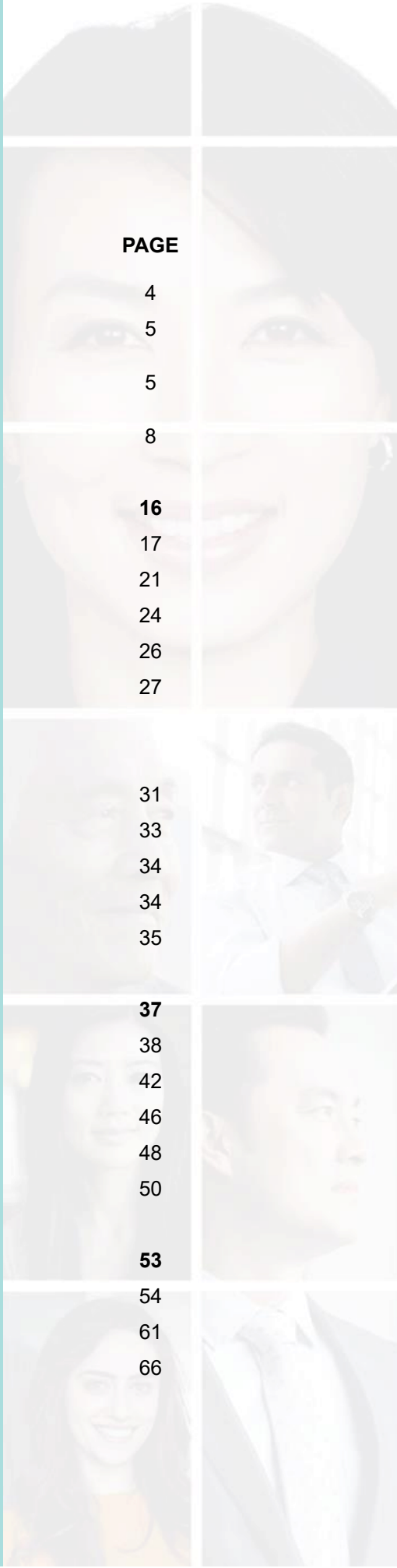
DREW NETWORK ASIA

DNA ASEAN GUIDE TO:

DATA PROTECTION AND CYBERSECURITY REGULATION IN SOUTHEAST ASIA

Edited by Lim Chong Kin and David N. Alfred

CONTENTS



1. OVERVIEW AND ASEAN FRAMEWORKS

A) Southeast Asia and ASEAN

Southeast Asia is a very diverse region with more than 680 million people across the following 11 countries:

- Brunei Darussalam
- Cambodia
- Indonesia
- Lao People's Democratic Republic
- Malaysia
- Myanmar
- The Philippines
- Singapore
- Thailand
- Timor-Leste
- Vietnam

All but one of the above-mentioned countries are members of the Association of Southeast Asian Nations ("**ASEAN**"), a regional grouping that aims to promote economic growth, social progress, cultural development and regional peace and stability. The sole exception, Timor-Leste, is in the process of joining ASEAN following the in-principle agreement of the other ASEAN members in November 2022 to admit it as the eleventh member of ASEAN.

Geographically, Southeast Asia stretches more than 5,000 km from East to West (longer than the distance across continental USA) and covers an area of more than 4.5 million square kilometres. It includes the world's two largest archipelagic nations, Indonesia and the Philippines, as well as one of the world's smallest nation states, Singapore. Each country in Southeast Asia exhibits distinctive social and cultural elements and there are also elements that are blended across neighbouring countries and sub-regions.

B) Data Protection and Cybersecurity Laws in Southeast Asia: An Overview

The data protection landscape in Southeast Asia has evolved significantly over the past decade. Prior to 2010, none of the countries in Southeast Asia had enacted a general data protection law. This changed in the early 2010s when Malaysia, the Philippines and Singapore enacted their first general data protection laws. They were followed by Laos (for electronic data), Thailand, Indonesia and Vietnam in 2017, 2019, 2022 and 2023 respectively (see Table 1 below).

Other jurisdictions in Southeast Asia have also taken steps towards enacting a general data protection law. These include Brunei Darussalam and Cambodia, both of which have issued public consultations on upcoming laws in recent years. Some jurisdictions, including Cambodia and Myanmar, and have enacted sector-specific requirements (such as requirements relating to e-commerce).

Table 1. Data protection laws in Southeast Asia (excluding sector-specific laws)

Jurisdiction	Law	Year Enacted
Brunei	Personal Data Protection Order	Upcoming
Cambodia	Personal Data Protection Law	Upcoming
Indonesia	Law on Protection of Personal Data (Law No. 27 of 2022)	2022
Laos	Law on Electronic Data Protection	2017
Malaysia	Personal Data Protection Act 2010 (Act 709)	2010
Myanmar	Law Protecting the Privacy and Security of Citizens	2017
Philippines	Data Privacy Act of 2012 (Republic Act 10173)	2012
Singapore	Personal Data Protection Act 2012 (No. 26 of 2012)	2012
Thailand	Personal Data Protection Act 2019 (B.E. 2562 (2019))	2019
Vietnam	Decree on Personal Data Protection (Decree No. 13/2023/ND-CP)	2023

Data protection laws in the region are also continuing to develop. Singapore amended its law in 2021/2022 to introduce several new provisions and provide for increased penalties for contraventions. Both Malaysia and the Philippines have consulted on proposed amendments to their respective laws.

While there are some similarities among the various data protection laws in Southeast Asia, there are also significant differences due to a diversity of approaches taken and a desire in each jurisdiction to address local considerations. For example, many of the laws have requirements relating to the following:

- Limits on processing of personal data (e.g. requirements relating to purpose of processing, notification of purposes and legal bases for processing);
- Care of personal data (e.g. requirements relating to security, retention and accuracy of personal data); and

- Data subject rights (e.g. requirements relating to access to and correction of personal data).

However, there are differences among the various jurisdictions as to the scope of the above-mentioned requirements (e.g. in relation to legal bases for processing or data subject rights that are available in particular jurisdictions). There are also other requirements which may be found in some, but not all of the laws (e.g. requirements relating to cross-border data transfers and notification of data breaches).

Furthermore, while the data protection authorities in Malaysia, the Philippines and Singapore have administered and enforced their respective laws for more than 10 years, the other jurisdictions are in the starting stages of establishing their data protection authorities and the required implementing regulations and frameworks for their laws. As such, it remains to be seen how laws in those jurisdictions will be applied in practice. Fortunately, as discussed below, there are also a number of regional efforts aimed at standardising the approach taken across the region.

In relation to cybersecurity, there are also significant differences in the approaches taken by different jurisdictions. In Singapore, for example, a key focus is on the regulation of cybersecurity in respect of critical information infrastructure. Other jurisdictions such as the Philippines do not have regulations that specifically deal with critical information infrastructure. Instead, regulations concerning cybercrimes and cybersecurity practices can be found in various cybercrime and criminal laws. Some jurisdictions such as Indonesia also do not have dedicated cybersecurity laws but rather, information and systems-related laws that contain general provisions pertaining to cybersecurity (see Table 2 below).

Table 2. Cybersecurity laws in Southeast Asia (excluding sector-specific laws)

Jurisdiction	Law	Year Enacted
Brunei	Cybersecurity Act	2023
Cambodia	Cybersecurity Law	Upcoming
Indonesia	Law on Electronic Information and Transactions (Law No. 11 of 2008)	2008
Malaysia	Cyber Security Act	Upcoming

Jurisdiction	Law	Year Enacted
Philippines	Cybercrime Prevention Act of 2012	2012

Singapore	Cybersecurity Act 2018	2018
Thailand	Cybersecurity Act 2019 (B.E. 2562 (2019))	2019
Vietnam	Law on Cybersecurity (No. 24/2018/QH14)	2018

At present, Malaysia, Cambodia and Myanmar do not have a dedicated cybersecurity law but have indicated that they are in the processing of developing such a law. The Philippines also has an upcoming Critical Information Infrastructure Protection Act.

The various data protection and cybersecurity laws in Southeast Asia are discussed in detail in the following chapters of this guide.

C) Regional Cooperation at ASEAN

At a regional level, the transformation of the region's digital economy, which is estimated to grow to US$1 trillion by 2030[1], has propelled collaborative efforts in respect of several areas including data protection and digital governance. This has led to the development and endorsement of several key frameworks by ASEAN to facilitate a unified approach within the region. Several of these efforts have been led by the ASEAN Digital Ministers Meeting (DGMIN), previously known as the ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN).

i. ASEAN Framework on Personal Data Protection

A key foundational framework in ASEAN is the *ASEAN Framework on Personal Data Protection* ("**PDP Framework**")[2] which was entered into by ASEAN TELMIN in 2016. While the PDP Framework is not legally binding (Paragraph 2), it states that it "*serves to strengthen the protection of personal data in ASEAN and to facilitate cooperation among the Participants [ASEAN member states], with a view to contribute to the promotion and growth of regional and global trade and the flow of information*" (Paragraph 1).

The PDP Framework seeks to achieve its objective by encouraging Participants to adopt a common set of personal data protection principles in their domestic law ("**PDP Principles**") while continuing to ensure and

[1] https://www.weforum.org/agenda/2024/01/asean-building-trust-digital-economy/#:~:text=One%20such%20huge%20opportunity%20is,2023%20and%204.8%25%20in%202024.
[2] Available at https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf.

facilitate free flow of information among ASEAN member states (Paragraph 3.1).

The PDP Principles include the following (Paragraph 6):

(1) **Consent, Notification and Purpose**: Collection, use and disclosure of personal data is permitted only for purposes that a reasonable person would consider appropriate and either with prior notification to, and the consent of, the individual concerned or where otherwise permitted or required under domestic law;

(2) **Accuracy**: Personal data should be accurate and complete to the extent necessary for the purposes for which it is to be used or disclosed;

(3) **Security**: Personal data should be appropriately protected against loss and unauthorised access, collection, use, disclosure, copying, modification, destruction or similar risks;

(4) **Access and Correction**: An individual's personal data should, upon request by the individual and subject to domestic law, provided to them or corrected (if it contains an error or omission).

(5) **Transfers to Another Country or Territory**: Personal data should not be transferred to another country or territory unless the prior consent of the individual concerned or the disclosing party takes reasonable steps to ensure that the recipient protects the personal data consistently with the PDP Principles.

(6) **Retention**: Documents containing personal data should not be retained (the means by which personal data in them can be associated with particular individuals should be removed) when retention is reasonably no longer necessary for legal or business purposes.

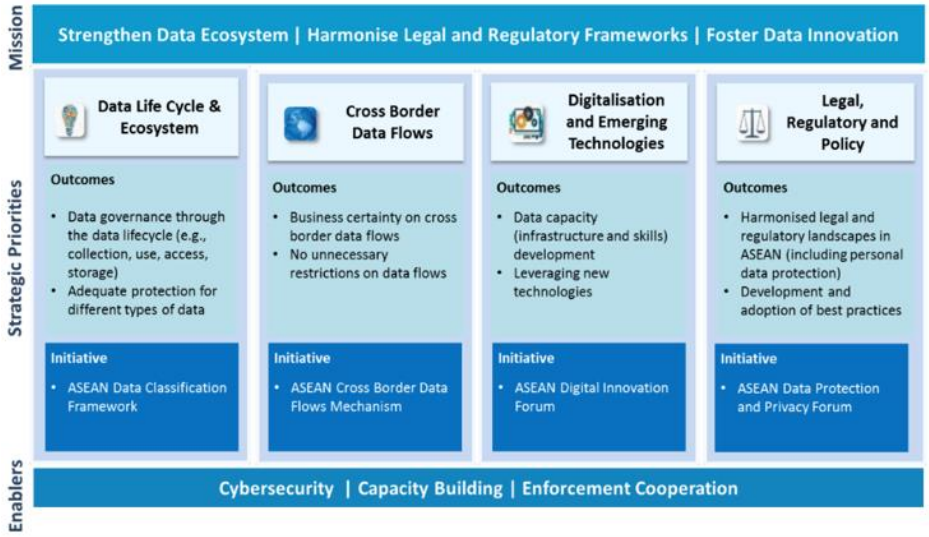
(7) **Accountability**: Organisations should be accountable for complying with measures that give effect to the PDP Principles, including making information available about its data protection policies and practices.

ii. ASEAN Framework on Digital Data Governance

ASEAN expanded its scope of cooperation significantly in 2018 when ASEAN TELMIN entered into the *ASEAN Framework on Digital Data Governance* ("**DDG Framework**").[3] The DDG Framework sets out the region's strategic priorities in 4 key areas, with specific initiatives in each area, in order to guide member states in their regulatory approaches (see Figure 1 below).

Figure 1. Summary of the DDG Framework (Source: ASEAN, DDG Framework)

[3] Available at https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf.



The first strategic priority, **Data Life Cycle and Ecosystem**, focuses on the importance of data governance at every stage of the data life cycle and how that can contribute to the overall integrity and usability of data. This includes measures to track and ensure accuracy of data, ensuring use of data for appropriate purposes and implementing appropriate access controls and security measures. The initiative under this strategic priority was the development of the *ASEAN Data Management Framework* which was issued in 2021 (see below).

The second strategic priority, **Cross Border Data Flows**, recognises the importance of data to the digital economy. This includes measures to maximise the free flow of data within ASEAN while ensuring that transferred data is accorded the necessary protection. The initiative under this strategic priority envisioned the development of an ASEAN Cross Border Data Flows (CBDF) Mechanism. ASEAN DGMIN has since decided to develop two mechanisms under this initiative, the *ASEAN Model Contractual Clauses* (see further below) and the *ASEAN Certification for Cross Border Data Flows*, the latter of which is still under development.

For the third strategic priority, **Digitalisation and Emerging Technologies**, the key focus is on leveraging emerging technologies and human capacity building, in order to equip stakeholders (including organisations and their employees) with resources to evolve with new trends and technologies. The initiative under this strategic priority is the establishment of the ASEAN Digital Innovation Forum.

Finally, the fourth strategic priority, **Legal, Regulatory and Policy**, focuses on the development of a harmonised legal and regulatory environment for data protection within ASEAN, building on the PDP Framework. The initiative under this strategic priority was the

establishment of an annual ASEAN Data Protection and Privacy Forum for ASEAN member states to facilitate knowledge sharing and further discuss the initiatives under the DDG Framework.

iii. ASEAN Data Management Framework

The ASEAN Digital Senior Officials Meeting (ADGSOM) issued the ASEAN Data Management Framework ("**DMF**")[4] in 2021, as an initiative under the DDG Framework. It is aimed at helping businesses operating in ASEAN participate in the digital economy and adopt appropriate data governance measures throughout the data lifecycle, including adequate protection for different types of data. The DMF is voluntary, non-binding and may be adapted to meet varying business needs.

The following are six foundational components of the DMF (which are explained in greater detail in the DMF):

(1) **Governance and oversight**: Implementation of the DMF within an organisation (guidance to employees);

(2) **Policies and procedural documents**: Development of data management policies and procedures based on the DMF throughout the data lifecycle;

(3) **Data inventory**: Identification of data use and storage, to enable understanding of data taxonomy and data purpose;

(4) **Impact/risk assessment**: Impact assessment if confidentiality, integrity or availability of data is compromised;

(5) **Controls**: Design and implementation of controls to protect data; and

(6) **Monitoring and continuous improvement**: Monitoring, measurement, analysis and evaluation of implemented DMF components in order to ensure they are optimised and kept up-to-date.

iv. ASEAN Model Contractual Clauses

ASEAN has also issued a set of *ASEAN Model Contractual Clauses* ("**MCCs**")[5] pursuant to the DDG Framework. The MCCs provide a baseline set of contractual terms that businesses may voluntarily adopt in their legal agreements when transferring personal data among jurisdictions within ASEAN. The MCCs seek to ensure that data is protected based on the principles in the PDP Framework or as required by the law of an ASEAN member state. Businesses are free to adapt the

[4] Available at https://asean.org/wp-content/uploads/2-ASEAN-Data-Management-Framework_Final.pdf.
[5] Available at https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.

clauses, or adopt other clauses, that are appropriate for their commercial or business arrangements or rely on other transfer mechanisms that are permitted under the applicable law of an ASEAN member state.

The MCCs have been recognised by several data protection regulators, such as Singapore's Personal Data Protection Commission, the Philippines' National Privacy Commission and Indonesia's Kominfo, in their guidance materials or public statements. Further, Thailand's recently enacted transfer regulations expressly recognise the use of the MCCs as a lawful mechanism for cross-border data transfers.

The MCCs include two "modules", which address data controller to data processor and data controller to data controller data transfers. The former may be used in situations where the data exporter transfers data to a data importer who may be a contractor or vendor (referred to as a data processor or data intermediary) that processes the data on behalf of, and for the purposes of, the data exporter. The latter module may be used in situations where the data exporter transfers data to a data importer who may process the data for its own purposes.

Each module includes clauses covering the following topics (which, as noted above, may be amended by the parties as appropriate):

- Definitions;
- Obligations of the data exporter;
- Obligations of the data importer;
- Obligations of both parties (for controller-to-controller transfers);
- Additional terms for individual remedies; and
- Boilerplate clauses (referred to as "commercial components") dealing with matters such as choice of law, disputes, suspension of transfers, termination of contract, undertakings and variation of contract.

v. Joint Guide to ASEAN MCCs and EU Standard Contractual Clauses

ASEAN's MCCs are also a useful resource for cross-border data transfers between an ASEAN jurisdiction and other, non-ASEAN jurisdictions. At present, several other jurisdictions have developed their own set of model or standard contractual clauses ("**SCCs**") which may be used, if not required, for data transfers from those jurisdictions. These include, for example, the European Union ("**EU**"), China, Hong Kong and New Zealand. The growing number of SCCs presents a challenge to organisations operating globally who may need to transfer data between two or more jurisdictions (that is, with data flows between the jurisdictions and not just from one jurisdiction to another).

To aid organisations transferring data between a jurisdiction in ASEAN and a jurisdiction in the EU, ASEAN and the EU have issued a *Joint Guide to ASEAN Model Contractual Clauses and EU Standard*

Contractual Clauses ("**Joint Guide**").[6] The first part of the Joint Guide, referred to as the Reference Guide, provides information about the ASEAN MCCs and EU SCCs, including information about similarities and differences between them. The second part, referred as at the Implementation Guide, provides additional information on adopting the ASEAN MCCs and EU SCCs.

Notably, both the ASEAN MCCs and EU SCCs may be incorporated into a boarder commercial contract between the relevant parties. However, while the ASEAN MCCs may be adapted and modified as required (subject to the requirements of the applicable data protection laws), the EU SCCs may not be changed. Both the ASEAN MCCs and EU SCCs include definitions of important terms such as "personal data" and "processing" as well as obligations for the transferor and recipient of the data, for example, in the following areas:

- Lawfulness of transfer;
- Purpose limitation and specifying the purpose;
- Accuracy;
- Data minimisation;
- Storage (retention) limitation;
- Security and confidentiality;
- Onward transfers;
- Data subject rights (including third-party beneficiary rights and redress); and
- Responsibility/accountability for transferred data.

The Joint Guide also provides information on general contractual requirements applicable to the ASEAN MCCs and EU SCCs such as dispute resolution, termination and survival clauses (amongst others).

vi. ASEAN Cybersecurity Cooperation Strategy

On the cybersecurity front, the growing volume and sophistication of cyber threats has triggered regional efforts to articulate a roadmap for achieving a safe and secure cyberspace. The ASEAN member states endorsed an *ASEAN Cybersecurity Cooperation Strategy (2017-2020)*[7], subtitled "Broadening and deepening cybersecurity cooperation for a secure and resilient ASEAN cyberspace", in 2017. This provided for the establishment of an ASEAN Regional Computer Emergency Response Team ("**CERT**") to give national CERTs a formal mechanism to tighten coordination and bolster the overall effectiveness of regional incident response capabilities.

[6] Available at https://asean.org/wp-content/uploads/2024/02/Joint-Guide-to-ASEAN-Model-Contractual-Clauses-and-EU-Standard-Contractual-Clauses.pdf.
[7] Available at https://asean.org/wp-content/uploads/2021/08/ASEAN-Cybersecurity-Cooperation-Strategy.pdf.

More recently, ASEAN member states have endorsed the *ASEAN Cybersecurity Cooperation Strategy (2021 - 2025)*.[8] This builds on the foundation laid by the earlier strategy and sets out various specific initiatives in the following areas:

(1) Advancing Cyber Readiness Cooperation;

(2) Strengthening Regional Cyber Policy Coordination;

(3) Enhancing Trust in Cyberspace;

(4) Regional Capacity Building; and

(5) International Cooperation.

[8] Available at https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

CONTACTS

LIM Chong Kin

Managing Director, Corporate & Finance Co-head, Data Protection, Privacy & Cybersecurity Co-head, Drew Data Protection & Cybersecurity Academy, Drew & Napier LLC

E:Chongkin.Lim@drewnapier.com

David N. ALFRED

Director and Co-head, Data Protection, Privacy & Cybersecurity Co-head and Programme Director, Drew Data Protection & Cybersecurity Academy, Drew & Napier LLC

E:David.Alfred@drewnapier.com

Anastasia CHEN

Director, Corporate & Finance and Data Protection, Privacy & Cybersecurity, Drew & Napier LLC

E:Anastasia.Chen@drewnapier.com

BRUNEI DARUSSALAM

2. BRUNEI DARUSSALAM

A) OVERVIEW

Legal Framework

1. What are the main laws governing data protection and cybersecurity in Brunei Darussalam?

At present, there is no general data protection law in Brunei. Brunei's info-communications regulatory authority, the Authority for Info-communications Technology Industry ("**AITI**"), issued a public consultation paper in May 2021 on a proposed framework for personal data protection for the private sector in Brunei ("**Consultation Paper**"). AITI subsequently issued a response to the feedback received during the public consultation in December 2021 ("**Response**"). Since then, AITI has conducted a number of industry engagement sessions and a new law, the Personal Data Protection Order ("**PDPO**") is expected to be enacted later this year. This chapter highlights some of the expected requirements of the PDPO, based on AITI's proposed positions in the Consultation Paper and Response. This remains to be confirmed when the final PDPC is enacted.

