International
Comparative
Legal Guides

Practical cross-border insights into data protection law

Data Protection 2022

Ninth Edition

Contributing Editors:
Tim Hickman & Dr. Detlev Gabel
White & Case LLP

ICLG.com

Expert Analysis Chapters

1 **The Rapid Evolution of Data Protection Laws**
Tim Hickman & Dr. Detlev Gabel, White & Case LLP

7 **Data Breach Response Strategy**
Daniela Fábián Masoch, FABIAN PRIVACY LEGAL GmbH

12 **Initiatives to Boost Data Business in Japan**
Takashi Nakazaki, Anderson Mōri & Tomotsune

19 **Brave New (Virtual) World**
Jenny L. Colgate & Caitlin M. Wilmot, Rothwell Figg

25 **Privacy Risks in M&A**
Kelly Hagedorn, Julia Apostle, Dr. Christian Schröder & Colette Deamer
Orrick, Herrington & Sutcliffe LLP

31 **"Selling" or "Sharing" Personal Information Under California Law**
Paul Lanois, Fieldfisher

Q&A Chapters

35 **Australia**
MinterEllison: Anthony Borgese, Helen Cheung, Zoe Zhang & Tony Issa

49 **Belgium**
Sirius Legal: Bart Van den Brande

61 **Brazil**
ASBZ Advogados: Luiza Sato, Guilherme Braguim, Igor Baden Powell & Geórgia Costa

71 **Canada**
McMillan LLP: Lyndsay A. Wasser & Kristen Pennington

84 **China**
King & Wood Mallesons: Susan Ning & Han Wu

97 **Denmark**
Lund Elmer Sandager: Torsten Hylleberg, Emilie Ipsen & Anders Linde Reislev

108 **France**
White & Case LLP: Clara Hainsdorf & Bertrand Liard

118 **Germany**
Noerr Partnerschaftsgesellschaft mbB: Daniel Ruecker, Julian Monschke, Pascal Schumacher & Korbinian Hartl

127 **Greece**
Nikolinakos & Partners Law Firm: Dr. Nikos Th. Nikolinakos, Dina Th. Kouvelou & Alexis N. Spyropoulos

139 **India**
Khaitan & Co LLP: Harsh Walia & Supratim Chakraborty

150 **Indonesia**
H & A Partners in association with Anderson Mōri & Tomotsune: Steffen Hadi, Sianti Candra & Dimas Andri Himawan

162 **Isle of Man**
DQ Advocates Limited: Kathryn Sharman & Sinead O'Connor

172 **Israel**
Naschitz, Brandes, Amir & Co., Advocates: Dalit Ben-Israel & Maya Peleg

187 **Italy**
FTCC Studio Legale Associato: Pierluigi Cottafavi & Santina Parrello

198 **Japan**
Mori Hamada & Matsumoto: Hiromi Hayashi & Masaki Yukawa

210 **Korea**
D'LIGHT Law Group: Iris Hyejin Hwang & Hye In Lee

220 **Mexico**
OLIVARES: Abraham Diaz Arceo, Gustavo Alcocer & Carla Huitron

229 **Nigeria**
Udo Udoma and Belo-Osagie: Jumoke Lambo & Chisom Okolie

241 **Norway**
Wikborg Rein Advokatfirma AS: Gry Hvidsten & Emily M. Weitzenboeck

254 **Pakistan**
S. U. Khan Associates Corporate & Legal Consultants: Saifullah Khan & Saeed Hasan Khan

263 **Peru**
Iriarte & Asociados: Erick Iriarte Ahón & Fátima Toche Vega

272 **Poland**
Leśniewski Borkiewicz & Partners S.K.A.: Grzegorz Leśniewski, Mateusz Borkiewicz & Jacek Cieśliński

Q&A Chapters Continued

285 **Saudi Arabia**
Hammad & Al-Mehdar Law Firm: Suhaib Hammad

294 **Senegal**
LPS L@w: Léon Patrice SARR

303 **Singapore**
Drew & Napier LLC: Lim Chong Kin

319 **Sweden**
Synch Advokat AB: Josefin Riklund & Johannes Hammarling

329 **Switzerland**
Homburger AG: Dr. Gregor Bühler, Luca Dal Molin & Dr. Kirsten Wesiak-Schmidt

