferors must qualify for one of the available exemptions, such as compliance with the law, consent acquisition, contract performance, and others. Another useful exemption includes providing adequate safeguards, such as intra-group transfers under a Binding Corporate Rule ("**BCR**") approved by the Office. Another safeguard involves transfers under a Standard Contractual Clause ("**SCC**"). Under the respective subordinate law, the provisions under the ASEAN Model Contractual Clauses for Cross Border Data Flows and GDPR's Standard Contractual Clauses for the Transfer of Personal Data to Third Countries are considered acceptable by the Office.

25. What personal data security obligations are imposed by the data protection laws in your jurisdiction?

General security obligations are imposed on Controllers and Processors, as outlined below..

- Controllers are obligated to do followings:
  - provide appropriate security measures to prevent unauthorized or unlawful access to or loss, use, alteration, or disclosure of Personal Data, and such measures must be reviewed when it is necessary or when technology has changed to efficiently maintain appropriate security and safety. It must also be in accordance with minimum standards specified and announced by the PDPC;
  - when Personal Data is to be provided to other persons, Controller must ensure that such persons not use or disclose such Personal Data unlawfully or without authorization; and
  - notify the Office of any Personal Data breach without delay and, where feasible, within 72 hours after having become aware of it, unless such Personal Data breach is unlikely to result in a risk to rights and freedoms of a data subject. If the Personal Data breach is likely to result in a high risk to rights and freedoms of a data subject, the Controller must also notify the Personal Data breach and remedial measures to the data subject without delay.
- Processors are also obligated to provide appropriate security measures along the same line as outlined above and notify relevant Controller of Personal Data breach that has occurred.

In addition, there is PDPC notification re: security safeguard measures of the Controller B.E. 2565 (2022) mandating Controllers to arrange for appropriate security safeguards measures that includes the key concerns as

follows:

- cover all processing of Personal Data whether in written or electronic form or in any form;
- comprise appropriate organizational measures, technical measures, and may include physical measures,
- take into account the operation relating to security safeguard i.e., identification of the risk to information assets, protection and monitor of the possible major risks or data breach;
- take into account the ability to maintain security and safety measures for the system or service of Personal Data processing via principles of confidentiality, integrity, and availability;
- with regard to the processing of Personal Data in electronic form, the measures must cover components of the information system relating thereto;
- take into account necessity of access and use according to the nature and purpose of processing of Personal Data i.e., identity proofing and authentication, user access management, etc.

include promotion of privacy and security awareness including informing the Controllers' employees of such security safeguards measures.

26. Do the data protection laws in your jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances must such a breach be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

The PDPC Notification re: Criteria and Procedures for the Notification of Data Breach Incident B.E. 2565 (2022) prescribe that the security breaches or data breaches is an incident arising out of the breach of the security measures that causes unauthorized or unlawful loss, access, use, modification, or disclosure of Personal Data, whether resulting from an intentional, wilful, negligent, unauthorized, or unlawful act, an act related to computer crimes, cyber threats, mistakes or accidents, or any other act of Controllers. Moreover, the data breaches can occur from the Processers processing Person Data in accordance with the orders or on behalf of the Controllers, or employees, service providers representatives, or any related persons of Controllers.

In any regard, the notification also classifies data breaches into three categories i.e., confidentiality breach, integrity breach, and availability breach.

In the event of a security breach impacting personal data, Controllers must report the incident to the PDPC without undue delay and, in any case, within 72 hours of becoming aware of it. Controllers must also notify the affected data subjects if the breach is likely to result in a high risk to their rights and freedoms.

27. Do the data protection laws in your jurisdiction establish specific rights for individuals, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, and any exceptions.

The PDPA provides for the following individual data privacy rights:

i. Right to be notified of Personal Data collection and processing, prior to or during collection of Personal Data. Such notification shall consist of information such as purpose of collection, use, or disclosure of Personal Data, specific Personal Data to be collected, and retention period, etc.
ii. Right to access a data subject's own Personal Data, with exceptions of the following: (i) denial of access due to an applicable law or court order; or (ii) access may cause a detrimental effect on other data subjects' right and freedom.
iii. Right to receive a data subject's own Personal Data from a Controller or to request a Controller to transfer such Personal Data to other Controllers.
iv. Right to correct incomplete or inaccurate parts of Personal Data, although a Controller may verify the accuracy of new information provided by data subjects.
v. Right to suspend use of Personal Data in any of the following events: (i) when a Controller is in the process of verifying certain information to rectify, update, complete, or avoid any mishaps about Personal Data upon a request of the data subject; (ii) when Personal Data is to be erased as requested by a data subject but the data subject instead requests to suspend its use; (iii) when it is no longer necessary to store Personal Data, but a data subject requests a Controller to continue to store such Personal Data for establishing legal claims, legal compliance, exercise of legal rights or defenses; or (iv) when a Controller is in process of verifying its legitimate rights in its data collection or processing for purposes specified by law.
vi. Right to oppose collection, use, or disclosure of a data