Apart from a general data protection law, there may be sector-specific frameworks that contain requirements aimed at protecting personal data (although not necessarily defined as such and typically with a narrower scope of obligations as compared with a general data protection law). For example, for the telecommunications sector, end-user subscriber information ("**EUSI**") is protected under the Code of Practice for Competition in the Telecommunications Sector ("**Competition Code**") issued by AITI under the Telecommunications Order, 2001. EUSI is defined as including information regarding an end user's billing name, identification number, address, telephone number, IP address, location information and usage patterns, amongst other information (Competition Code, paragraph 1.3(n)). The Competition Code prohibits undertakings or enterprises that engage in commercial activities relating to telecom systems and services in Brunei (referred to as "**Market Players**") from using or disclosing EUSI except for the purposes stated in the Competition Code or otherwise with the consent of the end-user concerned (Competition Code, paragraph 3.2.8.12).

Cybersecurity is regulated in Brunei under the Cybersecurity Act (Chapter 272) ("**Cybersecurity Act**"). Various criminal activities are prohibited under the Computer Misuse Act (Chapter 194). Similar to other data protection laws, the PDPO is expected to include obligations related to the security of personal data. Sectoral frameworks may also include requirements relating to the protection of personal data. For example, Market Players are required to take reasonable measures to prevent unauthorised use of EUSI (Competition Code, paragraph 3.2.8.11).

Data Protection Law – Scope of Application

2. What is the intended objective or main scope of the PDPO?

AITI has explained in its Response that the rationale for introducing the PDPO is:

(a) To provide for the protection of individuals' personal data by private sector organisations which seek to collect, use, disclose or otherwise process personal data for their purposes; and

(b) To facilitate cross-border flows of personal data and further the development of the digital economy in Brunei.

Accordingly, the PDPO is intended to set out the obligations of private sector organisations with respect to their collection, use, disclosure and other processing of individuals' personal data and the rights of individuals in relation to the processing of their personal data.

3. What is the scope of personal data protected under the PDPO?

It is proposed in the Consultation Paper that the term "personal data" be defined under the PDPO as data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access. Related to this, an "individual" is proposed to refer to a natural person, whether living or deceased.

Based on the proposed definition of personal data, the PDPO would apply to all forms of personal data, including personal data in electronic or non-electronic form. While the PDPO does not include a defined category of sensitive personal data, such data would fall within the definition of personal data. Organisations which are required to comply with the PDPO would need to take into account the sensitivity of personal data, for example, when notifying individuals of the collection of their personal data or when determining the appropriate security arrangements to be put in place to protect the data.

It is further proposed in the Consultation Paper that business contact information fall outside of the scope of the PDPO. Such information is proposed to refer to an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his or her personal purposes.

4. Who must comply with the PDPO?

It is proposed in the Consultation Paper that the PDPO apply to organisations, which refers to any individual, company, association or body of persons, whether or not they are formed or recognised under the laws of Brunei or resident or have an office or place of business in Brunei.

However, it is also proposed that the PDPO does not apply to individuals acting in a personal or domestic capacity or as an employee or an officer of an organisation (that is, a director, secretary or similar officer).

As noted above, the PDPO is intended to apply to private sector organisations. As such, it is proposed that it does not apply to public agencies, which refers to the Government of Brunei (including any ministry, department, agency or organ of state), any tribunal appointed under any written law and any prescribed statutory body. The Consultation Paper notes that public agencies in Brunei are subject to the Government of Brunei's data protection rules.

Cybersecurity Law – Scope of Application

5. What is the intended objective or main scope of the Cybersecurity Act?

The Cybersecurity Act enables the Commissioner of Cybersecurity (the "**Commissioner**") to require or take measures to prevent, manage and respond to cybersecurity threats and incidents, as well as regulates owners of computer systems designated as critical information infrastructure ("**CII**").

6. Who must comply with the Cybersecurity Act?

Owners of computers or computer systems designated as CII by the Commissioner must comply with obligations under the Cybersecurity Act.

Pursuant to section 9 of the Cybersecurity Act, the Commissioner may designate a computer or computer system as CII if he is satisfied that: (a) the computer or computer system is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Brunei Darussalam; and (b) the computer or computer system is located wholly or partly in Brunei Darussalam.

The Schedule to the Cybersecurity Act prescribes the list of essential services. These services relate to the following industries: energy; info-communications; healthcare; banking and finance; defence and security; emergency services; aviation; the functioning of Government; media; and water.

Data Protection Authority, Enforcement and Appeals

7. Which are the key authorities that administer and enforce the PDPA? What powers do the key authorities have under the PDPA?

Brunei's Minister of Transport and Infocommunications has designated AITI as the Interim Data Office to develop the PDPO. In the Response, it was clarified that AITI will be the authority responsible for administering

and enforcing the PDPO (referred to in the Consultation Paper as the "**Responsible Authority**").

The Consultation Paper states that the Responsible Authority will have the power, upon receiving a complaint or of its own motion, to conduct an investigation into whether an organisation is complying with the PDPO. This includes the power to require, by written notice, an organisation to produce specified documents or information, to examine orally any person who appears to be acquainted with the facts and circumstances of a matter and to enter any premises with advance notice or by obtaining a search warrant.

The Responsible Authority may give directions to an organisation that has not complied with the PDPO. These may include the following directions:

- To stop collecting, using or disclosing personal data in contravention of the PDPO;
- To destroy personal data collected in contravention of the PDPO;
- To provide access to or correct personal data; and
- If the organisation intentionally or negligently contravened the PDPO, to require payment of a financial penalty of up to B$1 million or 10% of the annual turnover of the organisation in Brunei (whichever is higher).

8. Is there an avenue for appeal against an enforcement decision made under the PDPO?

The Consultation Paper states that where an individual or an organisation is aggrieved by a decision or direction of the Responsible Authority in the exercise of its powers under the PDPO, they may make a written application to the Responsible Authority to reconsider the decision or direction. Alternatively, an individual or an organisation may appeal to the Data Protection Appeal Panel ("**DPAP**") against the decision or direction of the Responsible Authority.

Where an appeal is lodged with the DPAAP, the Chairman of the DPAP shall nominate a Data Protection Appeal Committee ("**DPAC**") from among the members of the DPAP and the DPAC hearing an appeal may confirm, vary or set aside the decision or direction which is the subject of the appeal.

Cybersecurity Authority, Enforcement and Appeals

9. Which are the key authorities that administer and enforce the Cybersecurity Act? What powers do the key authorities have under the PDPA?

The authority responsible for the administration and enforcement of the Cybersecurity Act is Cyber Security Brunei, which is led by the Commissioner.

The Commissioner has a broad range of powers under the Cybersecurity Act. This includes:

- The power to issue directions to the owners of CII to take actions in relation to a cybersecurity threat, comply with any code of practice or standard of performance, appoint an auditor to audit their compliance with any code of practice or standard of performance, participate in cybersecurity exercises, or for any other matters necessary to ensure the cybersecurity of the CII; and
- The power to investigate and prevent cybersecurity incidents, including issuing requests for information and documents, and directions for remedial measures to be taken.

Depending on the non-compliance, penalties may include fines and/or terms of imprisonment.

10. Is there an avenue for appeal against a decision made under the Cybersecurity Act?

Persons who are aggrieved by a decision made under the Cybersecurity Act may make an appeal to the Minister of Transport and Infocommunications against a decision or direction of the Commissioner.

B) DATA PRIVACY AND DATA GOVERNANCE OBLIGATIONS

Obligations Relating to Collection, Use, Disclosure and/or Processing of Personal Data (Data Privacy)

11. What are the legal bases for processing personal data under the PDPO?

The Consultation Paper states that an individual's consent will be required under the PDPO before an organisation collects, uses or discloses the individual's personal data, unless collection, use or disclosure without consent is required or authorised by law or an exception under the PDPO applies.

Consent and Deemed Consent

The Consultation Paper notes that consent may be explicit or implied from the circumstances, for example, through an individual's actions or inaction.

In addition, the PDPO will provide for deemed consent, which may arise in the following circumstances:

(a) Where an individual voluntarily provides their personal data for a purpose, and it is reasonable that they would do so;
(b) If the collection, use or disclosure of an individual's personal data is reasonably necessary for the conclusion of a contract between the organisation and the individual; or
(c) Where the organisation conducts a prescribed assessment for adverse effect on the individual, notifies the individual of the purpose for collection, use or disclosure of their personal data and provides a reasonable period of time for them to opt out.

Exceptions to Consent under the PDPO

Although the Consultation Paper specifically mentions exceptions to the requirement to obtain consent, these exceptions are not described in the Consultation Paper or Response. Taking into account the overall approach taken by AITI in developing the PDPO, it is likely that such exceptions will be similar to those found in other jurisdictions data protection laws, including the following:

(a) exceptions relating to the vital interests of data subjects;
(b) exceptions relating to the public interest;
(c) exceptions relating to legitimate interests or organisations;
(d) exceptions relating to business asset transactions; and
(e) exceptions relating to research and business improvement purposes.

12. Does the PDPO impose other requirements for the collection and processing of personal data?

Purpose Limitation
The Consultation Paper states that organisations may only collect, use or disclose personal data under the PDPO for purposes that a reasonable person would consider appropriate in the circumstances.

Notification
In addition, as noted above, the PDPO will require organisations to inform individuals of the purpose for the collection, use or disclosure of personal data on or before collecting the personal data although there is no prescribed manner or form in which notice must be given.

13. Does the law impose separate or additional requirements in relation to specific categories of personal data (e.g. sensitive personal data)?

As noted above, PDPO will not include a defined category of sensitive personal data. However, such data would fall within the definition of personal data under the PDPO and organisations would need to take into account the sensitivity of personal data, for example, when notifying individuals of the collection of their personal data or when determining the appropriate security arrangements to be put in place to protect the data.

Obligations Relating to Care of Personal Data (Data Governance)

14. What obligations does the PDPO impose in relation to the care of personal data?

The Consultation Paper states that organisations will have the following obligations under the PDPO.

Accuracy
Organisations will be required to make a reasonable effort to ensure that personal data it has collected is accurate and complete, if it is likely to be used by the organisation to make a decision that affects the individual or it is likely to be disclosed by the organisation to another organisation.

Retention Limitation
Organisations will be required to cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data, and retention is no longer necessary for legal or business purposes.

Data Subject Rights

15. What rights do data subjects have under the PDPO?

The Consultation Paper states that individuals (data subjects) will have the rights described below under the PDPO.

Right of Access
Individuals will have the right to request an organisation to provide them with their personal data that is in the possession or under the control of the organisation, and information about the ways in which their personal data has been (or may have been) used or disclosed in the one year period preceding their request. This right will be subject to exceptions under the PDPO including, for example, if the information could reveal personal data about another individual.

Right of Correction
Individuals will have the right to request an organisation to correct or error or omission in their personal data that is in the possession or under the control of the organisation. This right will be subject to exceptions under the PDPO including, for example, in relation to opinion data kept solely for evaluative purposes.

Right to Data Portability
Individuals may have the right to request an organisation to transmit their personal data that is in the possession or under the control of the organisation to another organisation. This right will be subject to exceptions under the PDPO including, for example, data that is specifically excluded under the PDPO.

Right to Withdraw Consent

Individuals will have the right, at any time upon giving reasonable notice, to withdraw any consent given, or deemed to have been given, in relation to the collection, use or disclosure of their personal data. Organisations cannot prohibit individuals from withdrawing consent although this does not affect the consequences of such withdrawal.

Right of Private Action
An individual who suffers loss or damage directly as a result of a contravention by an organisation of certain provisions of the PDPO may commence a private civil action in court. However, where the Responsible Authority has made a decision in respect of the organisation's contravention of the PDPO, the right of private action is only exercisable after all avenues of appeal have been exhausted.

Remedy of Erasure
While the Consultation Paper does not mention that individuals will have a right to erasure of their personal data that is in the possession or under the control of an organisation, as noted above, the Responsible Authority will have the power to direct an organisation to destroy personal data that has been collected in contravention of the PDPO.

C) SECURITY OBLIGATIONS AND DATA BREACH NOTIFICATION

Protection of Personal Data

16. What security obligations are imposed under the PDPO in relation to the processing of personal data?

The Consultation Paper states that organisations will be required under the PDPO to protect personal data in their possession or under their control by making reasonable security arrangements to prevent:

(a) unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data, or similar risks; and
(b) loss of any storage medium or device on which personal data is stored.

Obligations under the Cybersecurity Act

17. What are the security obligations under the Cybersecurity Act?

Under the Cybersecurity Act, CII owners must establish mechanisms and processes for the purposes of detecting cybersecurity threats and incidents in respect of the CII, as set out in any applicable code of practice.

The Cybersecurity Code of Practice for Critical Information Infrastructure ("**Cybersecurity Code of Practice**") requires CII owners to implement security configuration baseline standards for all operating systems, applications, network devices and other CII assets that is commensurate with the cybersecurity risk profile of that CII. The security configuration baselines must address the following security practices at the very least:

- removal of inactive or unused accounts;
- password management (default passwords must be changed, and passwords shall be stored in their hash forms);
- removal of unnecessary services and applications;
- closure of unused or unnecessary network ports and services;
- enabling only external physical connections necessary for the operation of the CII;
- protection against malware; and
- timely update of software and security patches.

Notification of Security Incidents and Data Breaches

18. Are there notification requirements to notify regulatory authorities and affected data subjects of a data breach? What are the timelines for such notification?

The Consultation Paper states that organisations will be required under the PDPO to notify the Responsible Authority as soon as is practicable, but in any case, no later than 3 calendar days after making the assessment that a data breach:

(a) Will result, or is likely to result, in significant harm to the affected individuals; or
(b) Is, or is likely to be, of significant scale.

The terms "significant harm" and "significant scale" are not defined in the Consultation Paper. In the Response, it was noted that the Responsible Authority will take into account international norms and issue guidelines on the interpretation of these terms.

Organisations must also notify the affected individuals on or after notifying the Responsible Authority if the data breach will result, or is likely to result, in significant harm to the affected individuals. This obligation is subject to waiver and exceptions (which are not stated in the Consultation Paper).

19. Are there notification requirements in relation to other cybersecurity events? What are the timelines for such notification?

The Cybersecurity Act requires owners of CII to notify the Commissioner of the occurrence of any of the following:

(a) prescribed cybersecurity incident in respect of the CII;
(b) prescribed cybersecurity incident in respect of any computer or computer system under the control of the owner that is interconnected with or that communicates with the CII;
(c) any other type of cybersecurity incident in respect of the CII that the Commissioner has specified by written direction to the owner.

At the time of writing, the types of cybersecurity incidents and timeframes under this notification obligation have yet to be prescribed.

D) OUTSOURCING AND CROSS-BORDER TRANSFERS

International Data Transfers

20. Does the PDPO impose requirements in relation to the transfer of data to other jurisdictions? What are the ways in which these requirements may be met?

The Consultation Paper states that organisations must not transfer personal data to a country or territory outside Brunei Darussalam except in accordance with requirements prescribed under the PDPO to ensure that the transferred personal data will be accorded a standard of protection that is comparable to the protection under the PDPO.

In the Response, AITI states that it intends to provide guidance on specific cross-border transfer mechanisms that are permitted under the PDPO at a later date.

Appointment of Data Processors and Third-Party Vendors

21. What are the requirements and relevant obligations in relation to appointing a data processor to process personal data on behalf of the data controller?

The Consultation Paper states that the PDPO will contain a partial exception for organisations, referred to as data processors or data intermediaries, that process personal data on behalf of another organisation or a public agency. Data processors or data intermediaries that process personal data pursuant to a contract that is evidenced or made in writing will only be required to comply with requirements relating to the following obligations (which are summarised above):

(a) Protection (security) of personal data;
(b) Retention of personal data;
(c) Data breach notification obligation; and
(d) Transfer of personal data outside Brunei.

Organisations that engage a data processor or data intermediary will be subject to the obligations under the PDPO in respect of the personal data that is processed on their behalf by the data processor or data intermediary.

22. What obligations does the Cybersecurity Act impose on parties in relation to outsourcing arrangements?

Under the Cybersecurity Code of Practice, the CII owner remains responsible and accountable for the cybersecurity of the CII even if it engages an external party to perform or assist in performing any functions, activities or operations in respect of the CII. The CII owner shall establish processes to maintain oversight over all outsourced functions,

activities or operations, in order to minimise cybersecurity exposure arising from such outsourcing.

The Cybersecurity Code of Practices requires CII owners to include terms in their agreements with the external party to help ensure the cybersecurity of the CII and to reduce or mitigate the impact of any cybersecurity risks associated with the outsourcing. This shall include terms stipulating:

- The type(s) of access that the external party has to the CII, considering the CII owner's business requirements and the cybersecurity risk profile of the CII;
- The obligations of the external party to protect the CII against cybersecurity threats and report cybersecurity incidents; and
- The rights of the CII owner to commission an audit of the external party's cybersecurity posture in relation to the outsourced functions, activities or operations; or to require that the external party provide a copy of the audit report should the external party commission its own audit for these purposes.

Furthermore, the CII owner must establish processes for validating the external party's compliance with the terms in the agreement mentioned above and any other terms in the agreement relating to cybersecurity.

The CII owner must also ensure that it is able to renegotiate the terms of its agreements with external parties in the event of new legal or regulatory requirements.

E) ACCOUNTABILITY AND OTHER COMPLIANCE OBLIGATIONS

Data Protection Law – Appointment of Data Protection Officer and Accountability Requirements

23. Is there a requirement to appoint a data protection officer ("DPO")? If so, what is the scope of responsibilities of a DPO and are there any requirements in relation to the DPO's qualifications or experience?

The Consultation Paper states that organisations will be required under the PDPO to appoint a person to be responsible for ensuring that the organisation complies with the PDPA, who is referred to as the DPO.

The Consultation Paper does not state any specific responsibilities of DPOs or requirements relating to the qualifications or experience of DPOs.

24. Are there other obligations under the PDPO in relation to its data handling processes or compliance with the PDPO?

The Consultation Paper states that organisations will be required under the PDPO to:

(a) Develop and implement policies and practices that are necessary for it to meet its obligations under the PDPO, including a process to receive complaints;
(b) Communicate to its staff information about such policies and practices; and
(c) Make information available to individuals upon request about such policies and practices.

Cybersecurity Law – Accountability and Compliance Requirements

25. Does the Cybersecurity Act impose obligations in respect of demonstrating that compliance with the law is met?

Under section 17(1) of the Cybersecurity Act, CII owners are required to carry out an audit of the compliance of the CII with the Cybersecurity Act and the applicable codes of practice and standards of performance at least once every two years. The audit is to be carried out by an auditor approved or appointed by the Commissioner.

Additionally, section 17(1) of the Cybersecurity Act requires CII owners to conduct a cybersecurity risk assessment of the CII in the prescribed form and manner at least once a year.

26. What other key compliance obligations does the Cybersecurity Act impose?

The Commissioner may conduct cybersecurity exercises for the purpose of testing the state of readiness of CII owners in responding to significant cybersecurity incidents. CII owners must participate in a cybersecurity exercise if directed in writing to do so by the Commissioner (section 18 of the Cybersecurity Act).

Additionally, if there is a change in the beneficial or legal ownership of a CII, the relevant person must inform the Commissioner of the change in ownership not later than 7 days after the date of that change in ownership (section 15 of the Cybersecurity Act).

Additionally, CII owners may also be required to furnish, to the Commissioner, information such as information related to the design, configuration and security of the CII or that of any other computer or computer system under the control of the owner that is interconnected or communicates with the CII, among other things (section 12 of the Cybersecurity Act).

CONTACTS

LIM Chong Kin

Managing Director,
Corporate & Finance
Co-head, Data
Protection, Privacy &
Cybersecurity
Co-head, Drew Data
Protection &
Cybersecurity
Academy,
Drew & Napier LLC

E:Chongkin.Lim@drewnapier.com

David N. ALFRED

Director and Co-head,
Data Protection, Privacy
& Cybersecurity
Co-head and
Programme Director,
Drew Data Protection &
Cybersecurity Academy,
Drew & Napier LLC

E:David.Alfred@drewnapier.com

CAMBODIA

3. CAMBODIA

A) OVERVIEW

Legal Framework

1. What are the main laws governing data protection and cybersecurity in Cambodia?

Cambodia has not yet enacted any comprehensive cybersecurity and data protection legislation although the Ministry of Post and Telecommunication ("**MPTC**") announced in 2021 that it would be drafting the Personal Data Protection Law after finalising the draft Cybersecurity Law. As of mid-June 2024, the two drafts are still being discussed and developed.

Under current practices, matters pertaining to data protection and privacy fall broadly under the right to privacy as addressed in Cambodia's constitution, and certain provisions under the Civil Code, the Criminal Code, and other specific laws such as the Law on Electronic Commerce (E-commerce Law) and the Law on Banking and Financial Institutions. Those laws generally protect the right to privacy, which could possibly cover personal data.

Data Protection Law – Scope of Application

2. What is the intended objective or main scope of the data protection law?

The laws that have data protection and data privacy implications such as the Constitution, the Civil Code, and the E-Commerce Law are laws of general applications that would be applicable to any natural person or private/public organisation. The Constitution is considered as a supreme law of the country while the Civil Code is a codification of private law issues such as contracts, family law, property, and obligations. The E-Commerce Law is a specialised law governing the issue of e-commerce in Cambodia and between Cambodia and abroad.