339 **Taiwan**
Lee and Li, Attorneys at Law: Ken-Ying Tseng & Sam Huang

349 **Thailand**
Chandler MHM Limited: Pranat Laohapairoj & Atsushi Okada

357 **Turkey**
SEOR Law Firm: Okan Or & Yesim Odabas

367 **United Arab Emirates**
Bizilance Legal Consultants: Saifullah Khan & Saeed Hasan Khan

377 **United Kingdom**
White & Case LLP: Tim Hickman & Joe Devine

389 **USA**
White & Case LLP: F. Paul Pittman, Kyle Levenberg & Shira Shamir

Thailand


Pranat Laohapairoj


Atsushi Okada

Chandler MHM Limited

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Personal Data Protection Act, B.E. 2562 (2019) ("**PDPA**") is the principal legislation in Thailand. However, the effective date of most parts of the PDPA was recently further postponed for the second time by Royal Decree for another year, and the PDPA will, according to such Royal Decree, be fully effective and enforceable on 1 June 2022.

1.2 Is there any other general legislation that impacts data protection?

No, there is not.

1.3 Is there any sector-specific legislation that impacts data protection?

There are a few other industry-specific regulations that may touch upon data protection and overlap with the PDPA, such as the regulation governing telecommunication.

1.4 What authority(ies) are responsible for data protection?

The Personal Data Protection Committee ("**PDPC**") is responsible for data protection.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  The Personal Data Protection Committee ("**PDPC**").
- "**Processing**"
  There is no definition provided by law. In general, processing means any treatment of personal data.
- "**Controller**"
  A natural or juristic person having the power and duties to make decisions regarding the collection, use or disclosure of Personal Data.
- "**Processor**"
  A natural or juristic person who operates in relation to the collection, use or disclosure of Personal Data pursuant to the orders given by or on behalf of a Controller – such person not being the Controller.
- "**Data Subject**"
  There is no definition provided by law.
- "**Sensitive personal data**"
  There is no definition provided by law. However, explicit consent is necessary for collecting Personal Data pertaining to racial or ethnic origin, political opinions, cultic, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disabilities, trade union information, genetic data, biometric data or any data which may affect the data subject in the same manner as prescribed by the PDPC, subject to some exceptions.
- "**Data Breach**"
  There is no definition provided by law.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PDPA applies to the collection, use or disclosure of Personal Data of data subjects located in Thailand by businesses in other jurisdictions in the following circumstances:

(1) where the business offers goods or services to data subjects located in Thailand; or
(2) where the business monitors the behaviour of data subjects taking place in Thailand.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  The Controller must inform data subjects of the following details prior to or at the time of collecting Personal Data:
  (1) the purpose of the collection, use or disclosure of Personal Data;
  (2) a notification stating that data subjects must provide their Personal Data for compliance with a legal obligation, for the performance of a contract, or to enter into a contract, including notification of the possible effects in cases where data subjects do not provide such Personal Data;
  (3) the Personal Data to be collected and the period for which the Personal Data will be retained;

(4) the categories of persons or entities to whom the collected Personal Data may be disclosed;
(5) the information, address and contact channel details of the Controller and, if applicable, of the Controller's representative or Data Protection Officer; and
(6) the data subjects' rights.

