COUNTRY
COMPARATIVE
GUIDES 2022

The Legal 500
Country Comparative Guides

Thailand

DATA PROTECTION & CYBER SECURITY LAW

Contributing firm

Chandler MHM Limited

Pranat Laohapairoj

Partner | pranat.l@mhm-blobal.com

Suphakorn Chueabunchai

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

Theerapat Sombatsatapornkul

Senior Associate | theerapat.s@mhm-global.com

Nutcha Panomsuk

Associate | nutcha.p@mhm-global.com

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

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

THAILAND
DATA PROTECTION & CYBER SECURITY LAW

1. Please provide an overview of the legal and regulatory framework governing data protection and privacy 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). Are there any expected changes in the data protection and privacy law landscape in 2022-2023 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

CMHM: 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 will, in practice, be fully enforceable on 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:

<u>Lawful basis</u>:

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. 4.

<u>Rights of Data Subject</u>:

The PDPA provides for 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 data subject, rights of data subject 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. 32.

<u>Security measures</u>:

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. There is no current guideline on provision of such security measures, save for under the notification issued by the Ministry of Digital Economy and Society (“**MDES**”) prescribing minimum data security standards (i.e., administrative safeguards, technical safeguards, and physical safeguards for access control) for Personal Data under the PDPA. The notification is effective during the extended transition period and before the full enforcement of the PDPA (i.e., up until 31 May 2022.)

Please see further explanation in our response to Question No. 26.

Many provisions under the PDPA require enactment of subordinate laws (i.e., royal decrees, MDES notifications, MDES regulations) to prescribe further or more detailed requirements, guidelines, or clarifications. Currently, there are several 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:

- criteria and methods for obtaining of consent from a data subject;
- notification of purposes and details in processing Personal Data;
- security and safety measures for processing Personal Data;
- appropriate protection measures for processing sensitive Personal Data;
- records of data processing activities;
- codes of conduct for protection of Personal Data;
- data protection impact assessments;
- data protection officers;
- general duties of Processors; and
- procedures for receipt of complaints and administrative sanctions.

Please see more regarding these subordinate laws in our response to Question No. 40.

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

CMHM: The PDPA itself does not have any registration or licensing requirements for entities. However, draft subordinate laws may include registration requirements for institutions that act as certifying bodies for Data Protection Officers or those that issue certification of data privacy standards.

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

CMHM: 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.

<u>Ordinary Personal Data</u>

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

<u>Sensitive Personal Data</u>

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.

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

CMHM: Under the PDPA, all Controllers must establish a legal basis for 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.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

CMHM: 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. 4.

6. 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)?

CMHM: 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. 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 is a proposed subordinate law (i.e., the draft PDPC notification regarding criteria and methods for obtainment of consent from data subjects.) Under this proposed draft, the PDPC will publish a guideline or grant support for 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.

7. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

CMHM: Please see the response for Question No. 4 regarding bases for sensitive Personal Data.

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

Currently, there is a draft subordinate law (i.e., draft PDPC notification regarding appropriate protection measures for the processing of sensitive Personal Data) prescribing additional obligations on Controllers for processing sensitive Personal Data (e.g., provision of appropriate protection measures for processing and preparation of sensitive Personal Data protection policies to be disclosed to data subjects, etc.)

8. How do the laws in your jurisdiction address children's personal data or PII?

CMHM: 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 singly 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.

9. Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

CMHM: Please see the key points mentioned under our responses to the Questions Nos. 2-8.

10. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

CMHM: 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 to be 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.

11. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

CMHM: 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 a draft subordinate law (i.e., draft PDPC notification regarding recording of data processing activity.) Under this proposed draft, a Controller who is considered as a small- or medium-size business enterprise (SME) with processing activities of less than 1,000 data subjects is exempted from the abovementioned obligations, save for obligation No. 7). 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 will be stated in the draft subordinate law.

12. Do the laws in your jurisdiction require or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

CMHM: 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.)

13. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

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

14. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

CMHM: 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, etc.;
- 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.

15. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?

CMHM: The PDPA recognizes that there may be a need for many organizations to have a data protection officer, or multiple of them in cases of complex or large volumes of Personal Data. This position, although existing under the PDPA, is not yet mandatory as there is no supplementary regulation to provide guidelines as to what kind of entities need to have a data protection officer. A supplementary regulation (i.e., draft PDPC notification regarding data protection officer) is expected to issue specific characteristics that will require organizations to have a data protection officer, such as routine dealings with sensitive Personal Data and dealing with large-scale processing of Personal Data, which may be fixed at 50,000 data subjects for ordinary Personal Data or 5,000 data subjects for sensitive Personal Data during any 12-month period.

In line with other jurisdictions, data protection officers must be independent and will report directly to top management at such organization and will be at the forefront to deal with any leakage, mistreatment, complaints from data subjects, and liaison with governmental officers, as well as answering internal questions and undertaking monitoring and auditing of the organization's processes.

16. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

CMHM: There is no requirement under the PDPA.

17. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (e.g., posting an online privacy notice).