3. What is the scope of personal data protected under the data protection law?

There is no law or regulation defining of the term "personal data" although the term "data" was defined under the E-Commerce Law, which is the law that regulates domestic and cross-border e-commerce activities within and into Cambodia, as "a group of numbers, characters, symbols, messages, images, sounds, videos, information or electronic programs that are prepared in a form suitable for use in a database or an electronic system".

4. **Who must comply with the data protection law?**

   The Constitution, the Civil Code and the E-Commerce Law are laws of general application and do not contain a provision on extra-territorial application of the law.

Cybersecurity Law – Scope of Application

5. **What is the intended objective or main scope of the cybersecurity law?**

   The cybersecurity law in Cambodia is still being drafted.

6. **Who must comply with the cybersecurity law?**

   Not applicable.

Data Protection Authority, Enforcement and Appeals

7. **Which are the key authorities that administer and enforce the data protection law? What powers do the key authorities have under the data protection law?**

   There are no key authorities although the following authorities may have substantial powers over data protection matters in Cambodia since they are the authorities handling the drafting of the Personal Data Protection Law and Cybercrime Law or might relate to the drafted laws to some extent:

   - Ministry of Post and Telecommunication
   - Ministry of Interior
   - Ministry of Commerce.

8. **Is there an avenue for appeal against an enforcement decision made under the data protection law?**

   Not applicable.

Cybersecurity Authority, Enforcement and Appeals

9. **Which are the key authorities that administer and enforce the cybersecurity law? What powers do the key authorities have under the cybersecurity law?**

   There are no key authorities although the following authorities may have substantial powers over cybersecurity matters in Cambodia since they are the authorities handling the drafting of the Cybersecurity Law and Cybercrime Law:

   - Ministry of Post and Telecommunication

- Ministry of Interior.

10. Is there an avenue for appeal against a decision made under the cybersecurity law?

Not applicable.

B) DATA PRIVACY AND DATA GOVERNANCE OBLIGATIONS

Obligations Relating to Collection, Use, Disclosure and/or Processing of Personal Data (Data Privacy)

11. What are the legal bases for processing personal data?

There is a general recognition of the right to privacy and the obligation to protect data from unauthorised access. However, no legislation requires consent, which means no specific consent is required, and to the extent that a person obtains consent, there is no specific form of consent required.

12. Does the data protection law impose other requirements for the collection and processing of personal data?

Not applicable

13. Does the law impose separate or additional requirements in relation to specific categories of personal data (e.g. sensitive personal data)?

Not applicable

Obligations Relating to Care of Personal Data (Data Governance)

14. What obligations does the data protection law impose in relation to the care of personal data?

There are no specific laws regulating the accuracy, data minimisation and retention of personal data in general although sectoral laws provide some basic guidelines for how long information should generally be retained across various sectors. For example, payroll ledgers should be retained for at least three years.

Data Subject Rights

15. What rights do data subjects have under the data protection law?

Although there is no comprehensive data protection law, some data rights could be implied under the E-Commerce Law. For example, a data subject has the right to access, opt out and correct data under the E-Commerce Law.

C) SECURITY OBLIGATIONS AND DATA BREACH NOTIFICATION

Protection of Personal Data

16. What security obligations are imposed in relation to the processing of personal data?

Although the Personal Data Protection Law is still being drafted, the E-Commerce Law addresses (to some extent) security obligations surrounding personal data. Article 32 of the E-Commerce Law requires any person who stores electronic data to establish all necessary measures to ensure that the data is reasonably protected from loss, unauthorised access, use, alteration, leaks, or disclosure (to or by a third party), unless authorised by the data subject or permitted by law. However, the law did not specify what constitutes “necessary measures”.

Obligations under Laws Governing Cybersecurity

17. What are the security obligations under the cybersecurity law?

The cybersecurity law in Cambodia is still being drafted and no existing regulations address security obligations in the context of cybersecurity.

Notification of Security Incidents and Data Breaches

18. Are there notification requirements to notify regulatory authorities and affected data subjects of a data breach? What are the timelines for such notification?

No. There are no laws or regulations that address data breach notifications or procedures.

19. Are there notification requirements in relation to other cybersecurity events? What are the timelines for such notification?

No. There are no laws or regulations that address cybersecurity event notifications or procedures.

D) OUTSOURCING AND CROSS-BORDER TRANSFERS

International Data Transfers

20. Does the data protection law impose requirements in relation to the transfer of data to other jurisdictions? What are the ways in which these requirements may be met?

No. There are no regulations or provisions on restrictions on international transfers of data, except for personal data processed by licensed banks and financial institutions, which are required to follow the Technology Risk Management Guidelines.

Appointment of Data Processors and Third-Party Vendors

21. What are the requirements and relevant obligations in relation to appointing a data processor to process personal data on behalf of the data controller?

There are no laws or regulations explicitly listing the different obligations of data controllers and data processors or the differences thereof, and no laws related to appointing a data processor.

22. What obligations does the cybersecurity law impose on parties in relation to outsourcing arrangements?

There are no laws or regulations imposing obligations on parties in relation to outsourcing arrangements.

E) ACCOUNTABILITY AND OTHER COMPLIANCE OBLIGATIONS

Data Protection Law - Appointment of Data Protection Officer and Accountability Requirements

23. Is there a requirement to appoint a data protection officer ("DPO")? If so, what is the scope of responsibilities of a DPO and are there any requirements in relation to the DPO's qualifications or experience?

No. There is no requirement to appoint a data protection officer ("**DPO**").

24. Are there other obligations under the data protection law in relation to its data handling processes or compliance with the data protection law?

Not applicable.

Cybersecurity Law – Accountability and Compliance Requirements

25. Does the cybersecurity law impose obligations in respect of demonstrating that compliance with the law is met?

The cybersecurity law in Cambodia is still being drafted.

26. What other key compliance obligations does the cybersecurity law impose?

The cybersecurity law in Cambodia is still being drafted.

CONTACTS

Jay COHEN

Partner and Director, Cambodia
Tilleke & Gibbins
E: Jay.c@tilleke.com

Chandayya ING

Associate
Tilleke & Gibbins
E: Chandavya.i@tilleke.com

INDONESIA

4. INDONESIA

A) OVERVIEW

Legal Framework

1. What are the main laws governing data protection and cybersecurity in Indonesia?

Data Protection

The main law governing personal data protection in Indonesia is Law No. 27 of 2022 on Protection of Personal Data ("**PDP Law**"), which was enacted on 17 October 2022. Its implementing regulation is expected to be released within this year.

Once the PDP Law comes into full effect, all provisions issued under other regulations that regulate personal data protection will remain valid as long as they do not conflict with the PDP Law. This includes personal data protection provisions outlined in laws such as Law No. 11 of 2008 on Electronic Information and Transactions (as amended) ("**EIT Law**"), Government Regulation No. 71 of 2019 on the Organisation of Electronic Systems and Transactions ("**GR 71/2019**"), and the Ministry of Communication and Informatics ("**MOCI**") Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems ("**Regulation 20/2016**").

In addition, provisions related to personal data protection can also be found in industry-specific regulations. For instance, banks are regulated under Law No. 10 of 1998 on Banking (as amended) to prevent the unauthorised disclosure of customers' bank account information, including details of customers and their funds. Similarly, in the health sector, under Law No. 17 of 2023 on Health, doctors must protect patients' medical conditions, data and records.

Cybersecurity

While there are no regulations specifically covering cybersecurity, general provisions pertaining to cybersecurity can be found within the EIT Law. This law addresses various provisions related to electronic transactions, documents, systems, and networks. In addition, the regulation of National Code and Cyber Agency (*Badan Sandi dan Siber Nasional*, "**BSSN**") should also be observed. BSSN is a governmental institution under and has a direct responsibility to the President.

Data Protection Law – Scope of Application

2. What is the intended objective or main scope of the PDP Law?

Personal data protection is a citizen's basic right, guaranteed and protected by the Indonesian Constitution. The formulation of the PDP Law

reflects the need to protect individuals' rights in society regarding the processing of personal data, whether electronic and non-electronic, and the use of data processing tools. The law aims to prevent violations of personal data that could be experienced by individuals and/or legal entities.

3. What is the scope of personal data protected under the PDP Law?

All forms of personal data, whether electronic or non-electronic and regardless of the degree of sensitivity, are covered under the PDP Law.

"Personal Data" means the data of an individual that is or can be identified specifically or in combination with other information, either directly or indirectly, through an electronic or nonelectronic system. The PDP Law divides Personal Data into two categories:

Specific Data (i.e. sensitive personal data, the processing of which could have a significant impact on the data subject, such as discrimination or a loss)	**General Data**
a. health data and information b. biometric data c. genetic data d. criminal record e. children's data f. personal financial data g. other data referred to in the relevant laws and regulations	a. complete name b. gender c. nationality d. religion e. marital status f. combined data through which certain persons can be identified, e.g. telephone number and IP address

4. Who must comply with the PDP Law?

The PDP Law applies to any individual, corporation, public institution or international organisation that performs legal acts related to the law:

a. within the territory of Indonesia; and
b. outside the territory of Indonesia, that has a legal impact:

    i. within the territory of Indonesia; or
    ii. on Indonesian data subjects outside the territory of Indonesia.

However, the PDP Law does not apply to data processing by an individual for personal or household activities.

Cybersecurity Law – Scope of Application

5. What is the intended objective or main scope of the EIT Law?

Information technology, media, and communication have brought significant transformations in human behaviour and civilisation, leading to rapid social, economic, and cultural changes. Therefore, the Indonesian government recognises the importance of ensuring security and legal certainty in their utilisation, considering legal, technological, social, cultural, and ethical approaches. Among these, legal approaches play a crucial role in addressing security disruptions in electronic system operations to ensure legal certainty.

6. Who must comply with the EIT Law?

The EIT Law applies to all individuals (e.g. Indonesian citizens and foreign citizens) and legal entities engaging in actions regulated under the EIT Law, whether within or outside Indonesia's jurisdiction, that have legal consequences within or outside Indonesia and may harm Indonesia's interests.

Data Protection Authority, Enforcement and Appeals

7. Which are the key authorities that administer and enforce the PDP Law? What powers do the key authorities have under the PDP Law?

One of the forthcoming developments of the PDP Law is the establishment of the Personal Data Protection Agency ("**PDP Agency**"), formed by and directly accountable to the President. The PDP Agency will have substantial authority to implement and enforce personal data protection measures, including to formulate policies and strategies for personal data protection, supervise the implementation of personal data protection, impose administrative sanctions for non-compliance with the PDP Law, and facilitate alternative dispute resolutions. The PDP Agency is also granted the authority to issue orders, receive complaints or reports, conduct investigations into complaints, reports or supervision findings, summon individuals or public entities, and request information, data or documents regarding alleged violations of personal data protection.

As a reference, the administrative sanctions that can be imposed under the PDP Law by the PDP Agency include:

a. warnings;
b. a temporary suspension of data processing activities;
c. the deletion or destruction of data; or
d. a fine of up to 2% of the annual income or annual revenue for the violation variable.

Furthermore, the criminal sanctions under the PDP Law vary depending on the violations ranging from 4 - 6 years of imprisonment and/or IDR 4 - 6 billion of fines. Apart from this criminal sanction, additional criminal penalties can also be imposed in the form of confiscation of profits/assets obtained from criminal acts and payment for compensation.

If the criminal acts are committed by a corporation, the amount of fine that can be imposed is up to 10 times of the maximum fine outlined under the PDP Law. In addition to this fine, the corporation can be imposed with additional criminal sanction in the form of:

a. confiscation of profits and/or assets obtained from or resulting from criminal activities;
b. suspension of all or part of the company's operations;
c. permanent prohibition from engaging in certain activities;
d. closure of all or part of the company's business premises and/or activities;
e. fulfilment of neglected obligations;
f. payment of compensation;
g. revocation of licenses; and/or
h. dissolution of the company.

Although the PDP Agency has yet to be established, in practice, oversight of the PDP Law's implementation is considered to be within the purview of the MOCI. This is because the MOCI has previously issued a data protection regulation, namely MOCI Regulation No. 20 of 2016 on Protection of Personal Data in Electronic Systems.

8. Is there an avenue for appeal against an enforcement decision made under the PDP Law?

The PDP Law does not specifically outline an appeal process for sanctions imposed by the PDP Agency. However, it stipulates that disputes regarding personal data protection can be resolved through arbitration, litigation, or other alternative dispute resolution mechanisms in accordance with the provisions of the legislation.

For arbitration disputes, parties seeking to challenge an arbitration award may file a request for annulment with the relevant District Court. Subsequently, if the District Court annuls the arbitration award, an appeal may be made to the Supreme Court. For court trials before the Indonesian courts (with the District Court being the initial level), parties may appeal to the High Court, and then further to the Supreme Court. Appeals for disputes handled by alternative institutions follow the provisions applicable within those institutions.

In addition, the PDP also regulates the PDP Agency's authority to facilitate dispute settlements outside of court. However, pending the issuance of the Presidential Regulation on the establishment of PDP Agency and a Government Regulation detailing the implementation of its authorities, this section will need to be updated upon the enactment of these regulations.

Cybersecurity Authority, Enforcement and Appeals

9. **Which are the key authorities that administer and enforce the EIT Law? What powers do the key authorities have under the EIT Law?**

   There are no specific authorities designated to supervise the implementation of the EIT Law. According to its implementing regulation (GR 71/2019), the Indonesian minister responsible for communication and informatics affairs (currently, the MOCI) is empowered to oversee the operation of electronic systems. Furthermore, regulations concerning supervision over electronic systems in specific sectors are established by the relevant ministries or institutions after coordinating with the MOCI.

   Additionally, the EIT Law specifies that criminal investigations under the law follow the provisions of the Criminal Procedure Code, managed by the Indonesian National Police. However, apart from the police, certain civil servants within the government (currently under the MOCI), specialising in information technology and electronic transactions, are granted special investigation authority. These authorities include receiving and following up on reports, conducting inspections, seizures, and ordering the takedown of certain information and electronic systems.

   Regarding sanctions imposed under the EIT Law, they vary depending on the type of violation and can range from IDR 400 million - 12 billion fines to 2 - 12 years of imprisonment.

10. **Is there an avenue for appeal against a decision made under the EIT Law?**

    In addition to the criminal sanctions overseen by the above authorities, individuals can file lawsuits against parties operating electronic systems or utilising information technology that causes harm. Disputes may also be settled through arbitration or other alternative dispute resolution mechanisms.

    The appeal process remains consistent with the explanations provided in our response to Question 8 at paragraph 2 above.

B) DATA PRIVACY AND DATA GOVERNANCE OBLIGATIONS

Obligations Relating to Collection, Use, Disclosure and/or Processing of Personal Data (Data Privacy)

11. **What are the legal bases for processing personal data?**

    Data subject's consent is the main legal basis for processing personal data. When processing personal data, the data controller (i.e. any individual, public institution or international organisation that acts individually or jointly) must inform the data subject of the purpose of the data processing. Below is a detailed explanation of the bases for processing of personal data:

a. Explicit and valid consent of the subject for the purposes stated by the controller. The controller must state:

   i. the legal basis for data processing;
   ii. the purposes of the data processing;
   iii. the type and relevance of the data to be processed;
   iv. the retention period of the document containing the data;
   v. the details of the information collected;
   vi. the data processing period; and
   vii. the subject's rights.

If there are any changes to the above information, the controller must notify the subject prior to making the change.

a. Fulfilment of obligations under an agreement if the subject is a party to it or to fulfil the subject's request when entering into an agreement.
b. Fulfilment of the controller's obligations under the laws and regulations.
c. Protection of the vital interests of the subject, such as data processing for serious medical care purposes related to the subject's life.
d. Performance of tasks for public interest, public services, or by the authorisation of the controller.
e. Fulfilment of other valid interests, considering the objectives, needs and balance between the controller's interests and the subject's rights.

12. Does the PDP Law impose other requirements for the collection and processing of personal data?

Please refer to point (a) under Question 11 above. In addition, the processing of personal data must be conducted with written or recorded consent provided in the Indonesian language. Failure to comply with this requirement will render the consent to be null and void.

13. Does the law impose separate or additional requirements in relation to specific categories of personal data (e.g. sensitive personal data)?

Yes, the PDP Law stipulates that the processing of the data of minors and people with disabilities must be handled specially. This involves obtaining approval from the parents or guardians of minors and people with disabilities, or using certain communication methods for people with disabilities.

Sensitive personal data is not expressly defined under the PDP Law, as it only recognises general and specific personal data for which the consent requirement applies. Elucidation of the PDP Law defines specific data as personal data that, if processed, could have a greater impact on the personal data subject, including acts of discrimination and greater losses to the personal data subject. Given specific data covers the personal data or information listed in Question 3 above (e.g. biometric data and genetic data), these may be recognised as sensitive personal data in other countries.

Obligations Relating to Care of Personal Data (Data Governance)

14. What obligations does the PDP Law impose in relation to the care of personal data?

The care of personal data is generally incorporated within the obligations of a data controller, as follows:

a. Ensuring the accuracy, completion and consistency of data through verification.

b. Updating or correcting any mistakes or inaccuracies in data within 72 hours of receiving a request; informing the data subject of the outcome of the update or correction.

c. Maintaining records of all their data processing activities.

d. Providing data subjects with access to the processed data and processing history during the data retention period; granting access within 72 hours of receiving a request for access.

e. Allowing data subjects to modify their data if:

   i. it affects the security, physical or mental health of the data subject or others;
   ii. it impacts the disclosure of another person's data; or
   iii. it negatively affects national defence and security;

f. Assessing the impact of personal data protection in cases where the data processing poses a high-level potential risk to the data subject. This high-level risk may be a result of:

   i. automatic decision-making with a significant legal impact on the subject;
   ii. specific data processing;
   iii. large-scale data processing;
   iv. data processing for the purpose of the systematic evaluation, scoring or monitoring of the subject;
   v. data processing for the purpose of matching or combining a group of data;
   vi. the use of new technology in data processing; or
   vii. data processing that limits the exercising of the subject's rights.

g. Protecting and ensuring the security of the data it processes, by creating and implementing operational technical measures to protect data from unlawful processing interference and determining the data security level by considering the nature of and risk to the data.

h. Protecting the confidentiality of the data.

i. Supervising any party engaged in data processing under the controller's control.

j. Protecting data from unauthorised processing.

k. Preventing data from being accessed unlawfully by using a security system and/or by processing the personal data using a reliable, secure, and responsible electronic system.

l. Stopping the data processing upon the data subject's withdrawal of consent within 72 hours of receiving the withdrawal request.

m. Delaying and limiting the data processing, completely or partially, within 72 hours of receiving a delay and limit request. This may not apply if:

   i. the law does not allow delaying or limiting the data processing;
   ii. the delay or limiting could harm other people's safety; or
   iii. the subject is bound by a written agreement with the controller that prohibits delaying or limiting.

n. Terminating the data processing when the retention period expires, the purpose of the data processing has been achieved, or a termination request is received from the data subject.

o. Deleting data when it is no longer needed to achieve the purpose of the data processing, the subject withdraws their consent, there is a deletion request from the subject, or if the data was obtained or processed unlawfully.

p. Destroying the data in the event that:

   i. the retention period has expired and the data is described as destroyed according to the archive retention schedule;
   ii. there is a deletion request from the subject;
   iii. it is unrelated to the resolution of a dispute; or
   iv. the data was obtained or processed unlawfully.

q. Notifying the subject of the deletion or destruction of the data.

r. Being responsible for the data processing and demonstrating accountability for complying with its obligations.

Data Subject Rights

15. What rights do data subjects have under the PDP Law?

Data subjects have the right to, among other matters:

a. obtain information related to the clarity of their identity, the legal basis, the purpose and use of their personal data, as well the accountability of any party requesting the data;
b. complete, renew and amend mistakes or inaccuracies in their data according to the purpose of the data processing;
c. access and obtain copies of their data;
d. terminate, erase and destroy their data;

e. withdraw any consent to the processing of their data given to a controller;
f. object to any act or decision-making process that is based entirely on automatic processing, including profiling (e.g. occupation records, economic condition, health, personal preferences, interests, skills, behaviour, location, or electronic movement), which leads to legal implications and significantly impacts the subject in question;
g. postpone or limit the processing of any data on a proportional basis according to the purpose of the data processing;
h. file a civil lawsuit and receive indemnities in relation to any violation of the confidentiality of their data;
i. obtain and/or use their data provided by a controller, in commonly recognised forms and formats or in ways that can be read by electronic systems; and
j. use and submit their data to another controller, provided that the relevant systems are capable of safely communicating with each other in accordance with the data protection principles required by law.

However, the above rights are excluded if they pertain to national defence and security, law enforcement processes, public interest within the context of state administration, supervision of the financial services sector, monetary policy, payment systems, financial system stability carried out in the context of state administration, or statistical interests and scientific research interests.

C) SECURITY OBLIGATIONS AND DATA BREACH NOTIFICATION

Protection of Personal Data

16. What security obligations are imposed in relation to the processing of personal data?

Personal data controllers are required to protect and ensure the security of the personal data they process, by implementing the following measures:

a. Developing and implementing operational technical measures to protect personal data from interference with personal data processing that is contrary to the laws and regulations; and

b. Determining the level of security for personal data by taking into account the nature and risks associated with the personal data that must be protected during processing.

Obligations under EIT Law

17. What are the security obligations under the EIT Law?

Under the EIT Law, there are no specific security obligations apart from the general requirement for electronic system providers to ensure the security of their services. Additionally, they are obligated to inform users about the security measures implemented in their electronic systems.

