COUNTRY COMPARATIVE GUIDES 2024

The Legal 500 Country Comparative Guides

Thailand

DATA PROTECTION & CYBERSECURITY

Contributor

Chandler MHM

Mr. Pranat Laohapairoj

Partner | pranat.l@mhm-global.com

Mr. Suphakorn Chueabunchai

Senior Associate | suphakorn.c@mhm-global.com

Ms. Pitchaya Roongroajsataporn

Associate | pitchaya.r@mhm-global.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 by them; 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 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations,

expected regulations or amendments (together, "data protection laws"))?

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 while some of the drafts thereof have undergone public hearing process pending the announcement to be in effect. 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. Currently, there are several both official and unofficial drafts of subordinate laws to be issued under the PDPA that have undergone process of public hearings from business operations of different sectors, including following key topics:

- appropriate protection measures for processing sensitive Personal Data;
- codes of conduct for protection of Personal Data;
- data protection impact assessments; and
- general duties of Processors

3. Are there any registration or licensing requirements for entities covered by these data protection laws, and if so what are the requirements? Are there any exemptions?

The PDPA itself does not have any registration or licensing requirements for entities. However, certain subordinate laws include registration requirements for institutions that act as certifying bodies for Data Protection Officers or those that issue certification of data privacy standards. Furthermore, companies which have a Data Protection Officer ("**DPO**") must register the DPO with the Office.

4. How do these data protection laws define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data") versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

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. Personal Data is further dissected into: (i) ordinary Personal Data; and (ii) sensitive Personal Data.

i. Ordinary Personal Data

Ordinary Personal Data includes all Personal Data that does not fall into the category of sensitive Personal Data.

ii. Sensitive Personal Data

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.

5. What are the principles related to the general processing of personal data in your jurisdiction? For example, must a covered entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

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.

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

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. Please see further clarification on the bases in our response to the Question No. 5.

7. 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)?

Generally, consent must be clear and in written, electronic, or other unequivocal manners, and different objectives should be separately listed to ease understanding of data subjects. Generally, consent must not be a condition to the provision of any services or entry into any agreements, unless it is absolutely and objectively necessary. Generally, consent can not be assumed, implied, or by default pre-opted. Other information must also be given at the same time, such as rights of data subjects, contact information, retention periods, etc. A consent-seeking provision needs to be separate from other unrelated documents, such as a service contract.

Currently, there are guidelines regarding criteria and methods for obtainment of consent from data subjects issued by the PDPC. The guidelines lay down the concept supporting the governmental authorities, associations, or industrial groups to draft a voluntary standard consent form that will comply with the PDPA. For businesses governed by specific laws (e.g., businesses relating to finance, securities, insurance, etc.), such form or content must also comply with the governing law of each specific business.

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

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.

9. How do the data protection laws in your jurisdiction address health data?

Health data is categorized as sensitive Personal Data under PDPA. Please see the response in Question No. 5 for the bases for processing of sensitive Personal Data.

10. Do the data protection laws in your jurisdiction include any derogations, 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. 3-8.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

Obtainment of consent from an unemancipated minor is subject to additional requirements as follows:

- If a minor is not older than 10 years old, consent must be obtained from a legal guardian.
- If a minor is between the age of 11 and 20 years old, consent must be obtained from a legal guardian, except for certain activities for which the minor can unilaterally give consent without any guardian (i.e., actions granting rights and benefits which are free from any duties or obligations, actions which are strictly personal to the minor, and actions which are suitable to the minor's conditions of life and required for his or her reasonable needs.)

The above provision applies *mutatis mutandis* to the withdrawal of consent, notice given to a data subject, exercise of a data subject's rights, a data subject's complaints, and any acts under the PDPA for a data subject who is a minor.

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

The PDPA does not specifically outline such topics. However, 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. Also, see answers in No. 13 below for expanded explanation.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

PDPC is the regulator who oversees all compliance under the PDPA regardless of the types of data subject or whether the processing of personal data is conducted via online or offline.