subject's own Personal Data at any given time, with exception of Personal Data which is: (i) collected under bases other than consent (unless a Controller is able to prove that such collection, use, or disclosure is more legitimate or is for the exercise of the Controller's rights under the laws); and (ii) collected, used, or disclosed for scientific, historic, or statistical purposes (unless necessary for operation of Controller for public goods) or for the purpose of direct marketing.

vii. Right to delete a data subject's own Personal Data or to render such Personal Data unidentifiable upon the following cases: (i) there is no further necessity for retention of such Personal Data; (ii) the data subject retracts consent and there is no other basis for retention of such Personal Data; (iii) the data subject opposes collection, use, or disclosure and a Controller cannot deny such request.

viii. Right to withdraw consent at any time. However, withdrawal of consent will not have any effect on the Controller's previous data processing.

ix. Right to file a complaint with the supervisory authority (i.e., the Office) if the data subject believes that a Controller fails to comply with any requirements under the PDPA.

28. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

Under the PDPA and the PDPC regulation on the filing, rejection, termination and consideration period of complaint B.E.2565 (2022), a data subject has the right to file a complaint to the relevant authority or committee in an event that a Controller or Processor, including their employees or service providers, violates or does not comply with any provisions under the PDPA or any notifications issued thereunder. See Question No. 44 for expanded explanation.

29. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual and material damage to have been sustained, or is non-material injury to feelings, emotional distress or similar sufficient for such purposes?

Yes, individuals are entitled to monetary damages. The PDPA also allows for punitive damages in addition to actual damages to be rendered by a court as it deems fit but shall not exceed two times the amount of actual damages.

While it is stated under the PDPA that data subject is entitled to compensation when "damage" is caused towards such data subject from non-compliance of a Controller or Processor, there is no clear precedent on what constitutes damage. Given courts' interpretation of "damages" in similar legal concepts (i.e., tort law), it is possible that injury of feelings is sufficient to prove damage if such injury is a direct result from such non-compliance.

30. How are data protection laws in your jurisdiction typically enforced?

There are two main governmental authorities enforcing the PDPA:

1. The PDPC: The PDPC is mainly responsible for enactment of regulations, notifications, and guidelines relating to Personal Data protection, along with providing interpretation and decision regarding the PDPA and its supplemental laws.
2. The Office: The main objectives of the Office include provision of support for development of Personal Data protection within Thailand, such as development of security technology, keeping records of development of Personal Data protection around Thailand, provision of consultation to other governmental or business entities regarding Personal Data protection, and processing of complaints from data subjects.

31. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

There are three types of penalties as prescribed under the PDPA:

1. Penalties for civil breach

A damaged data subject may bring a civil suit against a Controller and/or Processor who has/have wronged him/her. The compensation will include actual damages as well as punitive damages as outlined above.

2. Penalties for criminal breach

The relevant authority under the PDPA may pursue a criminal case against a Controller for certain severe misconducts, and the maximum penalties are imprisonment of not exceeding one year or a fine of not exceeding Baht 1,000,000, or both.

Relevant directors or managers of a breaching Controller or Processor may be liable to the same penalties as well.

3. Penalties for administrative breach

The relevant authority under the PDPA may also pursue an administrative case against a Controller or Processor who has committed a wrongful act under the PDPA, and maximum fine is Baht 5,000,000.

32. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

Currently, there is none.

33. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

There is no specific process under the PDPA. However, orders of the regulators (i.e., the PDPC or the Office) are considered as administrative orders which can be appealed under administrative procedures. The appeal process involves submitting to the Administrative Court of Thailand a formal appeal document outlining the grounds for the appeal and any supporting evidence. The court will review the case and issue a determination based on the merits of the appeal.

34. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

The PDPC has been much more active on reviewing and inspecting data breach incidents. According to the report on PDPC's website, 899 data breach incidents were reported during October 2024 to March 2025. In addition to the inspection, the PDPC has received more than 100 complaints about non-compliance with the PDPA during July 2024 to September 2024, all of which naturally resulted in some level of investigation.

In addition, in 2024, the PDPC issued its first administrative enforcement decision under the PDPA, imposing the maximum fine of THB 7 million on a leading online retail company. The penalty was based on several key compliance failures, including the absence of a designated DPO and the lack of adequate technical and organizational security measures, which led to a personal data breach. The compromised data was subsequently exploited in fraudulent call centre schemes. Also, the company failed to notify the PDPC of the breach within the legally prescribed timeframe.

35. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide details.

The Cybersecurity Act B.E. 2562 (2019) ("**Cybersecurity Act**") is the principal legislation governing cybersecurity, aiming at protecting the country's significant information systems and information technology infrastructure. The Cybersecurity Act imposes several obligations on government agencies, regulatory organizations, and organizations designated as critical information infrastructure ("**CII**") (collectively, "**Regulated Entities**"). These obligations include the following:

- preparing a code of practice and a standard framework for maintaining Cybersecurity in accordance with standards prescribed by relevant regulations and guidelines;
- preventing, coping with, and mitigating risks from cyber threats in accordance with such code of practice,
- appointing executive officials and operational officials for coordinating cybersecurity efforts with the National Cybersecurity Agency ("**NCSA**").

In addition, the Cybersecurity Act designates certain institutions as supervising organizations, which are tasked with supervising and regulating the operations of those Regulated Entities ("**Supervising Organization**").

36. Do the cybersecurity laws in your jurisdiction impose specific requirements regarding supply chain management? If so, please provide details of these requirements.

The Cybersecurity Act does not explicitly impose specific requirements regarding supply chain management. However, it does require the Regulated Entities to comply with the cybersecurity standards and measures prescribed by the relevant authorities, which may include aspects of supply chain management.

37. Do the cybersecurity laws in your jurisdiction impose information sharing requirements on

organisations?

The Cybersecurity Act imposes information sharing requirements in the context of cybersecurity incidents. The Regulated Entities are required to report any cyber threat incidents to the relevant regulating office and their respective supervising organizations without delay. The Cybersecurity Regulatory Committee ("**CRC**") is also authorized to request information, documents, or cooperation from any person related to or affected by a cyber threat, and to share information and resources with both the public and private sectors.

38. Do the cybersecurity laws in your jurisdiction require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, what are their legal responsibilities?

The Cybersecurity Act imposes information sharing requirements in the context of cybersecurity incidents. The Regulated Entities are required to report any cyber threat incidents to the relevant regulating office and their Supervising Organisations without delay. The key supervising bodies under the Cybersecurity Act, CRC and the NCSA, are also authorized to request information, documents, or cooperation from any person related to or affected by a cyber threat, and to share information and resources with both the public and private sectors.

39. Are there specific cybersecurity laws / regulations for different industries (e.g., finance, healthcare, government)? If so, please provide an overview.

The Regulated Entities under the Cybersecurity Act are government agencies, the Supervising Organizations and the CII organizations. The NCSA is empowered to prescribe the characteristics of the organizations that qualify as the CII, based on the services they provide in the following sectors:

- national security;
- critical government services;
- banking and finance;
- information technology and telecommunications;
- transportation and logistics;
- energy and public utilities;
- public health;
- others as may be prescribed by the NCSC.

40. What impact do international cybersecurity standards have on local laws and regulations?

The Cybersecurity Act does not directly refer to any international cybersecurity standards. However, the NCSA, empowered to establish the standards and guidelines to enhance and develop service systems pertaining to maintaining cybersecurity, may take into account international cybersecurity standards when establishing and determining the standards and guidelines for maintaining cybersecurity in Thailand, and may align or harmonize local laws and regulations with international frameworks where appropriate and feasible.

41. Do the cybersecurity laws in your jurisdiction impose obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and under what circumstances must a cybersecurity incident be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

The Cybersecurity Act defines a cybersecurity incident as any event caused by any action or unlawful undertaking committed through a computer or computer system which may damage or affect cybersecurity, or the cybersecurity of a computer, computer data, computer system, or other data related to the computer system, and defines a cyber threat as any action or unlawful undertaking using a computer, computer system, or undesirable program with an intention to cause any harm to the computer system, computer data, or other relevant data, and posing an imminent threat of causing damage to or affecting the operation of a computer, computer system, or other relevant data. The Cybersecurity Act further classifies cyber threats into three levels: non-critical, critical, and crisis, depending on the nature, severity, and impact of the threat.