- **Lawful basis for processing**
  The Controller shall not process Personal Data without the consent of data subjects, unless:
  (1) it is for a purpose relating to the preparation of historical documents or archives for public interest, or for a purpose relating to research or statistics, in which suitable measures to safeguard data subjects' rights and freedoms are put in place and in accordance with the notification as prescribed by the PDPC;
  (2) it is for preventing or suppressing a danger to a person's life, body or health;
  (3) it is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
  (4) it is necessary for the performance of a task carried out in the public interest by the Controller, or it is necessary for the exercising of the official authority vested in the Controller;
  (5) it is necessary for the legitimate interests of the Controller or any natural or juristic persons other than the Controller, except where such interests are overridden by the fundamental rights of the data subject; or
  (6) it is necessary for compliance with a law to which the Controller is subject.
- **Purpose limitation**
  The collection, use or disclosure of Personal Data shall not be conducted in a manner that is different from the purpose previously notified to data subjects, unless data subjects have been informed of such new purpose and the consent is obtained prior to the time of such processing or otherwise permitted by law.
- **Data minimisation**
  The collection of Personal Data shall be limited to the extent necessary in relation to the lawful purpose of the Controller.
- **Proportionality**
  The Personal Data to be collected shall be limited to only those absolutely necessary for fulfilling the purpose outlined to data subjects.
- **Retention**
  The Controller must inform data subjects of the data retention period, prior to or at the time of collecting Personal Data. If it is not possible to specify the retention period, the expected data retention period according to the data retention standard must be specified. The Controller must put in place the examination system for erasure or destruction of Personal Data when the retention period ends, when Personal Data is irrelevant or beyond the purpose necessary for which it has been collected, or when data subjects exercise rights in accordance with the PDPA, subject to some exceptions.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  Data subjects have the right to request access to and obtain a copy of their Personal Data. The Controller may reject such request only where it is permitted by law or pursuant to a court order, and where such actions would adversely affect the rights and freedoms of others.
- **Right to rectification of errors**
  The Controller shall ensure that Personal Data remains accurate, up to date, complete and not misleading. Where a data subject requests the Controller to act in compliance therewith and the Controller does not take any action regarding such request, the Controller shall record such request together with the reasons for its non-compliance.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to request the Controller to erase or destroy their Personal Data, or anonymise their Personal Data, in cases where one of the following grounds applies:
  (1) such Personal Data is no longer necessary in relation to the purposes for which it was processed;
  (2) data subjects withdraw consent on which the processing is based, and where the Controller has no legal ground for such processing;
  (3) data subjects exercise the right to object to processing of their Personal Data as described below; or
  (4) such Personal Data has been unlawfully collected, used or disclosed.
- **Right to object to processing**
  Data subjects have the right to object to the collection, use or disclosure of their Personal Data under the following circumstances:
  (1) such Personal Data is collected with the exemption to consent requirements, unless the Controller can prove that: (a) there is a compelling legitimate ground for processing such Personal Data; or (b) processing of such Personal Data is carried out for the establishment, compliance or exercise of legal claims, or defence of legal claims;
  (2) such Personal Data is processed for the purpose of direct marketing; or
  (3) such Personal Data is processed for the purpose of scientific, historical or statistic research, unless it is necessary for the performance of a task carried out for reasons of public interest by the Controller.
- **Right to restrict processing**
  Data subjects have the right to request the Controller to restrict the use of their Personal Data in the following circumstances:
  (1) when the Controller is pending an examination process in accordance with the data subjects' request to rectify errors;
  (2) when such Personal Data shall be erased or destroyed, but the data subjects request the restriction of the use of such Personal Data instead;
  (3) when it is no longer necessary to retain such Personal Data for the purposes of such collection, but the data subjects have, by necessity, requested further retention for the purposes of the establishment, compliance or exercise of legal claims, or defence of legal claims; or
  (4) when the Controller is pending verification or pending examination with regard to the data subjects' request to object to processing.
- **Right to data portability**
  Data subjects have the right to receive their Personal Data from the Controller if the processing is based on consent or the performance of contracts. The Controller shall arrange such Personal Data to be in a format that is readable or commonly used by way of automatic tools or equipment, and can be used or disclosed by automated means. Data subjects are also entitled to:

(1) request the Controller to send or transfer their Personal Data in such formats to other Controllers if this can be done by automatic means; or
(2) request to directly obtain their Personal Data in such formats that the Controller sends or transfers to other Controllers, unless it is impossible to do so because of technical circumstances.

- **Right to withdraw consent**
  Data subjects may withdraw their consent at any time.
- **Right to object to marketing**
  Data subjects may object to direct marketing. Note that in general, direct and other types of marketing will require their own lawful basis, which arguably can be a legitimate interest in some cases, or consent in other cases.
- **Right protecting against solely automated decision-making and profiling**
  The law is silent on this point, but based on other provisions, any automated decision-making and profiling will be treated in the same way as other manners of data processing and will require their own lawful basis.
- **Right to complain to the relevant data protection authority(ies)**
  Data subjects may contact and complain to the authority at will.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

The law is silent on this point.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

Processing of Personal Data of a minor of up to 10 years of age will necessitate the guardian to be involved in the same way as processing an adult's Personal Data. Processing of Personal Data of a minor from the age of 11 will be dealt with in the same manner as outlined above, but with a categorical exemption that such minor will be empowered to unilaterally deal with the processing of his/her own Personal Data that is suitable to his/her age, including providing consent.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, there is no such obligation based on the current legislation. However, in an event of a certain serious data breach, the Controller must notify the authority of such breach within 72 hours.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The rules regarding notification in an event of a data breach have not been promulgated.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

The rules regarding notification in an event of a data breach have not been promulgated.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

The Controller must notify the authority in case of a data breach. However, it is also arguably possible according to the current wording of the law, but still pending the additional rules, that a local agent may do this on behalf of the foreign Controller.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The rules regarding notification in the event of a data breach have not been promulgated.