In terms of online safety, the Ministry of Digital Economy and Society ("**MDES**") is primarily responsible for implementing internet-related regulations including the Computer Crime Act, B.E. 2550 (2007) ("**CCA**"), which covers a wide range of online misconduct, including illegal content, cyberbullying, and identity theft. Moreover, there is also the Royal Decree on the Operation of Digital Platform Service Businesses That Are Subject to Prior Notification, B.E. 2565 (2022) ("**Royal Decree**") issued and supervised by the Electronic Transactions Development Agency ("**ETDA**"). This Royal Decree aims to regulate the provision of digital platform services which includes imposing minimum requirements of the terms and conditions and notification that the provider of digital platform services shall explicitly inform to their users for transparency and fairness.

The regulatory bodies work in cooperation rather than having strictly defined areas of responsibility. For example, an online safety issue involving children's personal data could be jointly handled by the PDPC and MDES. Enforcement powers under these laws, in addition to those in the PDPA per the response for Question No. 43-44, include the ability to issue orders to violators, impose administrative fines, and even pursue legal action which can result in imprisonment for serious offenses.

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

At the time of writing, there is no existing or any draft law in relation to the amendment of the online safety landscape.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

There is no explicit delineation between the principles of data protection by design and data protection by default under the PDPA. However, practical implication may not

differ much even without this delineation as PDPA requires Controllers to abide by the security-related principles already elicited in the PDPA and security measures prescribed in subordinate regulations, and also burdens them with severe liabilities under the law in case of breach. Furthermore, under the law, Controllers by default cannot retain more Personal Data than necessary, or retain Personal Data longer than necessary, to achieve specific purposes supported by specifically identified bases.

16. Are controllers and/or processors of personal data required to maintain any internal 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 from 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.

Currently, there is PDPC notification regarding recording of data processing activity for small Controllers. Under this notification, a Controller who falls under one of the following criteria is considered as a small business enterprise that is exempted from the abovementioned obligations, save for obligation No. 7).

1. small or medium-sized enterprise under the law on medium and small-sized enterprise promotion;
2. community enterprise or its network under the law on community enterprise promotion;
3. social enterprise or a social business group under the law on social enterprise promotion;
4. cooperative, a federation of cooperatives, or a farmers group under the law on cooperatives;
5. foundation, an association, a religious organization or a non-profit organization; or
6. family business or other businesses with the same characteristics.

Such small Controller who is exempted must not be a service provider of storage of computer traffic data under the law on offences relating to computer, unless it is a service provider of internet shop/cafe, which will be exempted.

However, such exemption is not applicable upon the followings events: (i) if such processing activity yields risk to right and freedom of a data subject; (ii) if such processing activity is not conducted only on occasions; or (iii) if such processing activity is for sensitive 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.

17. 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. 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.)

18. Under what circumstances is a controller operating in your jurisdiction 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.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk assessments typically carried out?

The PDPA does not specifically outline such topics. However, there is a draft subordinate law (i.e., draft PDPC notification regarding data protection impact assessment ("**DPIA**")) that touches upon the subject.

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.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and

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 a 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:

1. provide advices to Controllers or Processors, including their employees or service providers with respect to compliance with the PDPA;
2. 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;
3. 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
4. keep confidentiality of the Personal Data known or acquired in the course of his or her performance of duty under the PDPA.

21. 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).

There is no requirement under the PDPA.

22. 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.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

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.

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

The PDPA requires a data processing agreement or provision between a Controller and a Processor. However, the PDPA itself does not specify contract terms to be included.