However, BSSN through its Regulation No. 8 of 2020 concerning Security Systems in the Implementation of Electronic System ("**Regulation 8/2020**") further obliges electronic system providers to conduct self-assessment to categorise its systems as follows:

a. Strategic electronic system, i.e. those having significant impact to public interests, public service, state defence and security. The providers of strategic electronic systems must implement:

   (i) SNI ISO/IEC 27001;
   (ii) other security standards related to cybersecurity established by the National Code Cyber Agency; and
   (iii) other security standards related to cybersecurity established by the relevant ministry or agency.

b. High (risk) electronic system, i.e. those having limited impact to the interest of certain sector and/or region. The providers of high (risk) electronic systems must implement:

   (i) SNI ISO/IEC 27001 and/or other security standards related to cybersecurity established by the National Code Cyber Agency; and
   (ii) other security standards related to cybersecurity established by the relevant ministry or agency.

c. Low (risk) electronic systems, i.e. electronic systems that are not categorised under the strategic or high (risk) electronic systems above. The providers of low (risk) electronic systems must implement:

   (i) SNI ISO/IEC 27001; or
   (ii) and/or other security standards related to cybersecurity established by the National Code Cyber Agency.

Afterward, the self-assessment result must be reported to BSSN for verification and determination.

Notification of Security Incidents and Data Breaches

18. Are there notification requirements to notify regulatory authorities and affected data subjects of a data breach? What are the timelines for such notification?

Yes, under the PDP Law, In the event of a failure to protect personal data, the data controller must deliver written notification no later than 72 hours to the relevant data subject and the PDP Agency (not yet established, but this currently refers to the MOCI). For reference, failure to protect data means a failure to protect the confidentiality, integrity and availability of the data. This includes security breaches, whether intentional or unintentional, leading to the destruction, loss, alteration, disclosure or unauthorised access to the data sent, stored or processed.

The notification must at least contain information regarding:

a. the data breach;
b. when and how the data is breached; and
c. the impact of the failure and efforts to handle or recover from the failure.

Following the notification to the MOCI, it may request further information and clarification as it deems necessary. Additionally, it may also require the data controller to notify the public about such failures. According to the law, this would occur if:

a. the data breach disrupts public services; and/or
b. the data breach has a serious impact on the interests of the public.

19. Are there notification requirements in relation to other cybersecurity events? What are the timelines for such notification?

EIT Law is silent on the requirement for cybersecurity events. Newly issued BSSN Regulation No. 1 of 2024 on Cyber Incident Management, however, requires electronic system organisers to form a Cybersecurity Response Team (and to be registered with the National Cybersecurity Response Team). The regulation is silent on the timeline to report cybersecurity events, but explicitly states that the report must be made within 24 hours for the organisers in the strategic sectors (which may have serious impact on public interest, public service, national defence, security and the economy).

Also note that if this incident involves personal data, the notification requirement referred to in Question 18 will apply.

D) OUTSOURCING AND CROSS-BORDER TRANSFERS

International Data Transfers

20. Does the PDP Law impose requirements in relation to the transfer of data to other jurisdictions? What are the ways in which these requirements may be met?

Under the PDP Law, cross-border transfer obligations for the sending party (i.e. the personal data controller in Indonesia) are set out in the following hierarchical manner:

1. The sending party must ensure the recipient party's country/state has a personal data protection level that is equal to or higher than the provisions in the PDP Law.

2. If the requirement in No. 1. is not met, the sending party must ensure the existence of adequate and binding data protection.

3. If the requirements in Nos. 1. and 2. are not met, the last option is to obtain consent from the data subject before conducting the cross-border transfer.

However, from our interpretation of the above provision, it appears that obtaining consent for cross-border data transfers remains necessary, even if the conditions in items Nos. 1. or 2. above are met. This is because, in principle, the transfer of personal data constitutes a form of personal data processing and the PDP Law predominantly adopts a consent-based model for data processing. Therefore, to be prudent, obtaining the data subject's consent for cross-border data transfers remains necessary.

Furthermore, as both GR 71/2019 and MOCI Regulation 20/2016 remain in effect, the transfer of personal data by Indonesian private or public entities to abroad must be done in coordination with the MOCI or an authorised official/institution, in the form of:

1. A report on the planned personal data transfer, listing the destination country, the recipient's name, the transfer date, and the purpose of the transfer (a form for this is provided by the MOCI);

2. An advocacy request to the government, such as consultation, if necessary; and

3. A report on the implementation of the personal data transfer (a form for this is provided by the MOCI).

Nonetheless, the enforcement and operationalisation of this requirement are not yet clear at present date.

Appointment of Data Processors and Third-Party Vendors

21. What are the requirements and relevant obligations in relation to appointing a data processor to process personal data on behalf of the data controller?

When appointed by a controller, a processor must process the data according to the controller's orders. In this case, the data processing remains the controller's liability. The law allows a processor to engage another third party (i.e. another processor), provided that it has obtained the prior written approval of the controller.

Some of the controller's obligations also extend to processors, including to:

a. ensure the accuracy, completion and consistency of data through verification;
b. record all their data processing activities;
c. protect and ensure the security of the data it processes, by creating and implementing operational technical measures to protect the data from unlawful processing interference, and determining the data security level by considering the nature of and risk to the data;
d. protect the confidentiality of the data;
e. supervise any party engaged in the data processing under the controller's control; and
f. protect the data from unauthorised processing.

22. What obligations does the EIT Law impose on parties in relation to outsourcing arrangements?

While the EIT Law may not explicitly address this issue, our interpretation of the law and common practices suggest that all protections provided under the EIT Law must be upheld when using third-party services (outsourcing). This includes ensuring data security, confidentiality, and compliance with relevant regulations, as well as maintaining accountability for the processing of personal data, even if it is outsourced to a third party.

Additionally, under Regulation 8/2020, if the party being outsourced for information security system management is a foreign expert, a non-disclosure agreement must be entered into by the parties and approval from BSSN is required. If BSSN notices any violation of this provision, an administrative sanction in the form of a written warning will be imposed.

E) ACCOUNTABILITY AND OTHER COMPLIANCE OBLIGATIONS

Data Protection Law - Appointment of Data Protection Officer and Accountability Requirements

23. Is there a requirement to appoint a data protection officer ("DPO")? If so, what is the scope of responsibilities of a DPO and are there any requirements in relation to the DPO's qualifications or experience?

Yes, the PDP Law obliges a data controller and data processor to appoint a data protection officer ("**DPO**") if:

a. the data is processed for the purposes of public services;
b. the data controller's core activity requires the regular and systematic large-scale monitoring of the personal data; and
c. the data controller's core activity is the large-scale processing of specific personal data or personal data related to criminal activities.

However, there are no specific qualifications outlined regarding the requirements for the appointed official. Nevertheless, it is anticipated that the upcoming implementing Government Regulation will elaborate further on this matter.

Under the PDP Law, a DPO must have at least the following tasks:

a. informing and advising the controller or processor about compliance with the prevailing laws and regulations;
b. supervising and ensuring compliance with the PDP Law and the controller or processor's policies;
c. providing suggestions upon assessing the impact of the data processing and overseeing the performance of the controller and processor; and
d. coordinating and acting as a liaison for issues related to data processing.

24. Are there other obligations under the PDP Law in relation to its data handling processes or compliance with the PDP Law?

Yes, please refer to Questions 14 and 21.

Cybersecurity Law – Accountability and Compliance Requirements

25. Does the EIT Law impose obligations in respect of demonstrating that compliance with the law is met?

Under the EIT Law, electronic system providers must, unless specified otherwise by separate legislation, ensure that their electronic systems meet the following minimum requirements:

a. capable of displaying electronic information and/or documents entirely in accordance with the retention period mandated by law. Generally, under Regulation 20/2016, for electronic system providers, the retention period is 5 years;
b. able to protect the availability, integrity, authenticity, confidentiality, and accessibility of electronic information within the operation of the systems;
c. operable in accordance with the procedures or guidelines established for their operation;
d. equipped with procedures or guidelines communicated in a language, information, or symbols understandable to the involved parties; and
e. maintain continuous mechanisms to ensure the novelty, clarity, and accountability of procedures or guidelines.

Although these requirements are set out, there are no specific provisions within the EIT Law mandating the demonstration of compliance with them.

Nonetheless, electronic system providers are required to categorise their electronic systems pursuant to Regulation 8/2020 as per our response in Question 17. While there are no specific obligations to demonstrate compliance with the requirements as set out in Question 17, the regulation states that where the BSSN notices non-compliance with this provision, an administrative sanction in the form of a written warning will be imposed.

26. What other key compliance obligations does the EIT Law impose?

Another significant aspect of the EIT Law is the requirement for electronic system providers to ensure protection for children who use or access electronic systems. In fulfilling this obligation, electronic system providers must:

a. provide information regarding the minimum age limits for minors who can use their products or services;
b. establish mechanisms for verifying child users; and
c. establish mechanisms for reporting misuse of products, services, and features that violate or potentially violate children's rights.

As per our response in Question 25, while these requirements are set out, there are no specific provisions mandating the demonstration of compliance with them.

CONTACTS

Heru MARDIJARTO

Partner
Makarim & Taira S.

E:Heru.mardijarto@makarim.com

Reagan Roy TEGUH

Partner
Makarim & Taira S.

E:Reagan.teguh@makarim.com

Lia ALIZIA

Partner
Makarim & Taira S.

E:Lia.alizia@makarim.com

MALAYSIA

5. MALAYSIA

A) OVERVIEW

Legal Framework

1. What are the main laws governing data protection and cybersecurity in Malaysia?

The main law governing data protection in Malaysia is the Personal Data Protection Act 2010 ("**PDPA**"). The PDPA must be read together with its subsidiary legislation, such as the following:

- **Personal Data Protection Regulations 2013:** the Personal Data Protection Regulations 2013 ("**2013 Regulations**") have been introduced pursuant to section 143 of the PDPA to clarify certain concepts and requirements under the PDPA. The 2013 Regulations serve as a supplement to the PDPA to ensure compliance with the seven principles of data processing;
- **Personal Data Protection (Class of Data Users) Order 2013:** the Personal Data Protection (Class of Data User) Order 2013 ("**the Order**") provides for the classes of data users that have to be registered as a data user;
- **Personal Data Protection (Registration of Data Users) Regulations 2013:** Personal Data Protection (Registration of Data Users) Regulations 2013 provides for the procedure for registration as a data user;
- **Personal Data Protection (Fees) Regulations 2013**: the Personal Data Protection (Fees) Regulations 2013 provides for the maximum fee that may be imposed for access requests;
- **Personal Data Protection Standard 2015:** Personal Data Protection Standard 2015 ("**the 2015 Standards**") sets out the minimum standards to be observed by data users to ensure security of the personal data, the retention period, and on data integrity standards in relation to personal data that apply to both electronically and non-electronically processed personal data. The 2015 Standards are intended to be a minimum requirement for all data users; and
- **Personal Data Protection (Compounding of Offence) Regulations 2016:** the Personal Data Protection (Compounding of Offence) Regulations 2016 outline the offences that may be compounded.

All processing of personal data in the context of commercial transactions are required to adhere to the provisions of the PDPA. Additionally, there are other sector-specific legislation that contain data protection requirements such as the Financial Services Act 2013 which governs information relating to the affairs or accounts of a customer of a financial institution; and the Private Healthcare Facilities and Services (Private Hospitals and Other Private Healthcare Facilities) Regulations 2006 which contains provisions prohibiting the removal of a patient's medical records from a private medical clinic or dental clinic except under a court order. In recognition of the fact that separate sectors/industries may have specific industry practices in relation to the manner in which personal data is

handled and/or may have deployed unique technologies that require specific data protection rules, the PDPA permits the formation and designation by the Personal Data Protection Commissioner ("**the Commissioner**") of data user forums, and the preparation of codes of practice for specific sectors/industries.

In this regard, there have to date been in total 8 industry-specific codes of practice introduced for the following, which are for certain classes of data users that have been registered by the Commissioner under the PDPA:

- Code of Practice for the Banking and Financial Sector 2017;
- Personal Data Protection Code of Practice for the Malaysian Aviation Sector;
- Code of Practice on Personal Data Protection for the Insurance and Takaful Industries in Malaysia 2017;
- the Personal Data Protection Code of Practice for the Communications Class Data Users 2017;
- the Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry;
- the Personal Data Protection Code of Practice for the Utilities Sector (Water);
- the Personal Data Protection Code of Practice for the Utilities Sector (Electricity); and
- the General Code of Practice of Personal Data Protection, which shall apply to the classes of data users that have not prepared a code of practice, and have no data user forum to prepare the relevant code of practice.

Pursuant to the Schedule of the Personal Data Protection (Class of Data Users) Order 2013, data users are classified according to industry sectors including communications, banking and financial institutions, insurance, health, tourism and hospitalities, transportation, education, direct selling, services, real estate, utilities, pawnbroker, moneylender. Cybersecurity in Malaysia on the other hand is broadly regulated by separate pieces of legislation, including the Computer Crimes Act 1997, Communications and Multimedia Act 1998, the Copyright Act 1987, the Penal Code, Strategic Trade Act 2010, Digital Signature Act 1997 and the PDPA mentioned above. Such legislation governs matters not limited to cyber offences and the security of personal data.

The Cyber Security Bill 2024 ("**Proposed Cybersecurity Act**") was passed in the Malaysian Parliament after the third reading on 3 April 2024, and is set to be the first dedicated cybersecurity legislation in Malaysia. Apart from these, sectoral regulators such as the Central Bank of Malaysia and Securities Commission of Malaysia have also issued mandatory policies and guidelines requiring financial institutions and capital market entities to comply with certain prescribed cybersecurity-related measures including the preparation of cyber incident response plans. For purposes of this chapter, such requirements of the Central Bank of Malaysia and Securities Commission of Malaysia have not been considered as they are not of general applicability.

Data Protection Law – Scope of Application

2. What is the intended objective or main scope of the PDPA?

The PDPA was enacted in 2010 to enhance public confidence and trust with ongoing enforcement, to mitigate and minimise data breach incidents, to improve the efficiency and governance of personal data collection and management and to ensure the prudence and integrity of personally identifiable information. The PDPA confers rights on individuals ("**data subjects**") in relation to the collection, use, and/or retention ("**processing"**) of their personal data, and places obligations on those persons/entities processing the same ("**data users**"). Under the PDPA, all data users, defined as persons who either alone or jointly or in common with other persons process any personal data or have control over or authorise the processing of any personal data, are required to comply with the PDPA and its subsidiary legislation when processing personal data.

The act of processing, in relation to personal data, as contemplated by the PDPA includes collecting, recording, holding, or storing of personal data, or carrying out of any operation or set of operations on personal data, including:

a) the organisation, adaptation, or alteration of personal data;
b) the retrieval, consultation, or use of personal data;
c) the disclosure of personal data by transmission, transfer, dissemination, or otherwise making available; or
d) the alignment, combination, correction, erasure, or destruction of personal data.

The PDPA embodies seven Personal Data Protection Principles, namely the *General Principle, Notice and Choice Principle, Disclosure Principle, Security Principle, Retention Principle, Data Integrity Principle, and Access Principle*, each of which are enumerated in sections 6 to 12 of the PDPA. The PDPA also provides for, among others:

a) the registration of certain data users within the classes of data users specified in the Data Protection (Class of Data Users) Order 2013 as mentioned above; and
b) the establishment, and powers and functions of the Commissioner, the Appeal Tribunal; the Personal Data Protection Fund, and the Personal Data Protection Advisory Committee.

3. What is the scope of personal data protected under the PDPA?

Personal data is defined to mean any information in respect of commercial transactions, which:

- is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
- is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010. The PDPA also provides for the processing of "sensitive personal data", which is defined as any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister charged with the responsibility for the protection of personal data may determine by order published in the Gazette, subject to the additional provisions under section 40 of the PDPA.

4. Who must comply with the PDPA?

The PDPA is the primary legislation that regulates the processing of personal data and applies to any person who processes any personal data in respect of commercial transactions, as well as any person who has control over or authorises the processing of any personal data in respect of commercial transactions. In this regard, "commercial transactions" is defined to mean "any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services". The PDPA shall not apply to personal data processed outside Malaysia unless that data is intended to be further processed in Malaysia.

Further, the PDPA applies to a person in respect of personal data if: (a) the person is established in Malaysia and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment, or (b) the person is not established in Malaysia, but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia. Where the processing of personal data is carried out by a data processor on behalf of the data user, the data user has the duty to ensure compliance by the data processor with the relevant provisions under the PDPA. In this regard, "data processor" is defined as any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes.

The PDPA does not, however, apply to the Federal Government and State Governments of Malaysia. Notwithstanding this, government-related data is subject to being classified as either "top secret", "secret", "confidential", or "restricted", the classification of which will render the data an official secret under the Official Secrets Act 1972 ("**OSA**"), and the transfer of which overseas is generally prohibited unless the transferor is duly authorised to do so.

Cybersecurity Law – Scope of Application

5. What is the intended objective or main scope of the Proposed Cybersecurity Act?

The Proposed Cybersecurity Act aims to establish an overarching regulatory framework designed to fortify national cybersecurity by providing for:

(a) the establishment of the National Cyber Security Committee;
(b) the duties and powers of the Chief Executive of the National Cyber Security Agency ("**Chief Executive**");
(c) the functions and duties of the national critical information infrastructure sector leads ("**NCII sector leads**") and national critical information infrastructure entities ("**NCII entities**");
(d) the management of cybersecurity threats and cybersecurity incidents to national critical information infrastructures ("**NCIIs**"); and
(e) the regulation of the cybersecurity service providers through licensing.

and to provide for related matters.

6. Who must comply with the Proposed Cybersecurity Act?

The Proposed Cybersecurity Act is intended to have extra-territorial application and shall apply to any person, irrespective of nationality or citizenship, and shall have effect outside as well as within Malaysia. The Federal Government and State Governments are also subject to the Proposed Cybersecurity Act (although they will not be liable to prosecution for any offence under the Proposed Cybersecurity Act). Entities and persons (including Government Entities and businesses) operating within an NCII sector designated as an NCII entity will be required to adhere to certain obligations under the Proposed Cybersecurity Act.

In this regard, "Government Entity" means any ministry, department, office, agency, authority, commission, committee, board, council or other body, of the Federal Government, or of any of the State Governments, established under any written law or otherwise, and any local authority. A NCII sector lead may, in respect of the NCII sector for which it is appointed, designate in such manner as may be determined by the Chief Executive, any Government Entity or person as a NCII entity if the national critical information infrastructure sector lead is satisfied that the Government Entity or person owns or operates a national critical information infrastructure. An NCII is defined under the Proposed Cybersecurity Act as a computer or computer system which the disruption to or destruction of the computer or computer system would have a detrimental impact on the delivery of any service essential to the security, defence, foreign relations, economy, public health, public safety or public order of Malaysia, or on the ability of the Federal Government or any of the State Governments to carry out its functions effectively.

The NCII sectors identified under the Schedule of the Proposed Cybersecurity Act are the government; banking and finance; transportation; defence and national security; information, communication and digital; healthcare services; water sewerage and waste management; energy; agriculture and plantation; trade, industry and economy; and science, technology and innovation. The Proposed Cybersecurity Act also mandates that cybersecurity providers (i.e. persons who provide cybersecurity services) shall obtain a licenced under, and comply with the licensing conditions and other duties imposed by the Proposed Cybersecurity Act. However, the types of services constituting "cybersecurity services" that are subject to this requirement have yet to be defined and prescribed by the Minister charged with the responsibility for cybersecurity.

Data Protection Authority, Enforcement and Appeals

7. Which are the key authorities that administer and enforce the PDPA? What powers do the key authorities have under the PDPA?

The Department of Personal Data Protection ("**Department**") is an agency under the Ministry of Communications and Digital ("**MCMC**") established on 16 May 2011 after the Parliament passed the bill relating to the PDPA. The Commissioner is the Director of the Department. Pursuant to the PDPA, the Commissioner is responsible for the administration and enforcement of the PDPA.

In enforcing the PDPA, the Commissioner is mandated to register all classes of data users. The Commissioner has the power to carry out inspections of any personal data system used by data users and also accepts and investigates complaints from data subjects against data users. Where the Commissioner receives a complaint in relation to an act, practice or request, among others, that may be a contravention of the provisions of the PDPA, including any codes of practice, the Commissioner has the power to carry out an investigation in relation to the relevant data user to ascertain whether the act, practice or request specified in the complaint contravenes the provisions of the PDPA.

Further, an authorised officer may investigate the commission of any offence under the PDPA. For purposes of the PDPA, the authorised officer shall have all or any of the special powers of a police officer of whatever rank in relation to police investigations in seizable cases as provided for under the Criminal Procedure Code. In the context of enforcement, following the completion of an investigation about an act, practice or request specified in the complaint, if the Commissioner is of the opinion that the relevant data user is contravening a provision of the PDPA, the Commissioner may serve on the relevant data user an enforcement notice to, among others, direct the relevant data user to take such steps as are specified in the enforcement notice to remedy the contravention or, as the case may be, the matters occasioning it within such period as is specified in the enforcement notice.

A person who fails to comply with an enforcement notice commits an offence and shall, on conviction, be liable to a fine not exceeding

RM200,000 or to imprisonment for a term not exceeding two years or to both. In relation to the various offences under the PDPA, the Commissioner may, with the consent in writing of the Public Prosecutor, compound any offence committed by any person under the PDPA and prescribed to be a compoundable offence by making a written offer to the person suspected to have committed the offence to compound the offence upon payment to the Commissioner of an amount of money not exceeding 50% of the amount of maximum fine for that offence within such time as may be specified in his written offer. Despite the powers of the Commissioner, no prosecution for an offence under the PDPA shall be instituted except by or with the written consent of the Public Prosecutor.