CMHM: 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.

18. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (e.g., are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

CMHM: 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.

19. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

CMHM: 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.

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

CMHM: 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.

21. Please describe any restrictions on cross-contextual behavioral advertising. How is this term or related terms defined?

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

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

CMHM: There is no definition of or a separate concept for the sale of Personal Data or any other related terms, or any specific restrictions therefor. All general principles and concepts that broadly apply to processing of Personal Data will apply, as applicable, to the sale and similar activities.

23. Please describe any 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?

CMHM: There is no definition of or a separate concept for these activities, or any specific restrictions therefor. All general principles and concepts that broadly apply to 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. 14 for clarification regarding DPIA.

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

CMHM: “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. 4. 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.)

25. Is the transfer of personal data or PII outside the 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? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

CMHM: The PDPA does not prohibit the offshore transfer of Personal Data, but mandates additional obligations on transferors.

By default, Personal Data can be transferred offshore only to jurisdictions that are pre-approved to have adequate Personal Data protection measures, such approval being in a form of a list of countries and organizations, which, as of today, has yet to be prescribed by the PDPC. If a particular destination is not pre-approved, transferors must qualify for one of the available exemptions, including compliance with law, obtainment of consent, performance of contract, etc. Another useful exemption is intra-group transfers under a Binding Corporate Rule (“**BCR**”) that has been approved by the Office. A similar exemption is transfers under a Standard Contractual Clause (“**SCC**”), which must also be approved by the Office.

To further clarify a SCC, under a draft subordinate law (i.e., the draft PDPC notification regarding rules and policies for protection of Personal Data transferred overseas), contents of the SCC include representations and warranties from a transferor and a transferee regarding their compliance to relevant data protection laws, especially that the transferee must procure appropriate security measures, etc.

26. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

CMHM: 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 a draft supplementary regulation (i.e., draft PDPC notification regarding security and safety measures for processing of Personal Data) mandating Controllers and Processors to arrange for appropriate organizational and technical measures, as follows:

- pseudonymization or encryption of Personal Data;
- maintenance of security and safety measures for the system or service of Personal Data processing via principles of confidentiality, integrity, and availability;
- ability to immediately recover systems or services of Personal Data processing upon infringement; and
- efficiency examinations and assessment for such organizational and technical measures.

Both Controllers and Processors must also inform their own employees of such measures.

27. Do the laws in your jurisdiction address security breaches and, if so, how does the law define "security breach"?

CMHM: There is no specific definition of "security breach" under the PDPA. However, Controllers must abide by principles and notification requirement as outlined above in Question No. 26.

28. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

CMHM: 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.

29. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

CMHM: See Question No. 26 for clarification.

30. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

CMHM: 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.

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

CMHM: 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.

32. Do the 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 the rights, how they are exercised, what exceptions exist and any other relevant details.

CMHM: The PDPA provides for the following individual data privacy rights:

1. 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.
2. 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.
3. 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.
4. Right to correct incomplete or inaccurate parts of Personal Data, although a Controller may verify the accuracy of new information provided by data subjects.
5. 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.
6. 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.
7. 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.
8. Right to withdraw consent at any time. However, withdrawal of consent will not have any effect on the Controller's previous data processing.

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

CMHM: 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.

34. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

CMHM: 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.

Under a draft subordinate law (i.e., draft PDPC notification regarding procedure for receipt of complaint and administrative sanctions), a data subject is entitled to the right to file a complaint to the authority only when such complaint has been filed to a relevant Controller or Processor, as the case may be, but no actions to remedy have been taken within 30 days.

35. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

CMHM: 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.

36. How are the laws governing privacy and data protection enforced?

CMHM: 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.

37. What is the range of sanctions (including fines and penalties) for violation of these laws?

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

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.

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.

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.

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

CMHM: Currently there is none.

39. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

CMHM: 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.

40. Are there any proposals for reforming data protection or cybersecurity laws currently under review? Please provide an overview of any proposed changes and

how far such proposals are through the legislative process.

CMHM: In February and June of 2021, the Office arranged for unofficial public hearing sessions for subordinate laws, which include following key topis:

- criteria and methods for obtaining consent from data subjects;
- notification of purposes and details for processing Personal Data;
- security and safety measures for processing Personal Data;
- appropriate protection measures for processing sensitive Personal Data;
- recording of data processing activity;
- codes of conduct for Personal Data protection;
- data protection impact assessments;
- data protection officers;
- general duties of Processors; and
- procedures for receipt of complaints and administrative sanctions.

The Office has already consolidated results of the hearings into key summaries of each proposed draft subordinate law and proposed the results to the PDPC for further consideration.

Contributors

Pranat Laohapairoj **Partner**	pranat.l@mhm-blobal.com	
Suphakorn Chueabunchai **Senior Associate**	suphakorn.c@mhm-global.com	
Theerapat Sombatsatapornkul **Senior Associate**	theerapat.s@mhm-global.com	
Nutcha Panomsuk **Associate**	nutcha.p@mhm-global.com	