7.6 What are the sanctions for failure to register/notify where required?

The administrative fine for failure to notify the authority in the event of a data breach (and also data subjects in the event of a data breach which has a high possibility of effects on the data subjects) is up to THB 3 million.

7.7 What is the fee per registration/notification (if applicable)?

There is no fee in an event of notification for a data breach.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable in our jurisdiction.

7.9 Is any prior approval required from the data protection regulator?

This is not applicable in our jurisdiction.

7.10 Can the registration/notification be completed online?

The rules regarding notification in the event of a data breach have not been promulgated.

7.11 Is there a publicly available list of completed registrations/notifications?

As of today, there is no such list. The rules regarding notification in the event of a data breach have not been promulgated.

7.12 How long does a typical registration/notification process take?

The rules regarding notification in the event of a data breach have not been promulgated.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer is mandatory in the following circumstances:

(1) the Controller or Processor is a public authority as prescribed by the PDPC;

(2) the activities of the Controller or Processor in the collection, use or disclosure of Personal Data require regular monitoring of Personal Data or the system, by reason of having a large number of Personal Data as prescribed by the Committee; or

(3) the core activity of the Controller or Processor is the collection, use or disclosure of sensitive Personal Data (i.e., Personal Data pertaining to racial or ethnic origin, political opinions, cultic, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disabilities, trade union information, genetic data, biometric data, or any data which may affect the data subject in the same manner as prescribed by the PDPC).

Note that the PDPC is in the process of prescribing the numerical thresholds of personal data queries within each entity, which will require appointment of the DPO.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The administrative fine is up to THB 1 million.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The Controller or Processor is prohibited from dismissing or terminating the Data Protection Officer's employment as the Data Protection Officer performs his or her duties under the PDPA. In the event that there is any problem when performing the duties, the Data Protection Officer must be able to directly report to the highest management person of the Controller or Processor.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

In the event that the Controllers or Processors are in the same affiliated business or are in the same group of undertakings, in order to jointly operate the business or group of undertakings as prescribed by the PDPC, such Controllers or Processors may jointly designate a single Data Protection Officer. In this regard, each establishment of the Controller or Processor in the same affiliated business or in the same group of undertakings must be able to easily contact the Data Protection Officer.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

It is expected that the PDPC will prescribe and announce the qualifications of the Data Protection Officer by taking into account the knowledge or expertise with respect to the protection of Personal Data.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

The Data Protection Officer shall have the following duties:

(1) give advice to the Controller or Processor, including the employees or service providers of the Controller or Processor with respect to compliance with the PDPA;

(2) investigate the performance of the Controller or Processor, including the employees or service providers of the Controller or Processor with respect to the collection, use or disclosure of Personal Data for compliance with the PDPA;

(3) coordinate and cooperate with the PDPC in circumstances where there are problems with respect to the collection, use or disclosure of Personal Data undertaken by the Controller or Processor, including the employees or service providers of the Controller or Processor with respect to compliance with the PDPA; and

(4) keep confidential Personal Data known or acquired in the course of his or her performance of duty under the PDPA.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The Controller and Processor must disclose the information of the Data Protection Officer, including contact address and contact channels, to the PDPC.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Controller and Processor must disclose the information of the Data Protection Officer, including the contact address and contact channels, to data subjects. Data subjects shall be able to contact the Data Protection Officer with respect to the collection, use or disclosure of their Personal Data and the exercise of rights of data subjects under the PDPA.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

In the circumstance where Personal Data is provided to a Processor, the Controller shall have a data processing agreement with the Processor to ensure that the Processor will follow and comply with its duties under the PDPA and the Controller must take action to prevent the Processor from using or disclosing such Personal Data unlawfully or without authorisation. The Processor may carry out the activities related to processing of Personal Data only pursuant to the instruction given by the Controller, except where such instruction is contrary to laws.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The PDPA does not specifically refer to the formalities of or items to be covered by data processing agreements.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

There is no special legislation restricting digital marketing. Depending on the circumstances, direct marketing may require consent, but under some circumstances may be carried out under a legitimate interest basis.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The law does not make any difference between the two types.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

This is not applicable in our jurisdiction.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, they do.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