8. Is there an avenue for appeal against an enforcement decision made under the PDPA?

Any person who is aggrieved by the decision of the Commissioner under the PDPA may appeal to the Appeal Tribunal (established under section 83) by filing a notice of appeal with payment of prescribed fees, if such decision relates to matters including:

a) the registration of a data user under Division 2 of Part II of the PDPA;
b) the refusal of the Commissioner to register a code of practice under section 23(5) of the PDPA;
c) the failure of the data user to comply with a data access request or data correction request under Division 4 of Part II of the PDPA;
d) the issuance of an enforcement notice under section 108 of the PDPA;
e) the refusal of the Commissioner to vary or revoke an enforcement notice under section 109 of the PDPA; and
f) the refusal of the Commissioner to carry out or continue an investigation initiated by a complaint under Part VIII of the PDPA.

A decision of the Appeal Tribunal shall be final and binding on the parties to the appeal.

<u>Cybersecurity Authority, Enforcement and Appeals</u>

9. Which are the key authorities that administer and enforce the Proposed Cybersecurity Act? What powers do the key authorities have under the Proposed Cybersecurity Act?

Pursuant to section 5 of the Proposed Cybersecurity Act, the authority mainly responsible for the administration of the Proposed Cybersecurity Act is the Chief Executive who will act as the secretary to the Committee. The Chief Executive has a broad range of powers under the Proposed Cybersecurity Act, which includes:

a) the power to gather information by directing persons to provide information and evidence or produce document to him under section 14 of the Proposed Cybersecurity Act;
b) the power to investigate cybersecurity incidents and to issue a directive on the measures necessary to respond to or recover from

the cybersecurity incident and to prevent such cybersecurity incident from occurring in the future under section 35 of the Proposed Cybersecurity Act; and

c) the power to issue licences to cybersecurity service providers.

With regard to enforcement, the Minister charged with the responsibility for cybersecurity may in writing authorise any public officer to exercise the powers of enforcement under the Proposed Cybersecurity Act. Penalties for offences under the Proposed Cybersecurity Act will depend on the non-compliance and may include fines and/or terms of imprisonment. For instance, pursuant to section 14(6) of the Proposed Cybersecurity Act, the failure to comply with directions of the Chief Executive to provide and produce information may result in a fine not exceeding RM200,000 and/or imprisonment for a term up to 3 years. Notwithstanding the foregoing, no prosecution for an offence under the Proposed Cybersecurity Act shall be instituted except by or with the written consent of the Public Prosecutor.

10. Is there an avenue for appeal against a decision made under the Proposed Cybersecurity Act?

Persons aggrieved by the refusal of the Chief Executive to issue him a licence or by the revocation or suspension of his licence may appeal in writing against such decisions to the Minister responsible for cybersecurity within 30 days after being informed in writing of such decisions. After considering the appeal, the Minister may confirm or set aside the decision appealed against.

B) DATA PRIVACY AND DATA GOVERNANCE OBLIGATIONS

Obligations Relating to Collection, Use, Disclosure and/or Processing of Personal Data (Data Privacy)

11. What are the legal bases for processing personal data?

Section 6 of the PDPA imposes an obligation on the data user to obtain consent of a data subject before processing the data subject's personal data, subject to the following exceptions where the processing is necessary:

a) for the performance of a contract to which the data subject is a party;
b) for the taking of steps at the request of the data subject with a view to entering into a contract;
c) for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract;
d) in order to protect the vital interests of the data subject;
e) for the administration of justice; or
f) for the exercise of any functions conferred on any person by or under any law.

Although the term "consent" has not been formally defined, it is generally understood that consent must be freely given by the data subject, be

clear, and easily withdrawn, and organisations must exercise caution when relying on consent as a legal basis. Other specific situations where consent may not be required are set out in various other provisions of the PDPA, some of which are set out below. Specifically for the disclosure of personal data, a disclosure may be made without the consent of the data subject where:

a) the disclosure is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations, or the disclosure was required or authorised by or under any law or by the order of a court;
b) the data user acted in the reasonable belief that he had in law the right to disclose the personal data to the other person;
c) the data user acted in the reasonable belief that he would have had the consent of the data subject if the data subject had known of the disclosing of the personal data and the circumstances of such disclosure; or
d) the disclosure was justified as being in the public interest in circumstances as determined by the Minister responsible for the protection of personal data.

In relation to the processing of sensitive personal data, the explicit consent of the data subject may not be required in the situations described in Question 13 below. Note however that the applicability of some of the exceptions in relation to the processing of sensitive personal data may be subject to further conditions or restrictions as may be prescribed by the Minister responsible for personal data protection. In the context of transferring personal data to places outside of Malaysia, Question 20 below addresses certain circumstances where personal data may be transferred without the consent of the relevant data subject.

Further to the above, other exemptions from the requirement to obtain the data subject's consent include:

a) where personal data is processed for the prevention or detection of crime or for the purpose of investigations;
b) where personal data is processed for the apprehension or prosecution of offenders;
c) where personal data is processed for the assessment or collection of any tax or duty or any other imposition of a similar nature;
d) where personal data is processed for preparing statistics or carrying out research, provided that such personal data is not processed for any other purpose and that the resulting statistics or the results of the research are not made available in a form which identifies the data subject;
e) where personal data is necessary for the purpose of or in connection with any order or judgement of a court;
f) where personal data is processed for the purpose of discharging regulatory functions if the consent requirement would be likely to prejudice the proper discharge of those functions;
g) where personal data is processed only for journalistic, literary or artistic purposes, provided that the processing is undertaken with a view to the publication by any person of the journalistic, literary or artistic material; the data user reasonably believes that, taking into

account the special importance of public interest in freedom of expression, the publication would be in the public interest; and the data user reasonably believes that in all the circumstances, compliance with the consent requirement is incompatible with the journalistic, literary or artistic purposes.

The Minister responsible for personal data protection may also, upon the Commissioner's recommendation, introduce further exemptions from the requirement to obtain the data subject's consent for processing personal data.

12. Does the PDPA impose other requirements for the collection and processing of personal data?

As mentioned in Question 11, generally, the data user must obtain consent of a data subject before processing the data subject's personal data. Further, personal data shall not be processed unless:

a) the personal data is processed for a lawful purpose directly related to an activity of the data user;
b) the processing of the personal data is necessary for or directly related to that purpose; and
c) the personal data is adequate but not excessive in relation to that purpose.

Specifically in relation to the disclosure of personal data, no personal data shall, without the consent of the data subject, be disclosed:

a) for any purpose other than the purpose for which the personal data was to be disclosed at the time of collection of the personal data, or for any purpose other than a purpose directly related to the foregoing purpose; or
b) to any party other than a third party of the class of third parties as specified in the notice given to the data subject pursuant to section 7 of the PDPA (usually known as a "privacy notice" or "privacy policy").

In this regard, section 7 of the PDPA provides that a data user shall by written notice in the national language of Malaysia (i.e. Bahasa Malaysia), and English, inform a data subject about the matters as required by section 7(1), including that personal data of the data subject is being processed by or on behalf of the data user, and, as mentioned above, the class of third parties to whom the data user discloses or may disclose the personal data. The aforementioned written notice shall be given as soon as practicable by the data user:

a) when the data subject is first asked by the data user to provide his personal data;
b) when the data user first collects the personal data of the data subject; or
c) in any other case, before the data user uses the personal data of the data subject for a purpose other than the purpose for which the personal data was collected, or discloses the personal data to a third party.

13. Does the law impose separate or additional requirements in relation to specific categories of personal data (e.g. sensitive personal data)?

Pursuant to section 40 of the PDPA, in the case of sensitive personal data, the data user shall not process sensitive personal data of a data subject except in accordance with the following conditions:

a) the data subject has given his explicit consent to the processing of the personal data;
b) the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data user in connection with employment;
c) the processing is necessary in order to protect the vital interests of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data user cannot reasonably be expected to obtain the consent of the data subject;
d) the processing is necessary in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;
e) the processing is necessary for medical purposes and is undertaken by a healthcare professional, or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional;
f) the processing is necessary for the purpose of, or in connection with, any legal proceedings;
g) the processing is necessary for the purpose of obtaining legal advice;
h) the processing is necessary for the purposes of establishing, exercising or defending legal rights;
i) the processing is necessary for the administration of justice;
j) the processing is necessary for the exercise of any functions conferred on any person by or under any written law;
k) the processing is necessary for any other purposes as the Minister thinks fit; or
l) the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

Obligations Relating to Care of Personal Data (Data Governance)

14. What obligations does the PDPA impose in relation to the care of personal data?

Security Principle

The PDPA imposes an obligation on the data user to take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. The data user shall protect the personal data by having regard:

a) to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction;

b) to the place or location where the personal data is stored;
c) to any security measures incorporated into any equipment in which the personal data is stored;
d) to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and
e) to the measures taken for ensuring the secure transfer of the personal data.

Retention Principle

Further, in relation to the retention or storage of personal data, section 10 of the PDPA provides that the personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose. The data user shall take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.

Data Integrity Principle

The PDPA requires a data user to take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed. In this regard, Regulation 8 of the 2013 Regulations provides that for the purposes of section 11 of the PDPA, the data user shall process the personal data in accordance with the data integrity standard set out from time to time by the Commissioner.

Data Subject Rights

15. What rights do data subjects have under the PDPA?

Right to access personal data

The PDPA provides that the data subject shall be entitled to be informed by a data user whether his personal data is being processed by or on behalf of the data user.

Right to correct personal data

In the event a data subject knows that his personal data being held by the data user is inaccurate, incomplete, misleading or not up-to-date, the data subject may make a data correction request in writing to the data user that the data user makes the necessary correction to the personal data.

Right to withdraw consent

A data subject may by written notice withdraw his consent to the processing of personal data in respect of which he is the data subject.

Right to prevent processing likely to cause damage or distress

A data subject may at any time by written notice require the data user to cease or not begin the processing of or processing for a specified purpose or in a specified manner any personal data in respect of which he is the data subject, if based on reasons to be stated by him the processing of that personal data or the processing of personal data for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another person.

Right to prevent processing for purposes of direct marketing

A data subject may, at any time by written notice to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his personal data for purposes of direct marketing, which is the communication by whatever means of any advertising or marketing material which is directed to particular individuals.

C) SECURITY OBLIGATIONS AND DATA BREACH NOTIFICATION

Protection of Personal Data

16. What security obligations are imposed in relation to the processing of personal data?

As mentioned in Question 14, a data user shall take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction when processing personal data. The PDPR requires a data user to develop and implement a security policy, which complies with the security standard for personal data processed electronically and non-electronically as set out in the 2015 Standards. The data user shall ensure that the security standard in the processing of personal data be complied with by any data processor that carry out the processing of the personal data on behalf of the data user.

Obligations under the Proposed Cybersecurity Act

17. What are the security obligations under the Proposed Cybersecurity Act?

Section 21(1) of the Proposed Cybersecurity Act provides for the duty of an NCII entity to implement measures, standards and processes as specified in the code of practice or any alternative and additional measures, standards and processes for the purpose of ensuring the cybersecurity of its NCII. Implementation of measures, standards and processes under any other written law for the purpose of ensuring the cybersecurity of the NCII which is not in contravention with the code of practice shall be deemed to be compliant with section 21. Notwithstanding the foregoing, section 21(2) provides that NCII entities may implement any alternative measures, standards and processes, provided that the entity can prove that such alternatives provide equal or

higher level of protection to the NCII owned or operated by the NCII entity.

Additionally, pursuant to section 21(3) of the Proposed Cybersecurity Act, an NCII entity may, in addition to the measures, standards and processes mentioned above establish and implement the measures, standards and processes on cybersecurity based on internationally recognised standards or framework. Under section 21(4) of the Proposed Cybersecurity Act, an NCII entity shall also be deemed to have complied with section 21 if the cybersecurity measures, standards and processes implemented are those required by any other written law, to the extent that such measures, standards and processes are not in contravention with the code of practice. Note however that the Proposed Cybersecurity Act is pending royal assent and there have not been any proposed codes of practice introduced as at the date of writing.

Notification of Security Incidents and Data Breaches

18. Are there notification requirements to notify regulatory authorities and affected data subjects of a data breach? What are the timelines for such notification?

To date, there is no such requirement under the PDPA. Notwithstanding the foregoing, the Commissioner has in a Public Consultation Paper No.01/2020 proposed to introduce a mandatory provision in the PDPA for a data user to report a data breach incident, and a guideline on the reporting mechanism for data breach. Further, according to the Minister, a "Notification of Data Breach Guidelines" was set to be developed by the Personal Data Protection Department ("**PDPD**").

It is however unclear whether the aforesaid proposal will come into force.

19. Are there notification requirements in relation to other cybersecurity events? What are the timelines for such notification?

Under section 23 of the Proposed Cybersecurity Act, there is a duty to give notification on cybersecurity incidents. Specifically, if it comes to the knowledge of a NCII entity that a cybersecurity incident has or might have occurred in respect of the NCII owned or operated by the NCII entity, the NCII shall notify the Chief Executive and its NCII sector lead on such information. However, the period and manner for such notification have not yet been prescribed.

The Proposed Cybersecurity Act considers a "cybersecurity incident" as an act or activity carried out on or through a computer or computer system, without lawful authority, that jeopardises or adversely affects the cybersecurity of that computer or computer system or another computer or computer system.

D) OUTSOURCING AND CROSS-BORDER TRANSFERS

International Data Transfers

20. Does the PDPA impose requirements in relation to the transfer of data to other jurisdictions? What are the ways in which these requirements may be met?

Section 129(1) of the PDPA prohibits a data user from transferring any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister responsible for personal data protection, upon the recommendation of the Commissioner, by notification published in the Gazette. In this connection, the Minister may specify in the Whitelist any places outside Malaysia if there is in that place in force any law which is substantially similar to the PDPA, or that serves the same purposes as the PDPA, or that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the PDPA. However, as at the date of writing, no such place outside Malaysia has been specified by the Minister pursuant to section 129(1). For completeness, the Commissioner has in a Public Consultation Paper No.01/2020 proposed to abandon the above whitelist approach. Further, according to the Minister, a "Cross-border Data Transfer Guidelines and Mechanism" was set to be developed by the PDPD. It is however unclear whether the aforesaid proposal will come into force.

Notwithstanding the foregoing, a data user may transfer any personal data to a place outside Malaysia if:

a) the data subject has given his consent to the transfer;
b) the transfer is necessary for the performance of a contract between the data subject and the data user;
c) the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which is entered into at the request of the data subject, or is in the interests of the data subject;
d) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;
e) the data user has reasonable grounds for believing that in all circumstances of the case the transfer is for the avoidance or mitigation of adverse action against the data subject, it is not practicable to obtain the consent in writing of the data subject to that transfer, and if it was practicable to obtain such consent, the data subject would have given his consent;
f) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of the PDPA;
g) the transfer is necessary in order to protect the vital interests of the data subject; or
h) the transfer is necessary as being in the public interest in circumstances as determined by the Minister responsible for personal data protection.

Appointment of Data Processors and Third-Party Vendors

21. What are the requirements and relevant obligations in relation to appointing a data processor to process personal data on behalf of the data controller?

As stated in Question 4 above, the PDPA defines "data processor" as any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user and does not process the personal data for any of his own purposes. Where processing of personal data is carried out by a data processor on behalf of the data user, the data user has the duty to ensure compliance by the data processor with the relevant provisions under the PDPA. In this regard, the data user has the duty to ensure the data processor provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and takes reasonable steps to ensure compliance with those measures.

Further, per paragraph 4 of the 2015 Standards, in the case where personal data is processed electronically, the data user shall bind an appointed third party with a contract for operating and carrying out personal data activities.

22. What obligations does the Proposed Cybersecurity Act impose on parties in relation to outsourcing arrangements?

To date, there is no obligation imposed on parties in relation to outsourcing arrangements under the Proposed Cybersecurity Act similar to those considered above in Question 21 in relation to the PDPA. However, note that in the context of the provision of cybersecurity services (the scope of which is yet to be defined pursuant to section 27(2) of the Proposed Cybersecurity Act), which may potentially be provided as part of an outsourcing arrangement, a licensed cybersecurity service provider shall observe the record-keeping requirements mandated by the Proposed Cybersecurity Act on each occasion it is engaged to provide cybersecurity services, including keeping and maintaining the following records:

a) the name and address of the person engaging the licensed cybersecurity service provider for the cybersecurity service;
b) the name of the person providing the cybersecurity service on behalf of the licensed cybersecurity service provider (if any);
c) the date and time of cybersecurity service that was provided by the licensed cybersecurity service provider or other person on behalf of the licensed cybersecurity service provider;
d) details of the type of cybersecurity service provided; and
e) such other particulars as may be determined by the Chief Executive.

E) ACCOUNTABILITY AND OTHER COMPLIANCE OBLIGATIONS

Data Protection Law - Appointment of Data Protection Officer and Accountability Requirements

23. Is there a requirement to appoint a data protection officer ("**DPO**")? If so, what is the scope of responsibilities of a DPO and are there any requirements in relation to the DPO's qualifications or experience?

To date, there is no such requirement under the PDPA. However, according to the Minister, a Data Protection Officer Guidelines was set to be developed by the PDPD. It is however unclear whether the aforesaid proposal will come into force.

24. Are there other obligations under the PDPA in relation to its data handling processes or compliance with the PDPA?

As stated in Question 16, the PDPR requires data users to develop and implement security policies that comply with the security standard as set out in the 2015 Standards. In this regard, the 2015 Standards establishes the security standards for personal data processed electronically and non-electronically. Pursuant to the security standards, some of the manners in which the data user can protect their personal data, among others, include:

a) registering all employees involved in the processing of personal data;
b) terminating an employee's access rights to personal data after his/her resignation, termination, termination of contract or agreement, or adjustment in accordance with changes in the organisation;
c) controlling and limiting employees' access to personal data systems for the purpose of collecting, processing and storing of personal data;
d) establishing physical security procedures;
e) maintaining a proper record of access to personal data periodically and making such record available for submission when directed by the Commissioner.

The PDPR also requires a data user to keep and maintain a list of disclosures to third parties in relation to personal data of the subject data that has been or is being processed by him. Other provisions of the 2015 Standards may also provide for the requirement to develop policies and processes and maintain records. With regard to the retention and disposal of personal data, the 2015 Standards require:

a) maintaining a proper record of personal data disposal periodically and making such record available for submission when directed by the Commissioner;
b) disposing personal data collection forms used in commercial transactions within the period not exceeding 14 days, except where the forms carry legal values in relation to the commercial transaction;

c) preparing a personal data disposal schedule for inactive data with a 24 month period. The personal data disposal schedule should be maintained properly.

Cybersecurity Law – Accountability and Compliance Requirements

25. Does the Proposed Cybersecurity Act impose obligations in respect of demonstrating that compliance with the law is met?

Under section 22(1)(b) of the Proposed Cybersecurity Act, NCII entities shall carry out an audit by an auditor approved by the Chief Executive to determine compliance with the Proposed Cybersecurity Act within a period that has yet been prescribed. Additionally, section 22(1)(a) of the Proposed Cybersecurity Act also requires NCII entities to conduct a cybersecurity risk assessment in respect of the NCII owned or operated by the NCII entity in Accordance with the code of practice and directive. Pursuant to section 22(2) of the Proposed Cybersecurity Act, such security risk assessment report or audit report shall then be submitted to the Chief Executive within the period of thirty days after the completion of such cybersecurity risk assessment report or audit report.

26. What other key compliance obligations does the Proposed Cybersecurity Act impose?

Under section 24(1) of the Proposed Cybersecurity Act, the Chief Executive may conduct a cybersecurity exercise for the purpose of assessing the readiness of any NCII entity in responding to any cybersecurity threat or cybersecurity incident. Under section 20 of the Proposed Cybersecurity Act, there is also a duty for an NCII entity to provide information relating to its NCII to the NCII sector lead when it procures or has come into possession or control of any additional computer or computer system which in its opinion is an NCII, or when any material change is made to the design, configuration, security or operation of its existing NCII.

CONTACTS

Timothy SIAW

Co-Head, Technology, Media & Telco
Partner, Intellectual Property
Partner, Healthcare and Life Sciences
Shearn Delamore & Co.

E:Timothy@shearndelamore.com

Janet TOH

Head, Personal Data
Co-Head Technology, Media & Telecommunications
Partner, Intellectual Property
Shearn Delamore & Co.

E:Janet.toh@shearndelamore.com

MYANMAR

6. MYANMAR

A) OVERVIEW

Legal Framework

1. What are the main laws governing data protection and cybersecurity in Myanmar?

The Telecommunications Law (2013) primarily targets the telecommunications sector, albeit with limited provisions related to cybersecurity. The main purposes of this law include protecting against cybercrime activities involving telecommunications services and preventing unauthorised disclosure of information kept within secured or encrypted systems to third parties.

The Electronic Transactions Law (2004, amended in 2014 and 2021) facilitates electronic transactions and includes provisions on data protection and cybersecurity. It recognises electronic records and signatures as legally binding and imposes penalties for cybercrimes such as hacking and unauthorised data access.

The Law for Protection of Personal Privacy and Personal Security of Citizens is aimed at protecting individual privacy and personal security. It provides for several rights, including the right to personal privacy free from unauthorised surveillance. It also mandates obtaining consent before collecting and processing personal data. Importantly, the law prohibits the unauthorised collection, use, or dissemination of personal data. Violations are subject to penalties outlined in the law. However, the provisions designed to protect individuals from unauthorised surveillance and the requirements for consent before collecting and processing personal data, as well as the prohibition against unauthorised collection, use, or dissemination of personal data, have been suspended since 2021.

Additionally, within sector-specific sectors, the Financial Institutions Law mandates that banks must maintain confidentiality regarding user information, including accounts, records, and transactions, ensuring data protection within the financial industry.