Once a cyber threat incident occurs, the Regulated Entities are required to report the incident to the NCSA and their respective Supervising Organizations without delay. They must also cooperate and assist in preventing, coping with, and mitigating the risks posed by the cyber threat. The CRC and the NCSA are then authorized to:

- notify the public of the cyber threat incident, as deemed necessary and appropriate;
- request information, documents, or cooperation from any person related to or affected by the cyber threat; and
- access, examine, monitor, seize, or freeze any computer, computer system, or any equipment related

to or affected by the cyber threat, with or without a court order, depending on the level and urgency of the threat incident, and subject to certain conditions and safeguards.

42. How are cybersecurity laws in your jurisdiction typically enforced?

Cybersecurity laws in Thailand are primarily enforced through the mechanisms established under the Cybersecurity Act, which grants enforcement authority to the National Cyber Security Committee ("**NCSC**") and the NCSA. For organizations designated as the CII, the NCSA has the power to conduct inspections, request information, and issue orders to implement or improve cybersecurity measures. In cases of non-compliance, the NCSA may issue **corrective orders**, and failure to comply may lead to **administrative or criminal penalties**, depending on the severity and impact of the violation. In urgent situations involving threats to national security, the law also authorizes the NCSA to take immediate actions, including accessing systems or ordering the suspension of operations, subject to oversight and subsequent review by the NCSC. Enforcement is generally proactive in CII sectors, while for other entities, it may be reactive—triggered by incidents, complaints, or regulatory investigations.

43. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

Under the Cybersecurity Act, regulators are granted broad powers of oversight, inspection, and audit, particularly in relation to entities classified as the CII. Key authorities involved include the NCSA, the CRC, and the NCSC, each with distinct but coordinated roles:

The NCSA has authority to:

- conduct inspections and audits of the CII entities to assess compliance with applicable cybersecurity standards;
- require the submission of relevant information, documents, or access to computer systems and physical premises;
- issue corrective orders in cases of non-compliance or detected vulnerabilities;
- access or seize systems and data with court approval in serious cyber threat situations; and
- take immediate action without prior court approval in urgent cases, subject to subsequent judicial review.

The CRC plays a supporting role by:

- setting minimum cybersecurity standards and codes of practice; and
- issuing technical directives to prevent or mitigate cyber threats, particularly within CII sectors.

The NCSC provides overarching policy direction by:

- supervising the NCSA's activities and national enforcement priorities;
- coordinating with relevant agencies; and
- authorizing or directing significant enforcement actions in response to national-level cybersecurity threats.

This framework ensures that cybersecurity oversight in Thailand is both proactive and responsive, particularly in protecting essential services and national interests.

44. What is the range of sanctions (including fines and penalties) for violations of cybersecurity laws in your jurisdiction?

Penalties under the Computer Crime Act:

- Fine (criminal or not): Up to THB 500,000; and/or
- Imprisonment: Up to 20 years.

Penalties under the Cybersecurity Act:

- Fine (criminal or not): Up to THB 300,000; and/or
- Imprisonment: Up to 3 years.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

Each specific violation typically carries a range of penalties prescribed by the law, such as a fine of up to X amount, imprisonment of up to X year, or both. However, the court retains the discretion to determine the actual penalty within this range based on the circumstances of each case.

46. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

There is no specific process under the Cybersecurity Act. Please refer to our response to Questions 33 for details regarding appeal procedures. In any case, the Cybersecurity Act stipulates that only a cyber threat

classified as non-severe are eligible for appeal.

47. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

Currently, there are no clearly identifiable trends or stated regulatory priorities in enforcement activity that we are aware of.

Contributors

Pranat Laohapairoj
Partner
pranat.l@morihamada.com

Suphakorn Chueabunchai
Senior Associate
suphakorn.c@morihamada.com

Pitchaya Roongroajsataporn
Associate
pitchaya.r@morihamada.com

Tatchai Luangphatarawong
Associate
tatchai.l@morihamada.com

Thanachart Osathanondh
Associate
thanachart.o@morihamada.com