This is yet to be witnessed, as the last member of the PDPC has very recently been appointed, thereby completing the composition of the PDPC.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

The purchase of a marketing list must be on a lawful basis, whatever that may be under the specific circumstance.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum administrative penalty is THB 5 million.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There is no specific legislation focused on cookies. Cookies are treated as a simple collection and processing of Personal Data under the PDPA, so long as they enable the identification of data subjects, whether directly or indirectly.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

No, they do not.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

As of today, there has been no enforcement, as the law is yet to be fully effective and enforceable. The law will be effective as of 1 June 2022.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

The maximum administrative penalty is THB 5 million.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

It is permitted to transfer Personal Data to destination countries or international organisations that have an adequate data protection standard, which will be prescribed by the PDPC.

If the destination country is not designated by the PDPC as having an adequate data protection standard, an international data transfer may be permitted under the following circumstances:

(1) where it is for compliance with the law;
(2) where the consent of data subjects has been obtained, provided that the data subject has been informed of the inadequate Personal Data protection standards of the destination country or international organisation;
(3) where it is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
(4) where it is for compliance with a contract between the Controller and other natural or juristic persons for the interests of the data subject;
(5) where it is to prevent or suppress a danger to the life, body or health of the data subject or other persons, when the data subject is incapable of giving consent at such time; or
(6) where it is necessary for carrying out activities in relation to substantial public interest.

Otherwise, the Controller or Processor may transfer Personal Data to a foreign country if the Controller or Processor provides suitable protection measures which enable the enforcement of data subjects' rights, including effective legal remedial measures

according to the rules and methods which will be prescribed and announced by the PDPC.

Further, there is a special mechanism applicable to an international data transfer between group companies: in the event that the foreign Controller or Processor has put in place a Personal Data protection policy regarding the transferring of Personal Data, and is in the same affiliated business, or is in the same group of undertakings, in order to jointly operate the business or group of undertakings, an international data transfer is permitted if such policy has been reviewed and certified by the PDPC. However, the criteria of such Personal Data protection policy have not yet been established.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

As the supplementary rules are not yet available, the simplest and safest form of basis now is consent or contractual performance.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

As the supplementary rules are not yet available, there is no requirement for notification.

12.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in Schrems II (Case C-311/18)?

As the PDPA is not fully effective and the PDPC has yet to be officially announced in the Gazette, there is none.

12.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses published on 4 June 2021?

As the PDPA is not fully effective and the PDPC has yet to be officially announced in the Gazette, there is none.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The law is silent on this, but the general rule is that anyone can submit any complaint to the authority at any time, as an affected data subject or concerned person.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

The law is silent on this point, but both types of reports are acceptable.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

There is no requirement to register with or notify the authority. However, in general, the collection and processing of Personal Data via CCTV for security purposes will require simple notification to the public (visitors and internal personnel). There is no rule on what form the notice must be in, but the general principle under the PDPA is that notification must be clear, reasonable and visible. As of now, it is generally agreed that a clear sign at the entrance to the premises and a detailed notification in the privacy policy of the premises are sufficient.

14.2 Are there limits on the purposes for which CCTV data may be used?

Lacking specific consent, CCTV recordings can only be used for security purposes.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Monitoring that is reasonable and reasonably expected by the employees, and which is not unduly intrusive, can be undertaken.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Monitoring, as long as it abides by the characteristics stated above in question 14.1, can be undertaken under legitimate interest or a contractual performance basis. However, some employers may choose consent to be the basis to increase clarity, but this may mean easy revocation by the employees as well. In either case, proper notification is required, whether in the consent form or in the employee data protection policy.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

None. Only the data subjects – in this case the employees – need to be notified.

15.4 Are employers entitled to process information on an employee's COVID-19 vaccination status?

The processing of an employee's vaccination status will require a proper basis. As vaccination records are treated as Sensitive Personal Data, in general, consent is one option for a proper basis, but there may be other exemptions depending on the specific circumstance of the employment and the pandemic.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The Controller and Processor must provide appropriate security measures for preventing unauthorised or unlawful loss, access, use, alteration, correction or disclosure of Personal Data.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The Controller must notify the PDPC 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 the rights and freedoms of data subjects. The notification and the exemption from the notification shall be made in accordance with the rules and procedures which will be set forth by the PDPC.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

If the Personal Data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Controller must also notify the Personal Data breach and the remedial measures to the data subjects without delay. The notification and the exemption from the notification shall be made in accordance with the rules and procedures which will be set forth by the PDPC.