Data Protection Law – Scope of Application

2. What is the intended objective or main scope of the Telecommunications Law and Electronic Transactions Law?

The Telecommunications Law was enacted in 2013 and amended in 2017. The main aims of this law are to support the development of telecommunication technology, expand the telecommunications network across the whole country, provide guidelines and issue licenses to telecommunication service providers, establish technical standards for telecommunications, and safeguard telecommunication service providers and users. In addition, this law is designed to prevent theft, fraud, misappropriation, or mischief involving money or property through the use

of telecommunications networks. It also aims to protect individuals from extortion, coercion, wrongful restraint, defamation, disturbance, undue influence, or threats made using any telecommunications network.

The Electronic Transactions Law, enacted in 2004 and amended in 2014 and 2021, is aimed at facilitating the country's development through electronic technology. It acknowledges the authenticity and integrity of electronic records and data messages, offering legal protection for electronic transactions and computer network usage, while also safeguarding the public's personal data. In addition, this law prohibits the disclosure of personal data without the individual's consent or legal authorisation. Moreover, this law aims to prevent cyber-attacks and cybercrimes.

3. **What is the scope of personal data protected under the Electronic Transactions Law?**

"Personal Data" is defined in the Electronic Transactions Law as information that identifies or is capable of identifying an individual. While the definition does not explicitly clarify whether it encompasses all forms of personal data, including non-electronic data, section 4(a) specifies the law's applicability to any electronic record and electronic data message. This implies that the law primarily covers electronic forms of personal data.

The law does not distinguish a separate category for sensitive personal data, indicating that all personal data, irrespective of its nature, is subject to the same level of protection under this legislation.

4. **Who must comply with the Electronic Transactions Law?**

This law applies to any individual, company, association, or body of persons that collect, use, or disclose personal data.

The territorial scope of the Electronic Transactions Law is extensive. It applies to any kind of electronic record and electronic data message used in the context of commercial and non-commercial activities, including domestic and international dealings, transactions, arrangements, agreements, contracts, exchanges, and storage of information. The law also holds jurisdiction over any person who commits any offence under this law within the country or from inside the country to outside the country, or from outside the country to inside the country through the use of electronic transactions technology.

Therefore, the law is applicable to all relevant entities, regardless of their location, whether they are established, resident in, or have an office or place of business in Myanmar or abroad.

Cybersecurity Law – Scope of Application

5. What is the intended objective or main scope of the Electronic Transactions Law?

The primary objective of the Electronic Transactions Law is to foster and regulate electronic transactions technology to build a modern, developed nation, facilitate economic growth, recognise the authenticity and integrity of electronic records and data messages, and ensure legal protection in both domestic and international transactions conducted through electronic means.

6. Who must comply with the Electronic Transactions Law?

Organisations and individuals engaged in electronic transactions, data processing activities, management of electronic records, electronic data messages, electronic signatures, and certification authorities must comply with this law.

Data Protection Authority, Enforcement and Appeals

7. Which are the key authorities that administer and enforce the Electronic Transactions Law? What powers do the key authorities have under the Electronic Transactions Law?

The Electronic Transactions Law establishes two key authorities for administration and enforcement: the Central Body of Electronic Transactions ("**CBET**") and the Electronic Transactions Control Board ("**ETCB**").

The CBET is responsible for planning extensive application of electronic transactions technologies, fostering cooperation with international and domestic organisations in this field, and supervising and guiding the Control Board. It holds authority to confirm, revise, or set aside orders or decisions made by the ETCB, and legal prosecution under this law requires prior approval from the CBET.

The ETCB, established with the CBET's approval, has the power to issue licenses to certification authorities and settle disputes between these authorities and subscribers. It also has investigative powers, allowing it to access, inspect, and check the operation of computer systems suspected of involvement in offences under the law. Furthermore, it may require identification documents from individuals related to such offences. In case of violations by certification authorities, the ETCB can impose administrative orders, including fines, as well as suspension or cancellation of licenses.

Penalties for contravention of this law include imprisonment ranging from 1 to 15 years and/or fines ranging from 100,000 to 30,000,000 kyats, depending on the severity of the offence committed.

Additionally, certification authorities found in violation of license conditions or convicted of offences under this Law face administrative remedies, including fines and suspension or cancellation of licenses.

8. **Is there an avenue for appeal against an enforcement decision made under the [Electronic Transactions Law?**

   A person/ an organisation dissatisfied with any order or decision made by the certification authority, such as the refusal to issue a certificate, suspension of a certificate for a specified time, or cancellation of a certificate, may apply for revision to the ETCB within 30 days from the date of the order or decision. If a person is dissatisfied with any order, decision, or administrative decision made by the ETCB, they may apply for revision to the CBET, whose decision is final and conclusive.

   Regarding criminal actions under this law, all offences are considered cognisable offences and must be submitted as complaints to the respective township police station.

Cybersecurity Authority, Enforcement and Appeals

9. **Which are the key authorities that administer and enforce laws on cybersecurity? What powers do the key authorities have under the laws on cybersecurity?**

   There is no separate law. The responses provided for Questions 7 and 8 apply.

10. **Is there an avenue for appeal against a decision made under the laws on cybersecurity?**

    There is no separate law. The responses provided for Questions 7 and 8 apply.

B) DATA PRIVACY AND DATA GOVERNANCE OBLIGATIONS

Obligations Relating to Collection, Use, Disclosure and/or Processing of Personal Data (Data Privacy)

11. **What are the legal bases for processing personal data?**

    The legal bases for processing personal data are multifaceted and context-dependent. While consent is the primary legal basis under the Electronic Transactions Law, as highlighted in section 38-B, it is not the sole basis. This section stipulates penalties for unauthorised actions concerning personal data, emphasising the importance of obtaining consent.

    However, there are specific circumstances outlined in this law where consent is not required for processing personal data. Section 27-C outlines these exceptions, mainly related to national security and law enforcement, as follows:

i. Prevention, search and enquiry, investigation, or the giving of evidence in court by a governmental department authorised by the CBET, an Investigative Team or a rule of law team in relation to cybersecurity, cyber-attacks, Cyber Terrorism, Cyber Misuse, and cyber accidents or crimes;
ii. Search and enquiry, investigation, gathering information, filing a charge, or the giving evidence in court by a governmental department authorised by the CBET, an Investigative Team or a rule of law team mandated to work on a criminal matter;
iii. Enquiry, investigation, gathering information or coordination of information undertaken if cybersecurity and cyber crimes issues are of concern to state sovereignty, peace and stability or national security.

When carrying out activities outlined in sub-section (iii), the CBET, relevant department, or organisation assigned by the CBET, operates with distinct authority and is required to adhere to prescribed relevant standards.

12. Does the Electronic Transactions Law impose other requirements for the collection and processing of personal data?

The Electronic Transactions Law does indeed limit the purposes for which personal data may be collected, used, disclosed, and processed. According to section 27-B, personal data can only be collected, used, disclosed, or processed for specific, lawful purposes directly related to the activities of the entity collecting the data.

In addition, according to section 27-A (3) of the law, the Personal Data Management Officer ("**PDMO**") must refrain from processing personal data contrary to the objectives set out in the law, implying that the data subjects must be informed about the purposes for which their data is being collected and processed. The notification must be provided at the time of the data collection or as soon as practicable thereafter.

13. Does the law impose separate or additional requirements in relation to specific categories of personal data (e.g. sensitive personal data)?

As per the response to Question 3, the law does not specify separate or additional requirements for distinct categories of personal data such as sensitive personal data. Instead, the law broadly addresses matters concerning electronic transactions, electronic records, electronic data messages, and electronic signatures within the context of data processing activities.

Obligations Relating to Care of Personal Data (Data Governance)

14. What obligations does the Electronic Transactions Law impose in relation to the care of personal data?

This law imposes several obligations regarding the care of personal data, including the requirement to systematically store, protect, and process personal data in accordance with its type and security level. The law

specifically prohibits the examination, disclosure, informing, dissemination, coordination, restriction, destroying, copying, or submitting personal data as evidence without consent. It also requires entities to refrain from processing personal data contrary to the objectives set out in the law. Additionally, there is an obligation to destroy all personal data retained within a designated period after the retention period expires.

Data Subject Rights

15. What rights do data subjects have under the Electronic Transactions Law?

While this law does not provide the data subject with specific rights such as the right to access, correction, data, portability, erasure, private action, or to object to the processing of personal data, it does broadly provide for the protection of personal data. The law delineates the responsibilities of the PDMO in handling and processing personal data in compliance with the law's provisions. This indicates that while direct rights may not be specified, the overarching intent of the law is to safeguard personal data through the duties and obligations it imposes on those responsible for managing such data.

C) SECURITY OBLIGATIONS AND DATA BREACH NOTIFICATION

Protection of Personal Data

16. What security obligations are imposed in relation to the processing of personal data?

While the Electronic Transactions Law does not explicitly impose security obligations in relation to the processing of personal data, it does establish comprehensive duties for the PDMO. Pursuant to section 27-A, these duties include the systematic storage, protection, and processing of personal data according to its type and security level in compliance with the law. Additionally, the PDMO is prohibited from allowing the examination, disclosure, informing, dissemination, transmission, alteration, destruction, copying, or submission as evidence of personal data without the consent of the individual or proper legal permission. The PDMO is also required to refrain from processing personal data in ways that are contrary to the objectives set out in the law and must systematically destroy all personal data that are retained beyond the designated retention period. These provisions collectively serve as a framework for the secure handling of personal data within the scope of the law.

Obligations under Electronic Transactions Law

17. What are the security obligations under the Electronic Transactions Law?

The Electronic Transactions Law outlines the security obligations for electronic transactions, which include recognising electronic transactions,

ensuring the authenticity and integrity of electronic records and data messages, protecting personal data, and regulating electronic signatures and certification authorities.

Section 40 allows individuals and entities engaging in electronic transactions to determine the required type and level of security for electronic records and electronic data messages. They are also empowered to select, use, and implement methods that meet their security requirements.

Notification of Security Incidents and Data Breaches

18. Are there notification requirements to notify regulatory authorities and affected data subjects of a data breach? What are the timelines for such notification?

There are no explicit requirements for notifying regulatory authorities or affected data subjects in the event of a data breach in Myanmar.

19. Are there notification requirements in relation to other cybersecurity events? What are the timelines for such notification?

The does not specify notification requirements for other cybersecurity events.

D) OUTSOURCING AND CROSS-BORDER TRANSFERS

International Data Transfers

20. Does the Electronic Transactions Law impose requirements in relation to the transfer of data to other jurisdictions? What are the ways in which these requirements may be met?

The law does not explicitly impose requirements for the transfer of data to other jurisdictions However, it does require consent as a legal basis for the transfer of personal data, unless another legislation permits it. There is no mention of any specific document submission or approval by relevant authorities for data transfer out of the jurisdiction. The law also does not detail any formalities or conditions that must be fulfiled for contractual arrangements in this context.

Appointment of Data Processors and Third-Party Vendors

21. What are the requirements and relevant obligations in relation to appointing a data processor to process personal data on behalf of the data controller?

The Electronic Transactions Law does not explicitly detail the requirements and obligations related to appointing a data processor to process personal data on behalf of a data controller. However, the law does emphasise the protection of personal data and outlines the

responsibilities of the PDMO in handling and processing personal data in accordance with the law.

The PDMO is required to ensure the systematic storage, protection, and processing of personal data in accordance with its type and security level. Additionally, the PDMO is responsible for preventing unauthorised actions such as the examination, disclosure, informing, dissemination, transmission, alteration, destruction, copying, or submission of personal data as evidence without the consent of the individual or proper legal permission. Furthermore, the PDMO must ensure that all processing activities align with the objectives set out in the law and that any personal data retained beyond the designated retention period is systematically destroyed.

No additional sectoral requirements exist in relation to outsourcing data processing.

22. What obligations does the Electronic Transaction Law impose on parties in relation to outsourcing arrangements?

This law does not specify obligations related to outsourcing arrangements. However, it does outline the responsibilities of certification authorities, subscribers, and other entities involved in electronic transactions. These obligations include maintaining the integrity of electronic signatures, complying with specified standards, disclosing services provided, and following security procedures to protect electronic data.

E) ACCOUNTABILITY AND OTHER COMPLIANCE OBLIGATIONS

Data Protection Law - Appointment of Data Protection Officer and Accountability Requirements

23. Is there a requirement to appoint a data protection officer ("DPO")? If so, what is the scope of responsibilities of a DPO and are there any requirements in relation to the DPO's qualifications or experience?

The law does not explicitly require the appointment of a data protection officer ("**DPO**"). There are also no rules and regulations to appoint a DPO. However, the law does outline the responsibilities of the PDMO, who is tasked with the systematic storage, protection, and processing of personal data according to its type and security level in compliance with the law. The PDMO must also prevent unauthorised actions such as examination, disclosure, informing, dissemination, transmission, alteration, destruction, copying, or submission of personal data as evidence without proper consent or legal permission. Additionally, the PDMO is required to ensure that all processing activities align with the objectives set out in the law and that any personal data retained beyond the designated retention period is systematically destroyed.

No requirements are specified for the PDMO's qualifications or experience.

24. Are there other obligations under the Electronic Transaction Law in relation to its data handling processes or compliance with the Electronic Transaction Law?

The law does not specifically require the development of policies and/or processes to demonstrate compliance, nor does it mandate the maintenance of records of data processing activities. In addition, there is no requirement under this law to conduct a data protection impact assessment or similar risk assessment.

The only requirements relevant to data handling are those of the PDMO, as outlined in the response to Question 23.

Cybersecurity Law – Accountability and Compliance Requirements

25. Does the Electronic Transaction Law impose obligations in respect of demonstrating that compliance with the law is met?

The law does not impose obligations in respect of demonstrating that compliance with the law is met.

26. What other key compliance obligations does the Electronic Transaction Law impose?

The key compliance obligations imposed by this law include recognising electronic transactions, ensuring the authenticity and integrity of electronic records and data messages, protecting personal data, and regulating electronic signatures and certification authorities.

CONTACTS

Yuwadee THEAN-NGARM

Partner and Director, Myanmar
Tilleke & Gibbins
E: Yuwadee.t@tilleke.com

Kyaw Min TUN

Associate
Tilleke & Gibbins
E: Myanmar@tilleke.com

PHILIPPINES

7. PHILIPPINES

A) OVERVIEW

Legal Framework

1. What are the main laws governing data protection and cybersecurity in the Philippines?

Data protection and cybersecurity are primarily governed by the Data Privacy Act of 2012 ("**DPA**") and its implementing rules and regulations ("**DPA Rules**").

Cybersecurity is governed by the Cybercrime Prevention Act of 2012 ("**CPA**") and its implementing rules and regulations ("**CPA Rules**")

The CPA defines acts that constitute cybercrimes. These include: (a) offences against the confidentiality, integrity, and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices, cybersquatting), (2) computer-related offences (computer-related forgery, computer-related fraud, computer-related identity theft), and (3) content-related offences (cybersex, child pornography, cyber libel, unsolicited commercial communications).

The CPA likewise covers all crimes defined and penalied under the Revised Penal Code and other special laws, if committed by, through and with the use of information communications technologies ("**ICT**"). These special laws include the following: (a) the Electronic Commerce Act of 2000 and its implementing rules and regulations; (b) the Anti-Online Sexual Abuse or Exploitation of Children and Anti-Child Sexual Abuse or Exploitation Materials Act; (c) the Access Devices Regulation Act of 1998; (d) Anti-Photo and Video Voyeurism Act of 2009; and (e) Subscriber Identity Module (SIM) Registration Act.

Currently pending with the House of Representatives and Senate is the proposed *Critical Information Infrastructure Protection Act*. The bill aims to provide a framework for ensuring the security and reliability of the country's critical information infrastructure ("**CII**"), such as water, electricity, banking and financial networks, telecommunications and other networks vital to the country's operation. The bill aims to protect the cybersecurity of CII by requiring: (a) the adoption of minimum information security standards, (b) the creation of a computer emergency response team and reporting of cybersecurity incidents, and (c) the development of a capable pool of cybersecurity professionals and practitioners that will be critical to the effective implementation of cybersecurity policy, rules and standards.

Data Protection Law – Scope of Application

2. What is the intended objective or main scope of the DPA?

The DPA was enacted in 2012 with the objective of protecting the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth. The DPA also encapsulates the State's recognition of the vital role of ICT in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and the private sector are secured and protected.

3. What is the scope of personal data protected under the DPA?

The DPA and the DPA Rules apply to the processing of all types of personal information including sensitive personal information and privileged information. These are collectively referred to in the DPA as "personal data". Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[9]

Personal information is considered sensitive personal information when it is:

- about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offence committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
- issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
- specifically established by an executive order or an act of Congress to be kept classified.[10]

Personal information is considered privileged information if it pertains to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication. Examples of privileged communication are those information made in confidence between married persons, priest and penitent, doctor and patient, and attorney and client.[11]

[9] Section 3(g), DPA.
[10] Section 3(l), DPA.
[11] Section 3(k), DPA.

The DPA however does not apply to the following:

- information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual;
- information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;
- information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;
- personal information processed for journalistic, artistic, literary or research purposes;
- information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions;
- information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with the Anti-Money Laundering Act and other applicable laws; and
- personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.[12]

4. Who must comply with the DPA?

The DPA applies to the processing of personal data and to any natural or juridical person involved in personal data processing including personal information controllers ("**PICs**") or personal information processors ("**PIPs**"), whether in the government or private sector, and who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines.[13]

It applies to an act done or practice engaged in and outside of the Philippines if:

- the natural or juridical person involved in the processing of personal data is found or established in the Philippines;

[12] Id.
[13] Section 4, DPA.

- the act, practice or processing relates to personal data about a Philippine citizen or a resident;
- the processing of personal data is being done in the Philippines; or
- the act, practice or processing of personal data is done or engaged in by an entity with links to the Philippines such as the following: (a) use of equipment located in the country, or maintaining an office, branch or agency in the Philippines for processing of personal information; (b) a contract is entered in the Philippines; (c) a juridical entity unincorporated in the Philippines but has central management and control in the country; (d) an entity that has a branch, agency, office or subsidiary in the Philippines, and the parent or affiliate of the Philippine entity has access to personal data; (e) an entity that carries on business in the Philippines; or (f) an entity that collects or holds personal data in the Philippines.[14]

Cybersecurity Law – Scope of Application

5. What is the intended objective or main scope of the CPA?

The main objective of the CPA is to create an environment conducive to the use and development of ICT to attain free, easy and intelligible access to the exchange and/or delivery of information, and to protect the integrity of computer, computer and communications systems, networks, and databases and the confidentiality, integrity, and availability of information and data stored therein by making punishable under the law the misuse, abuse, and illegal access to the same.

6. Who must comply with the CPA?

The CPA is primarily targeted at internet users, the same law being focused on prevention and prosecution of cybercrimes. In relation to the investigation and prosecution of cybercrimes, the CPA imposes certain duties upon service providers (including internet service providers or "**ISPs**") and internet hosts. A service provider refers to (a) any public or private entity that provides users of its service with the ability to communicate by means of a computer system, or (b) any other entity that processes or stores computer data on behalf of such communication service or users of such service. An internet host, on the other hand, refers to a person who hosts or who proposes to host internet content in the Philippines.

Data Protection Authority, Enforcement and Appeals

7. Which are the key authorities that administer and enforce the DPA? What powers do the key authorities have under the DPA?

The National Privacy Commission ("**NPC**") is the primary regulatory authority tasked to administer and implement the DPA, and to monitor

[14] Rule II, Section 4, DPA Rules.

and ensure the country's compliance with international standards set for data protection.[15]

To this end, the NPC is empowered to receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicise any such report. In addition, upon finding that the processing will be detrimental to national security and public interest, the NPC is likewise empowered to issue cease and desist orders, or impose a temporary or permanent ban on the processing of personal information. Further, in certain instances, the NPC may recommend to the Department of Justice (**"DOJ**") the prosecution and imposition of penalties in accordance with the DPA. It may also perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection.

Under NPC Circular No. 2024-01, the NPC's Compliance and Monitoring Division ("**CMD**") may conduct privacy sweeps over PICs and PIPs, as an initial mode of compliance check based on publicly available or accessible information (e.g. websites, mobile applications, raffle coupons, brochures, and privacy notices). Privacy sweeps may be on-the-spot, limited to public areas and publicly available or accessible information. The CMD may verify compliance by examining all physical or digital forms, including, but not limited to data processing systems, logbooks, raffle coupons, brochures, and posters used in the PIC's or PIP's operations.

Violations of the DPA, the DPA Rules and other NPC issuances, may merit criminal, civil, and administrative liabilities.

[15] Section 7, DPA.