There is a draft subordinate law (i.e., draft PDPC notification regarding general duties of Processor) which stipulates minimum contract terms that are reflective of Article 28 of the GDPR, namely that a Processor must have specific obligations, such as:

- to process Personal Data only on documented instructions from Controller, including transfers of Personal Data to a third country, unless otherwise specified by the law;
- to ensure that its personnel authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- to give a warranty that it has adequate security measures, both technical and organizational measures, toward Personal Data as required by the law;
- any sub-processing or change of the Processor must be subject to a written authorization from the Controller. Any sub-processor must be bound by contract and have duties of not less than what are specified in an agreement between the Controller and the Processor. The original Processor is, in any case, liable for failure of the sub-processor;
- to provide appropriate technical and organizational measures for fulfilment of the Controller's obligation to respond to requests for exercise of a data subject's rights;
- to assist the Controller in ensuring compliance regarding security and protection of Personal Data and reporting of infringements; and
- to delete, destroy, or return all Personal Data to the Controller upon their instruction and under relevant laws after the end of provision of services relating to processing.

Under the draft notification, if a Processor infringes upon any obligations stipulated in agreement, such Processor will be considered to be a Controller in respect of such processing.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

There is no requirement under the PDPA.

26. 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 terms defined, and what restrictions on their use are imposed, if any?

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.

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are these terms or any similar terms defined?

There is no concept of cross-contextual behavioral advertising under the PDPA.

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such related terms defined, and what restrictions are imposed, if any?

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.

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

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.

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined, and what restrictions are imposed, if any?

“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.)

31. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning (“AI”).

The PDPA does not specifically outline such topic.

32. 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.

33. What security obligations are imposed on data controllers and processors, if any, 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.

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a "security breach"?

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.

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

No, the security requirements as prescribed in the PDPA are generally imposed upon all Controllers and Processors.

Note that there is a draft subordinate law (i.e., draft PDPC notification regarding codes of conduct for Personal Data protection) that mandates mechanisms for any association or entity acting as the representative of Controllers or Processors within an industry to draft codes of conduct for Personal Data protection within such industry and submit those to the Office for consideration.

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

See Question No. 33 for clarification.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

There is no specific legal requirement or guidance under the PDPA regarding dealing with cybercrime. However, the Cybersecurity Act B.E. 2562 (2019) ("**Cybersecurity Act**") provides that upon an event of or anticipation of a cybersecurity threat to any governmental agency or Critical Information Infrastructure agency, the relevant entity must proceed in accordance with its guidelines and standards regarding cybersecurity and immediately inform the Office of National Cyber Security Committee.

38. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

In general, the Cybersecurity Act established two main governmental authorities to supervise cyber security activities, namely:

- the National Cyber Security Committee ("**NCSC**"), which is responsible for prescribing policies and regulations regarding cybersecurity; and
- the Cybersecurity Regulating Committee ("**CRC**"), which is responsible for prescribing codes of conduct or guidelines regarding cybersecurity and monitoring compliance with the regulations, including those prescribed by the NCSC.

39. Do the data protection laws in your jurisdiction provide individual data privacy rights, 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, any exceptions and any other relevant details.

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.

40. Are individual data privacy rights exercisable through the judicial system, enforced by a regulator, or both?

Both. Infringement is subject to civil and criminal penalties that proceed through the judicial system, and also administrative penalties which that proceed through the Office.

41. 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.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is 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.

43. How are data protection laws in your jurisdiction 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.

44. 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.

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

Currently, there is none.

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

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.

47. Are there any identifiable trends 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, it has inspected 16,941 entities during the period from November 2023 to January 2024, and 5,273 data breach incidents were discovered or voluntarily reported. In addition to the inspection, the PDPC has received more than 400 complaints about non-compliance with the PDPA, all of which naturally resulted in some level of investigation. The PDPC reported that as of the February 2024, 101 administrative orders have been imposed on responsible persons in order to address the non-compliance and any damages arising out of such actions.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

Currently, there is none.

Contributors

Mr. Pranat Laohapairoj
Partner
pranat.l@mhm-global.com

Mr. Suphakorn Chueabunchai
Senior Associate
suphakorn.c@mhm-global.com

Ms. Pitchaya Roongroajsataporn
Associate
pitchaya.r@mhm-global.com