16.4 What are the maximum penalties for data security breaches?

The maximum administrative penalty is THB 3 million.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

(a) **Investigative Powers**: Upon receiving complaints, the PDPA expert committee – a sub-committee appointed by the PDPC, can request for any document or information from any person related to the issue or summon them to give testimony.

(b) **Corrective Powers**: Before ordering a fine, the PDPA expert committee may request the Controller or the Processor to rectify the violation first.

(c) **Authorisation and Advisory Powers**: Same as (b). The expert committee may issue a warning first before ordering a fine, or simply issue advice for good practices.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The maximum administrative fine under the PDPA is THB 5 million.

(e) **Non-compliance with a data protection authority**: Any person who does not comply with the expert committee's order (as mentioned in (a)) shall be subject to an administrative fine of not more than THB 500,000.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Yes, and a court order is not required.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

To date, there is no precedent case.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

There is no precedent case as of today, but in theory the PDPC can attempt to enforce against offshore entities; whether such enforcement would be fruitful is yet to be seen.

18 E-discovery / Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

There is no law on this, meaning it is up to each business to decide whether compliance is in its best interest.

18.2 What guidance has/have the data protection authority(ies) issued?

As of today, no such guidance has been released.

19 Trends and Developments

19.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

As of today, there are no trends, and it is unclear what trends will emerge in the future.

19.2 What "hot topics" are currently a focus for the data protection regulator?

As of today, this point is unclear.

Pranat Laohapairoj is a Partner at Chandler MHM Ltd. and has been with the firm since 2012. He has worked with Thai and international clients on merger and acquisition, anti-trust, corporate, anti-corruption, compliance, and data protection, providing advice and services involving due diligence (for merger and acquisitions, anti-trust, and data protection), deal structuring, negotiation, contract drafting, deal execution, in-house training and public seminars (for anti-bribery, anti-trust, and data protection), internal misconduct investigations, anti-trust defence, and translation. He regularly works on both domestic Thai deals as well as on cross-border investments, and his experience spans multiple sectors, including oil and gas, mining and metal, automotive and automotive parts and support, manufacturing, wholesale and retail, consumer products, chemical, electronics, real estate and shared space, gaming and information technology, import and export, leasing, land and marine transport, hotel management, heavy machinery and machinery rental, investment and marketing consultancy, recruitment, pharmaceuticals and supplements, and food and beverage industries. He is admitted to the Bar of the State of New York.

Chandler MHM Limited
36th Floor, Sathorn Square Office Tower
98 North Sathorn Road
Silom, Bangrak, Bangkok 10500
Thailand

Tel: +66 2 009 5000
Email: pranat.l@mhm-global.com
URL: www.chandlermhm.com

Atsushi Okada is a Partner in Mori Hamada & Matsumoto's office in Tokyo and is Co-Head of the Firm's Data Security, IP, AI/IoT, Fintech and Healthcare practices. He regularly advises international and domestic companies in various industries on compliance with data protection/privacy regulations, including cross-border personal data transfer, and compliance with data protection laws in Japan, Europe, the U.S. and Asian countries. He has been recognised in Japan in major ranking tables, such as *Chambers Global*, *Chambers Asia-Pacific*, *The Legal 500 Asia Pacific*, *Asialaw Leading Lawyers*, *The Best Lawyers in Japan* and *IAM Patent 1000*.

Mori Hamada & Matsumoto
Marunouchi Park Building
2-6-1 Marunouchi
Chiyoda-ku Tokyo 100-8222
Japan

Tel: +81 3 5 220 1821
Email: atsushi.okada@mhm-global.com
URL: www.mhmjapan.com

Chandler MHM and Mori Hamada & Matsumoto recognise the importance of technology in today's constantly evolving technology-dependent world and the impact it has on business. Our priority is to help our clients navigate through the legal and regulatory challenges in the technology sector. Our team, which is based in Thailand and Japan, has extensive experience advising on corporate matters for technology companies including M&A. We can advise across a broad spectrum of technology-related areas including cyber security, data privacy, e-commerce, e-sports, fintech and health tech. With our strong on-the-ground presence in Asia and a global network, our experienced legal team will assist you in taking advantage of the opportunities presented by the fast-evolving technology landscape, while mitigating the associated risks.

www.chandlermhm.com / www.mhmjapan.com

MORI HAMADA & MATSUMOTO

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group