Criminal liability under the DPA[16]

Act	Fine (in PHP)	Imprisonment
1. Unauthorised Processing		
• Personal Information	500,000 - 2 million	1-3 years
• Sensitive Personal Information	500,000 - 4 million	3-6 years
2. *Accessing Information Due to Negligence*		
• Personal Information	500,000 - 2 million	1-3 years
• Sensitive Personal Information	500,000 - 4 million	3-6 years
3. *Improper Disposal*		
• Personal Information	100,000 - 500,000	6 months - 2 years
• Sensitive Personal Information	100,000.00 - 1 million	1-3 years
4. Processing for Unauthorised Purposes		
• Personal Information	500,000.00 - 1 million	1 year and 6 months - 5 years
• Sensitive Personal Information	500,000 - 2 million	2-7 years
5. Unauthorised Access or Intentional Breach	500,000 - 2 million	1-3 years
6. Concealment of Security Breaches Involving Sensitive Personal Information	500,000 - 1 million	1 year and 6 months - 5 years
7. Malicious Disclosure	500,000 - 1 million	1 year and 6 months - 5 years
8. Unauthorised Disclosure		
• Personal Information	500,000 -1 million	1-3 years
• Sensitive Personal Information	500,000 - 2 million	3-6 years
9. Combination or Series of Acts	1 million - 5 million	3-6 years

The maximum penalty in the scale of penalties shall be imposed when the personal data of at least 100 persons is harmed, affected or involved as the result of the above-mentioned actions.[17]

Should the violation be committed by a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers who participated in, or by their gross negligence allowed, the

[16] Sections 25 to 33, DPA.
[17] Sections 35, DPA.

commission of the crime.[18] Additionally, the court may suspend or revoke any of the juridical entity's rights under the DPA.[19]

In addition to the above penalties, if the offender is an alien, he or she shall be deported without further proceedings after serving the penalties prescribed.[20]

- **Civil liability under the DPA**

  In the event of a violation of data subject rights, a PIC or PIP may be held liable for damages. The NPC has clarified that it may award nominal damages in recognition of the violated legal rights of a complainant.[21]

- **Administrative liability under NPC Circular No, 2022-01**

  Administrative fines may be imposed for failure to abide by the requirements of the DPA, its Implementing Rules and Regulations ("**IRR**") and NPC issuances. NPC Circular No, 2022-01 imposes varying fines in accordance with the classification of infractions based on gravity:

  - *Grave infractions* pertain to violations of general privacy principles and data subject rights involving more than 1,000 data subjects. These likewise cover repetitions of the same infraction regardless of classification. An administrative fine may be imposed at the rate of 0.5% to 3% of the violator's annual gross income of the immediately preceding year when the infraction occurred.

  - *Major infractions* pertain to: (a) infraction of any of the general privacy principles in the processing of personal data, where the total number of affected data subjects is 1,000 or below; (b) each infraction of any of the data subject rights, where the total number of affected data subjects is 1,000 or below; (c) failure by a PIC to implement reasonable and appropriate measures to protect the security of personal data; (d) failure by a PIC to ensure that third parties processing personal data on its behalf shall implement security measures; or (d) failure by a PIC to notify the NPC and affected data subjects of personal data breaches. An administrative fine may be imposed at the rate of 0.25% to 2% of the violator's annual gross income of the immediately preceding year.

  - *Other infractions* pertain to failure to register the true identity or contact details and to provide updated information as to the identity or contact details of the PIC, the data processing system, or information on automated decision-making. For this, the penalty is between PHP 50,000 to PHP 200,000. Other infractions likewise cover the failure to comply with any order, resolution, or decision of the NPC and its corresponding implementing issuance, which shall be subject to a penalty not exceeding PHP 50,000, in addition to whatever fine may be imposed under the original order, resolution, or decision.

[18] Sections 34, DPA.
[19] *Id*.
[20] *Id*.
[21] *MNLC INC. represented by IKP v. PXXX Corporation, RMC and AD*, NPC Case No. 19-528, dated 23 February 2021, accessible at https://privacy.gov.ph/wp-content/uploads/2023/05/Resolution-02.23.2021-NPC-19-528-MNLC-vs-PXXX-Corporation.pdf.

The total imposable fine for a single act of a PIC or PIP however, whether resulting in single or multiple infractions, shall not exceed PHP 5 million.

8. **Is there an avenue for appeal against an enforcement decision made under the DPA?**

Under NPC Circular No. 2024-01, an organisation may file a motion for consideration within 15 calendar days from notice of the NPC's decision. Only one motion for reconsideration is allowed. Any appeal to the decision shall be to the proper courts.

Cybersecurity Authority, Enforcement and Appeals

9. **Which are the key authorities that administer and enforce the CPA? What powers do the key authorities have under the CPA?**

The key authorities that implement the CPA are the following:

- Cybercrime Investigation and Coordinating Center, an inter-agency body tasked to, among others, formulate a national cybersecurity plan, monitor cybercrime cases handled by participating law enforcement and prosecution agencies, and recommend the enactment of appropriate laws, issuances, measures and policies on cybersecurity.

- Department of Justice - Office of Cybercrime ("**DOJ-OOC**"), the central authority in matters related to cybercrime. It has the power to act on complaints/referrals and cause the investigation and prosecution of cybercrimes and other violations of the CPA, to issue preservation orders, subpoena and summon witnesses to appear in investigations or proceedings, and to require the submission of timely and regular reports from the Philippine National Police ("**PNP**") and the National Bureau of Investigation ("**NBI**") for monitoring and review.[22]

- Computer Emergency Response Team of the Department of Information and Communications Technology, serving as focal point for cybersecurity-related activities by providing technical analysis, conducting research and development, and conducting technical training.

- The cybercrime divisions of the law enforcement authorities, namely, the NBI and the PNP, with powers to investigate all cybercrimes where computer systems are involved.[23] These law enforcement authorities may be authorised to search and seize computer data upon proper application with and grant by the court of a warrant for the same.

[22] Sections 3(D) and 28, CPA Rules.
[23] Sections 10, CPA Rules.

The CPA Rules identify different punishable offences.

- Illegal access, illegal interception, data Interference, system interference, and misuse of devices are considered *offences against the confidentiality, integrity and availability of computer data systems*.[24] These offences are punishable by imprisonment of six years and one day to 12 years, or a fine of at least PHP 200,000 up to a maximum amount commensurate to the damage incurred, or both. For misuse of devices, the fine may not be more than PHP 500,000.

- *Computer-related offences*,[25] which refer to computer-related fraud, computer-related identity theft, and content-related offences, are punishable by imprisonment of six years and one day to 12 years, or a fine of at least PHP 200,000 up to a maximum amount commensurate to the damage incurred, or both.

- Aside from the above offences which pertain to the security of computer data, the CPA also punishes *content-related offences*[26] and *other cybercrimes*[27] done online or through the use of information and communication technology.

10. Is there an avenue for appeal against a decision made under the CPA?

The Regional Trial Court ("**RTC**") has jurisdiction over violations of the CPA.[28] An ordinary appeal from the decision of the RTC may be made by filing a notice of appeal to the Court of Appeals. In cases where only questions of law are raised, an appeal by certiorari may made to the Supreme Court by filing a petition for review on certiorari in accordance with rule 45 of the Rules of Court.

B) DATA PRIVACY AND DATA GOVERNANCE OBLIGATIONS

Obligations Relating to Collection, Use, Disclosure and/or Processing of Personal Data (Data Privacy)

11. What are the legal bases for processing personal data?

Consent is the main legal basis of processing personal data in the Philippines. However, processing of personal information without the consent of the data subject may be allowed if:

- necessary and related to the fulfilment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;

[24] Section 4(A), CPA Rules.
[25] Section 4(B), CPA Rules.
[26] Section 4(C), CPA Rules.
[27] Section 5, CPA Rules.
[28] Section 21, CPA Rules.

- necessary for compliance with a legal obligation to which the PIC is subject;
- necessary to protect vitally important interests of the data subject, including life and health;
- necessary in order to respond to national emergency, comply with requirements of public order and safety, or fulfil functions of public authority which necessarily includes the processing of personal data for the fulfilment of its mandate; or
- necessary for the purposes of the legitimate interests pursued by the PIC or by third parties to whom data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

Processing of sensitive personal information and privileged information is generally prohibited unless there is specific and prior consent from the data subject, or if:

- the processing of the data is provided for by existing law and regulations;
- necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
- necessary to achieve the lawful and noncommercial objectives of public organisations and their associations;
- necessary for the purposes of medical treatments, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
- the processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defence of legal claims, or when provided to government or public authority.

12. Does the DPA impose other requirements for the collection and processing of personal data?

Processing of personal data must adhere to the principles of transparency, legitimate purpose, and proportionality.

Simply put, the principle of transparency requires that the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks, safeguards involved, the identity of the PIC, his or her data subject rights and how these can be

exercised.[29] Accordingly, the data subject must be informed of the following before the entry of his or her personal information into the PIC's processing system or at the next practical opportunity:

- description of the personal data to be entered into the system;
- purposes for which they are being or are to be processed;
- scope and method of the personal data processing;
- the recipients or classes of recipients to whom they are or may be disclosed;
- methods utilised for automated access, if the same is allowed by the data subject, and the extent to which such access is authorised;
- identity and contact details of the personal information controller or its representative;
- period for which the information will be stored; and
- existence of the data subject's rights, i.e. to access, correction, as well as the right to lodge a complaint before the NPC.

The principle of legitimate purpose, on the other hand, states that personal data may be processed when not prohibited by law and pursuant to any of the legal bases (see Question 11).

Under the principle of proportionality, the processing of personal data must be adequate, relevant, suitable, necessary, and not excessive in relation to the declared and specified purpose.[30]

13. Does the law impose separate or additional requirements in relation to specific categories of personal data (e.g. sensitive personal data)?

Compared to personal information, the processing of sensitive personal and privileged information is generally prohibited unless pursuant to any of the legal bases discussed above (see Question 11). Notably, legitimate interest is not a ground for processing sensitive personal and privileged information.[31]

[29] NPC Privacy Policy Office Advisory Opinion No. 2022-015 dated 23 June 2022 accessible at https://privacy.gov.ph/wp-content/uploads/2022/08/Advisory-Opinion-No-2022-015-FINAL-sgd_Redacted.pdf.
[30] NPC Privacy Policy Office Advisory Opinion No. 2022-015 dated 23 June 2022 accessible at https://privacy.gov.ph/wp-content/uploads/2022/08/Advisory-Opinion-No-2022-015-FINAL-sgd_Redacted.pdf.
[31] NPC Circular No. 2023-07 dated 13 December 2023, accessible at https://privacy.gov.ph/wp-content/uploads/2024/01/NPC-Circular-No.-2023-07_Guidelines-on-Legitimate-Interest_13-December-2023.pdf.

Obligations Relating to Care of Personal Data (Data Governance)

14. What obligations does the DPA impose in relation to the care of personal data?

A PIC or PIP must ensure implementation of the following personal data processing principles, among others:

- Personal data must be accurate, relevant and, where necessary for purposes for which it is to be used, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.

- The personal data must be adequate and not excessive in relation to the purposes for which they are collected and processed. Only personal data that is necessary and compatible with the declared, specified and legitimate purpose shall be collected.

- The personal data must be retained only for as long as necessary for the fulfilment of the purposes for which the data was obtained or for the establishment, exercise or defence of legal claims, or for legitimate business purposes, or as provided by law. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorised access, or disclosure to any other party or to the public, or prejudice to the interests of the data subjects.

Data Subject Rights

15. What rights do data subjects have under the DPA?

Right to be informed

Data subjects have the right to be informed of the following: (a) that personal data pertaining to them have been processed or are being processed; (b) the existence of automated decision-making and profiling; (c) description of the personal data to be entered into the system; (d) purposes for which data are being processed; (e) basis of processing, if processing is not based on consent; (f) scope and method of personal data processing; (g) recipients and persons to whom personal data may be disclosed; (h) methods utilised for automated access, if the same is allowed by the data subject; (i) identity and contact details of the personal data controller or its representative; (j) period for which the information will be stored; and (k) existence of their rights as data subjects.

Right to object

Data subjects have the right to object to the processing of their personal data. The data subjects shall also be notified and given an opportunity to withhold their consent to the processing in case of changes or an amendment to the information supplied or declared to the data subject.

Right to access

Data subjects have the right to demand reasonable access to the following, among others: (a) the contents of the personal data that were processed; (b) sources from which personal data were obtained; (c) names and addresses of recipients of personal data, and the reasons for the disclosure to such recipients; (d) manner by which personal data was processed; and (e) date when personal data was last accessed and modified.

Right to rectification

In case of inaccuracies in the processed data, the data subject must also be given the right to have them corrected or rectified immediately.

Right to erasure or blocking

The right to erasure or blocking is also available when personal data are unlawfully obtained, outdated, no longer necessary for the purposes for which they were collected, actually contain private information prejudicial to the data subject, or the data subject has withdrawn consent, or when the PIC or PIP violated the rights of the data subject.

Right to data portability

Where the personal data of a data subject is processed by electronic means and in a structured and commonly used format, the data subject shall have the right to obtain from the PIC a copy of such data in an electronic or structured format that is commonly used and allows for further use by the data subject.

Right to damages

Data subjects may also demand indemnification for damages caused by inaccurate, erroneous, outdated, or unlawful processing of their data, and have the right to institute the appropriate action before the NPC.

C) SECURITY OBLIGATIONS AND DATA BREACH NOTIFICATION

Protection of Personal Data

16. What security obligations are imposed in relation to the processing of personal data?

PICs and PIPs are required to implement reasonable and appropriate organisational, physical, and technical security measures for the protection of personal data.[32] In determining the level of security appropriate, the nature of the personal data that requires protection, the risks posed by the processing, the size of the organisation and

[32] Section 20(a), DPA.

complexity of its operations, current data privacy best practices, and the cost of security implementation are taken into account.[33]

Obligations under the CPA

17. What are the security obligations under the CPA*?*

See Question 26 on relevant security obligations required of service providers.

Notification of Security Incidents and Data Breaches

18. Are there notification requirements to notify regulatory authorities and affected data subjects of a data breach? What are the timelines for such notification?

Under NPC Circular No. 16-03, "personal data breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A "security incident" on the other hand is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It includes incidents that would result in a personal data breach, if not for safeguards that have been put in place.

Notification of a personal data breach shall be required under the following conditions:

- Sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud are involved. Such other information include: (a) data about the financial or economic situation of the data subject, (b) usernames, passwords and other login data, (c) biometrics data, and (d) copies of identification documents;
- The information is reasonably believed to have been acquired by an unauthorised person; and
- The PIC or the NPC believes that such unauthorised acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[34]

Under section 38 of the DPA Rules, the PIC must notify the NPC and affected data subjects within 72 hours upon knowledge of, or when there is reasonable belief by the PIC or PIP that, a personal data breach requiring notification has occurred.

[33] Section 20 (c), DPA.
[34] Section 11, NPC Circular No. 16-03 dated 27 December 2016 accessible at https://privacy.gov.ph/npc-circular-16-03-personal-data-breach-management/#3.

Notification may be delayed to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. However, there shall be no delay in the notification if the breach involves at least 100 data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the NPC shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five days, unless the PIC is granted additional time by the NPC to comply.

19. Are there notification requirements in relation to other cybersecurity events? What are the timelines for such notification?

PICs and PIPs are required to submit Annual Security Incident Reports to the NPC, noting security incidents that do not constitute notifiable breach.

D) OUTSOURCING AND CROSS-BORDER TRANSFERS

International Data Transfers

20. Does the DPA impose requirements in relation to the transfer of data to other jurisdictions? What are the ways in which these requirements may be met?

Currently, there are no specific requirements on cross-border transfers. The transfer of data to other jurisdictions will be considered as processing of personal data within the scope of the DPA, and subject to the requirements and conditions for the processing of personal information discussed above.

Appointment of Data Processors and Third-Party Vendors

21. What are the requirements and relevant obligations in relation to appointing a data processor to process personal data on behalf of the data controller?

PICs may appoint PIPs who may process personal information for the PIC. The appointment of the PIP must be governed by a contract or other legal act that binds the PIP to the PIC. Section 44 of the DPA lists the required stipulations in the contract appointing a PIP. The contract must, among others, set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the personal information controller, and the geographic location of the processing under the subcontracting agreement.

The obligations of the PIP under the DPA are largely the same as the obligations of the PIC. Like the PIC, the PIP must abide by the general privacy principles, appoint a DPO and register with the NPC Registration System if required pursuant to NPC Circular Nol. 2022-04, uphold the rights of data subjects, implement security measures to protect data, and

abide by the provisions on data breach notification. Notwithstanding the appointment of a PIP, however, the PIC is still responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal data processed, prevent its use for unauthorised purposes, and that the data processing is compliant with the legal requirements on personal data processing.

22. What obligations does the CPA impose on parties in relation to outsourcing arrangements?

There are no specific requirements as to outsourcing under the CPA.

E) ACCOUNTABILITY AND OTHER COMPLIANCE OBLIGATIONS

Data Protection Law - Appointment of Data Protection Officer and Accountability Requirements

23. Is there a requirement to appoint a data protection officer ("DPO")? If so, what is the scope of responsibilities of a DPO and are there any requirements in relation to the DPO's qualifications or experience?

PICs and PIPs must have their own Data Protection Officer ("**DPO**"). The DPO should ideally be a regular or permanent position. Where the DPO's employment is based on contract, the term or duration thereof should at least be two years to ensure stability. Different entities may likewise appoint a "common DPO", defined as an individual who is a member of a group of related companies or an individual consultant under contract with several separate PICs and PIPs.

The DPO is primarily responsible for ensuring the PIC/PIP's compliance with the DPA, the DPA Rules and other relevant NPC issuances. A DPO must also ensure the conduct of Privacy Impact Assessments relative to the PIC/PIP's activities, measures, projects, programs, and systems; advise the PIC regarding the rights of data subjects and of complaints by such persons; ensure proper data breach and security incident management by the PIC/PIP; and serve as the contact person of the PIC/PIP vis-à-vis their data subjects, the NPC and all other authorities in matters concerning data privacy or security.

Given the scope of its tasks, the DPO must be knowledgeable of the relevant privacy or data protection policies and practices, and must have sufficient understanding of the processing and operations being carried out by the PIC/PIP such as the latter's information systems, data security, and/or data protection needs.

The PIC/PIP must provide the contact details of its appointed DPO on its website, privacy notice, privacy policy, and privacy manual or privacy guide.

24. Are there other obligations under the DPA in relation to its data handling processes or compliance with the DPA?

Privacy policy

The PIC or PIP must implement reasonable and appropriate organisational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing. The PIC or PIP shall take steps to ensure that any natural person acting under its authority and who has access to personal data does not process them except upon their instructions or as required by law. To this end, the NPC recommends organisations develop a privacy policy to serve as a guide or handbook for ensuring the organisation's compliance with the DPA.

Registration of data processing systems

NPC Circular No. 2022-04 provides for mandatory and voluntary registration of data processing systems, to ensure that PICs and PIPs keep a record of their data processing activities and to guarantee that information about data processing systems owned by PICs or PIP operating in the country are made accessible to the NPC.

PICs or PIPs who fall under the criteria below are mandated to register their data processing systems through the NPC's online registration portal, or the National Privacy Commission Registration System:

- a PIC or PIP that employs 250 or more persons; or
- those processing sensitive personal information of 1,000 or more individuals; or
- those processing data that will likely pose a risk to the rights and freedoms of data subjects; or
- any government agency or instrumentality.

Privacy Impact Assessment ("PIA")

As a general rule, a PIA should be conducted for every processing system involving the processing of personal data.[35] The PIA must be properly documented in a report that includes information on stakeholder involvement, proposed measures for privacy risk management, and the process through which the results of the PIA will be communicated to internal and external stakeholders.

[35] A PIA is conducted for the following purposes: (i) identify, assess, evaluate, and manage the risks represented by the processing of personal data; (ii) assist in preparing the records of its processing activities, and in maintaining its privacy management program; (iii) facilitate compliance with the DPA, and DPA IRR, and other applicable issuances of the NPC, by determining: (1) its adherence to the principles of transparency, legitimate purpose and proportionality; (2) its existing organisational, physical and technical security measures relative to its data processing systems; (3) the extent by which it upholds the rights of data subjects; and (iv) aid in addressing privacy risks by allowing it to establish a control framework.

NPC Advisory No. 2017-03 outlines the guidelines on privacy impact assessments ("**PIA Guidelines**"). This applies to all natural or juridical persons, or any other body in the government or private sector engaged in the processing of personal data within and outside of the Philippines.

Cybersecurity Law – Accountability and Compliance Requirements

25. Does the CPA impose obligations in respect of demonstrating that compliance with the law is met?

The purpose of CPA is to penalise activities detrimental to cybersecurity, rather than regulate the handling of ICTs or CII. As a special penal law, the CPA does not provide for obligations to demonstrate compliance with the law.

26. What other key compliance obligations does the CPA impose?

The following are the duties of a service provider:

- preserve the integrity of traffic data and subscriber information for a minimum period of six months from the date of the transaction;
- preserve the integrity of content data for six months from the date of receipt of the order from law enforcement or competent authorities requiring its preservation, and for an extended period of six months from the date of receipt of the order from law enforcement or competent authorities requiring extension of preservation;
- preserve the integrity of computer data until the final termination of the case and/or as ordered by the court;
- ensure the confidentiality of the preservation orders and its compliance;
- collect or record by technical or electronic means, and/or cooperate and assist law enforcement or competent authorities in the collection or recording of computer data that are associated with specified communications transmitted by means of a computer system;
- disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control to law enforcement or competent authorities upon receipt of order and/or copy of the court warrant;
- report to the DOJ-OOC compliance with its duties as provided in the CPA Rules; and
- immediately and completely destroy the computer data subject to preservation and examination by law enforcement or competent authorities after the expiration of the prescribed periods under the CPA.

Additionally, in relation to child pornography cases:

- An ISP or internet content host shall install available technology, program or software, such as, but not limited to, system/technology that produces hash value or any similar calculation, to ensure that access to or transmittal of any form of child pornography will be blocked or filtered;
- Service providers shall immediately notify law enforcement authorities of facts and circumstances relating to any form child pornography that passes through or are being committed in their system; and
- A service provider or any person in possession of traffic data or subscriber's information, shall, upon the request of law enforcement or competent authorities, furnish the particulars of users who gained or attempted to gain access to an internet address that contains any form of child pornography. ISPs shall also preserve customer data records, specifically the time, origin, and destination of access, for purposes of investigation and prosecution by relevant authorities.

CONTACTS

Erika B. PAULINO

Partner
Head, Data Privacy and Security
Martinez Vergara & Gonzalez Sociedad

E:Erika.paulino@mvgslaw.com

Kristine R. BONGCARON

Partner
Co-Head, Data Privacy and Security
Martinez Vergara & Gonzalez Sociedad

E:Kristine.bongcaron@mvgslaw.com

SINGAPORE

8. SINGAPORE

A) OVERVIEW

Legal Framework

1. What are the main laws governing data protection and cybersecurity in Singapore?

The main law governing data protection in Singapore is the Personal Data Protection Act 2012 ("**PDPA**"). Meanwhile, the Public Sector (Governance) Act 2018 ("**PSGA**") governs data protection and management in the public sector.

Additionally, there are other sector-specific legislation that contain data protection requirements such as the Banking Act 1970 which governs customer information obtained by banks; and the Healthcare Services Act 2020 which contains provisions relating to medical information and records. Further, certain legislation, such as the Telecommunications Act 1999 and Monetary Authority of Singapore Act 1970, empower regulatory authorities to issue codes and guidelines which are relevant to data protection.

Cybersecurity in Singapore is broadly regulated by a set of overlapping legislation. However, the main law governing cybersecurity in Singapore is the Cybersecurity Act 2018 ("**Cybersecurity Act**"). Other relevant laws include the Computer Misuse Act 1993 and the PDPA which, among other things, cover the enforcement against cyber-related offences and security over personal data respectively.

Aside from these, sectoral regulators such as the Info-communications Media Development Authority ("**IMDA**") and Monetary Authority of Singapore ("**MAS**") have also issued codes and guidelines with regard to cybersecurity practices.

Data Protection Law – Scope of Application

2. What is the intended objective or main scope of the PDPA?

The PDPA was enacted in 2012 with the aim of governing the collection, use and disclosure of personal data by organisations. It recognises the right of individuals to protect their personal data and the needs of organisations to collect and use personal data for appropriate purposes.

The PDPA also provides for the establishment of a national Do Not Call registry. Organisations engaged in certain telemarketing practices must comply with the PDPA's Do Not Call requirements.

3. What is the scope of personal data protected under the PDPA?

All forms of personal data, whether electronic or non-electronic and regardless of the degree of sensitivity, are covered under the PDPA.

"Personal data" is defined under the PDPA as data, whether true or not, about an individual who can be identified: (a) from that data; or (b) from that data and other information to which the organisation is likely to have access.

However, it should be noted that business contact information falls outside of the scope of the PDPA. Such information refers to an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his/her personal purposes.

4. Who must comply with the PDPA?

The PDPA applies to all organisations that collect, use or disclose personal data in Singapore. This includes any individual, company, association or body of persons regardless of where they are established, resident or have an office or place of business in Singapore.

However, the PDPA does not apply to individuals acting in a personal or domestic capacity or as an employee. Also, collection, use and disclosure of personal data by public agencies is governed by the PSGA.

Cybersecurity Law – Scope of Application

5. What is the intended objective or main scope of the Cybersecurity Act?

There are four key objectives of the Cybersecurity Act:

- To designate computer systems as Critical Information Infrastructure ("**CII**") to strengthen protection against cyber-attacks;
- To authorise and empower the Cyber Security Agency ("**CSA**") to prevent and respond to cybersecurity threats and incidents;
- To establish a framework for sharing cybersecurity information between the CSA and CII owners; and
- To establish a licensing framework for Cybersecurity Service Providers ("**CSPs**").

6. Who must comply with the Cybersecurity Act?

At present, the owners of CII, as designated by the Commissioner of Cybersecurity (the "**Commissioner**"), must comply with obligations under the Cybersecurity Act.

Pursuant to section 7 of the Cybersecurity Act, the Commissioner may designate a computer or computer system as CII if he is satisfied that: (a) the computer or computer system is necessary for the continuous

delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore; and (b) the computer or computer system is located wholly or partly in Singapore.

The First Schedule to the Cybersecurity Act states the list of essential services and these relate to the following industries: energy; info-communications; water; healthcare; banking and finance; security and emergency services; aviation; land transport; maritime; services relating to the functioning of government; and media.

Additionally, CSPs (i.e. persons who provide cybersecurity services as prescribed in the Second Schedule to the Cybersecurity Act) must be licensed under the Cybersecurity Act and comply with the Act as well as any licensing conditions.

On 7 May 2024, the Cybersecurity (Amendment) Bill ("**CS Amendment Bill**") was passed in the Singapore Parliament. Once these amendments are brought into force the coverage of the Cybersecurity Act will go beyond owners of CII, to also cover designated providers of essential services that rely on third-party-owned CII ("**designated provider responsible for third-party-owned CII**").

In addition, the scope of the Cybersecurity Act will be expanded to regulate the following categories of systems/services:

- Owners of computers or computer systems designated as systems of temporary cybersecurity concern ("**STCC**"), e.g. systems that are set up specifically to support high-key international events in Singapore or systems set up to support the distribution of vaccines during the COVID-19 pandemic.
- Designated entities of special cybersecurity interest ("**ESCI**"), e.g. systems that if compromised, could have a significant detrimental effect on the defence, foreign relations, economy, public health, safety or order of Singapore; and
- Designated providers of major foundational digital infrastructure ("**FDI**") services, e.g. cloud computing and data facility services that are integral to the functioning of Singapore's technological stacks;

Data Protection Authority, Enforcement and Appeals

7. Which are the key authorities that administer and enforce the PDPA? What powers do the key authorities have under the PDPA?

The Personal Data Protection Commission ("**PDPC**") is the authority responsible for the administration and enforcement of the PDPA.

Upon receiving a complaint or of its own motion, the PDPC may conduct an investigation into whether an organisation is complying with the PDPA. The PDPC's powers of investigation are provided under section 50, read with the Ninth Schedule to the PDPA. This includes the power to require documents or information and enter any premises with or without a warrant.

If the PDPC determines that an organisation has not complied with the PDPA, the PDPC may:

- Give the organisation a direction to ensure its compliance with the PDPA; and
- If satisfied that the organisation intentionally or negligently contravened the PDPA, require payment of a financial penalty not exceeding the higher of 10% of the organisation's turnover in Singapore or S$1 million (a lower maximum may apply in certain situations).

Where the PDPC has reasonable grounds to believe that an organisation has not complied with the PDPA, the PDPC may also accept a voluntary undertaking from the organisation (for example, an undertaking to take certain remedial action within a specified time). If the organisation subsequently fails to comply with the voluntary undertaking, the PDPC may take enforcement action against the organisation.

8. Is there an avenue for appeal against an enforcement decision made under the PDPA?

Where an organisation is unsatisfied with an enforcement direction or decision made by the PDPC under the PDPA, it may make a written application to the PDPC to reconsider the direction or decision under section 48N of the PDPA.

Alternatively, the organisation may make an appeal to the Data Protection Appeal Panel ("**DPAP**") if it is aggrieved by the direction or decision made by the PDPC.

Where the organisation wishes to appeal against the direction or decision of the DPAP on a point of law or in relation to a financial penalty amount, it may make an appeal to the General Division of the High Court pursuant to section 48Q of the PDPA.

Data subjects who are aggrieved by the decision or direction of the PDPC may also make such appeals to the PDPC, DPAP or General Division of the High Court.

Cybersecurity Authority, Enforcement and Appeals

9. Which are the key authorities that administer and enforce the Cybersecurity Act? What powers do the key authorities have under the PDPA?

The authority responsible for the administration and enforcement of the Cybersecurity Act is the CSA, which is led by the Commissioner.

The Commissioner has a broad range of powers under the Cybersecurity Act. This includes:

- The power to issue directions to the owners of CII (and once the CS Amendment Bill is in force, designated providers responsible for third-party-owned CII) to take actions in relation to a cybersecurity threat, participate in cybersecurity exercises, comply with any code of practice, appoint an auditor to audit their compliance with any code of practice, or for any other matters necessary to ensure the cybersecurity of the CII; and
- The power to investigate and prevent cybersecurity incidents, including making requests for information and documents and making directions for remedial action to be taken.

Depending on the non-compliance, penalties may include fines and/or terms of imprisonment

10. Is there an avenue for appeal against a decision made under the Cybersecurity Act?

Persons who are aggrieved by a decision made under the Cybersecurity Act may make an appeal to the Minister of Communications and Information against a decision or direction of the Commissioner/licensing officer.

B) DATA PRIVACY AND DATA GOVERNANCE OBLIGATIONS

Obligations Relating to Collection, Use, Disclosure and/or Processing of Personal Data (Data Privacy)

11. What are the legal bases for processing personal data?

The PDPA provides a number of legal bases for the collection, use and disclosure of personal data. In particular, section 13 of the PDPA provides that organisations may not collect, use or disclosure an individual's personal data except with the individual's consent or deemed consent or where collection, use or disclosure of the individual's personal data without their consent is permitted or required under the any written law (including the PDPA itself).

Valid Consent

For consent to be considered validly obtained, the organisation must first inform the data subject of the purposes for which his/her personal data will be collected, used or disclosed (section 14(1) read with section 20 of the PDPA).

Deemed Consent

The PDPA provides for three types of deemed consent: deemed consent by conduct (section 15(1) of the PDPA), deemed consent by notification (section 15A of the PDPA) and deemed consent by contractual necessity (sections 15(3) and 15(6) of the PDPA).

Deemed consent by conduct applies where a data subject voluntarily provides his/her personal data to an organisation for a purpose, and it is reasonable that he/she would voluntarily provide that data.

Deemed consent by notification applies where the data subject has been notified of the purpose for which his/her personal data is to be collected, used or disclosed, and he/she has not taken any action to opt out of the collection, use or disclosure of the personal data.

Deemed consent by contractual necessity applies where a data subject provides his/her personal data to an organisation with a view to the data subject entering into a contract with that organisation or pursuant to the contract between the data subject and the organisation.

Collection, Use and Disclosure without Consent under the PDPA

The First and Second Schedules to the PDPA provide for detailed exceptions to obtaining a data subject's consent to collect, use or disclose his/her personal data. In brief, personal data may be collected, used or disclosed without consent in situations relating to:

(f) the vital interests of data subjects;
(g) public interests;
(h) legitimate interests;
(i) business asset transactions;
(j) business improvement purposes; and
(k) research.

Vital Interests of Data Subjects

Part 1 of the First Schedule to the PDPA provides that consent for the collection, use or disclosure of personal data is not necessary where:

(a) the collection, use or disclosure of personal data is clearly in the individual's interests (provided that consent cannot be obtained in a timely way and the individual would not reasonably be expected to withhold consent);
(b) the collection, use or disclosure of personal data is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual;
(c) the collection, use or disclosure of personal data is for the purpose of contacting the next-of-kin or a friend of any injured, ill or deceased individual; or
(d) the consent for the collection, use or disclosure of personal data cannot be obtained in a timely manner and there are reasonable grounds to believe that the health or safety of the individual or another individual will be seriously affected.

Public Interests

Part 2 of the First and Second Schedule to the PDPA provide for exceptions to consent in relation to matters that affect the public or are in the public interest. This includes, but is not limited to, the collection, use

or disclosure of personal data that is publicly available, that is in the national interest, or by a news organisation solely for its news activity.

Some of these terms are defined in the PDPA. For example, "publicly available" is defined in section 2(1) of the PDPA and refers to personal data that is generally available to the public, including personal data which can be observed by reasonably expected means at a location or an event at which the individual appears and that is open to the public.

Legitimate Interests

Legitimate interests under the PDPA generally refer to any lawful interests of an organisation or other person.

Paragraphs 2 to 10 of Part 3 of the First Schedule to the PDPA prescribe specific purposes as "legitimate interests" and not require consent to collect, use or disclose personal data. Such purposes include evaluative purposes, the provision of legal services, managing or terminating the employment relationship with an individual and for the purposes of investigations or proceedings. (Some of these terms are defined in the PDPA.)

Aside from these specific purposes, Paragraph 1 of Part 3 of the First Schedule to the PDPA provides for a general exception that organisations may rely on for other "legitimate interests", even though they are not specifically prescribed. The organisation must, however, satisfy various conditions including conducting an assessment on relying on the legitimate interest exception and disclosing its reliance on the exception to the data subject.

Business Asset Transactions

Under Part 4 of the First Schedule to the PDPA, consent need not be obtained to collect, use or disclose personal data in respect of the following business transactions (subject to various conditions being met):

(a) business asset transactions involving the purchase, sale, lease merger or amalgamation or any other acquisition, disposal or financing of an organisation or part of the organisation/interest in an organisation/any business asset;
(b) business asset transactions involving the amalgamation of a corporation with one or more related corporations; and
(c) business asset transactions involving the transfer or disposal of any of the business assets of a corporation to a related corporation.

Business Improvement Purposes

Subject to fulfilling certain conditions, Part 5 of the First Schedule to the PDPA and Division 2 of Part 2 of the Second Schedule to the PDPA enable organisations to use, without consent, personal data that they had collected in compliance with the PDPA, where the use of the personal data falls within the scope of any of the following business improvement purposes:

(a) improving, enhancing or developing new goods or services;
(b) improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services;
(c) learning or understanding behaviour and preferences of individuals; or
(d) identifying goods or services that may be suitable for individuals or personalising or customising any such goods or services for individuals.

This exception also allows organisations to share personal data between entities belonging to a group of companies for business improvement purposes.

Research

Division 3 of the Second Schedule to the PDPA provides that organisations may, without consent, use and disclose personal data about an individual for a research purpose, including historical and statistical research, provided that the relevant requirements under the PDPA are met.

12. Does the PDPA impose other requirements for the collection and processing of personal data?

In addition to meeting the requirements of section 13 (summarised above), organisations may only collect, use or disclose personal data about a data subject for purposes that (a) a reasonable person would consider appropriate in the circumstances and (b) that the data subject has been informed of under section 20 of the PDPA (if applicable) (section 18 of the PDPA).

Section 20 of the PDPA requires organisations to inform data subjects of the purpose for the collection, use or disclosure of personal data on or before collecting the personal data. The PDPA does not prescribe the manner or form in which notice must be given to data subjects. However, the PDPC has provided guidance that it is good practice for the organisation to state its purposes in a written form.

13. Does the law impose separate or additional requirements in relation to specific categories of personal data (e.g. sensitive personal data)?

The PDPA does not expressly impose additional requirements for specific categories of personal data, neither does it define "sensitive personal data". However, as a number of data protection provisions in the PDPA adopt a standard of reasonableness, the sensitivity of personal data could affect the measures that an organisation must put in place to comply with the PDPA.

Organisations may also only collect, use or disclose personal data about a data subject for purposes that (a) a reasonable person would consider appropriate in the circumstances and (b) that the data subject has been

informed of under section 20 of the PDPA (if applicable) (section 18 of the PDPA).

For instance, section 24 of the PDPA requires organisations to implement "reasonable security arrangements" to protect personal data in its possession or under its control (the "**Protection Obligation**"). The PDPC has stated that organisations should consider the sensitivity and volume of personal data when deciding the appropriate level of security measures needed to comply with Protection Obligation.

Additionally, the PDPC has also provided guidance regarding National Registration Identity Card numbers and other national identification numbers. In this regard, the PDPC has noted that organisations are generally not allowed to collect, use or disclose such numbers unless it is required under the law (or an exception under the PDPA applies), or is necessary to accurately establish or verify the identity of the data subject to a high degree of fidelity.

Obligations Relating to Care of Personal Data (Data Governance)

14. What obligations does the PDPA impose in relation to the care of personal data?

Accuracy Obligation

Section 23 of the PDPA requires an organisation to make reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data is likely to be used by the organisation to make a decision that affects the individual or is likely to be disclosed by the organisation to another organisation. It does not matter whether the personal data was collected by the organisation itself or on its behalf (the "**Accuracy Obligation**").

Retention Limitation Obligation

Section 25 of the PDPA requires an organisation to cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data, and retention is no longer necessary for legal or business purposes (the "**Retention Limitation Obligation**").

Data Subject Rights

15. What rights do data subjects have under the PDPA?

Right of Access and Correction

Sections 21 and 22 of the PDPA provide for the rights of data subjects to request for access to their personal data and for correction of their

personal data that is in the possession or under the control of an organisation.

Data subjects also have the implicit right to request for the PDPC to review a failure or refusal by an organisation to provide access or make a correction to their personal data (pursuant to the data subjects' rights of access and correction), or a fee imposed by an organisation to respond to an access request (section 48H of the PDPA).

Right to Withdraw Consent

Pursuant to section 16 of the PDPA, data subjects may withdraw consent to the collection, use or disclosure of their personal data at any time with reasonable notice. This does not affect the consequences of such withdrawal. Organisations that receive a withdrawal of consent must cease to collect, use or disclose personal data (as the case may be) unless continued collection, use or disclosure of personal data without the data subject's consent is required or permitted by any written law.

Right of Private Action

Under section 48O of the PDPA, a person who suffers loss or damage directly as a result of a contravention by an organisation or person of specific provisions in the PDPA has a right of action for relief in civil proceedings in a court. This right of private action is only exercisable when the decision by the PDPC has become final.

Right to Data Portability

At the request of a data subject, organisations must transmit the individual's data that is in its possession or under its control, to another organisation in a commonly used machine-readable format.

At the time of publishing of this guide, the provisions relating to this right have not yet come into force.

Remedy of Erasure

The PDPA does not provide an express right of erasure to data subjects. However, section 25 of the PDPA requires organisations to cease to retain their documents containing personal data as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data, and retention is no longer necessary for legal or business purposes.

C) SECURITY OBLIGATIONS AND DATA BREACH NOTIFICATION

Protection of Personal Data

16. What security obligations are imposed in relation to the processing of personal data?

Section 24 of the PDPA requires organisations to make reasonable security arrangements to protect personal data in their possession or under their control in order to prevent: (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored.

Obligations under the Cybersecurity Act

17. What are the security obligations under the Cybersecurity Act?

Under Section 14(2) of the Cybersecurity Act, the owner of a CII must establish mechanisms and processes for the purposes of detecting cybersecurity threats and incidents in respect of the CII, as set out in any applicable code of practice. (Once the CS Amendment Bill is brought into force, major FDI service providers, ESCIs and STCC owners will similarly have to establish such mechanisms and processes.)

In this regard, under the present Cybersecurity Code of Practice for Critical Information Infrastructure ("**CII Cybersecurity Code**"), owners of CII are required to put in place security baseline configuration standards for all operating systems, applications and network devices of a piece of CII that is commensurate with the cybersecurity risk profile of that CII. The following security principles must be met by the security baseline configuration standards:

- least access privilege and separation of duties;
- enforcement of password complexities and policies;
- removal of unused accounts;
- removal of unnecessary services and applications (e.g. removal of compilers and vendor support applications);
- closure of unused network ports;
- protection against malware; and
- timely update of software and security patches that are approved by system vendors.

Notification of Security Incidents and Data Breaches

18. Are there notification requirements to notify regulatory authorities and affected data subjects of a data breach? What are the timelines for such notification?

Assessing Data Breaches

"Data breach" is defined in the PDPA as follows:

- the unauthorised access, collection, use, disclosure, copying, modification, or disposal of personal data; or
- the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification, or disposal of the personal data is likely to occur.

Where an organisation has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, the organisation must conduct, in a reasonable and expeditious manner (and generally, within 30 calendar days), an assessment of whether the data breach is a notifiable data breach.

A data breach is a notifiable data breach if the data breach (a) results in, or is likely to result in, significant harm to an affected individual; or (b) is, or is likely to be, of a significant scale (affecting at least 500 individuals).

Under the Personal Data Protection (Notification of Data Breaches) Regulations 2021 ("**Data Breach Regulations**"), a data breach is deemed to result in significant harm to an individual if the data breach relates to:

- the individual's full name or alias or identification number, and any of the personal data or classes of personal data relating to the individual set out in the Schedule to the Data Breach Regulations; or
- all of the following personal data relating to an individual's account with an organisation:
    - the individual's account identifier, such as an account name or number;
    - any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account.

Notifying the PDPC

Where an organisation assesses that a data breach is a notifiable data breach, the organisation must notify the PDPC as soon as is practicable, but in any case, no later than 3 calendar days after the day the organisation makes that assessment.

Notifying affected individuals

The organisation must also notify each affected individual affected by a notifiable data breach on or after notifying the PDPC in a reasonable manner unless:

- on or after assessing that the data breach is a notifiable data breach, the organisation takes any action in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or
- the organisation had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual.

Notifying the Data Controller

Where a data intermediary has reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation, the data intermediary must, without undue delay, notify that other organisation (i.e. the data controller) of the occurrence of the data breach.

Thereafter, that other organisation must assess if the data breach is a notifiable one.

19. Are there notification requirements in relation to other cybersecurity events? What are the timelines for such notification?

There are currently four types of cybersecurity incidents that CII owners must report to the Commissioner under the Cybersecurity (Critical Information Infrastructure) Regulations 2018 ("**CII Regulations**"). The cybersecurity incidents are:

(a) any unauthorised hacking of the critical information infrastructure or the interconnected computer or computer system to gain unauthorised access to or control of the CII or interconnected computer or computer system;

(b) any installation or execution of unauthorised software, or computer code, of a malicious nature on the CII or the interconnected computer or computer system;

(c) any man-in-the-middle attack, session hijack or other unauthorised interception by means of a computer or computer system of communication between the CII or the interconnected computer or computer system, and an authorised user of the CII or the interconnected computer or computer system, as the case may be; and

(d) any denial-of-service attack or other unauthorised act or acts carried out through a computer or computer system that adversely affects the availability or operability of the CII or the interconnected computer or computer system.

Additionally, CII owners must notify the Commissioner of any other type of cybersecurity incident in respect of the CII that the Commissioner has specified by written direction to the CII owner.

Pursuant to regulation 5 of the CII Regulations, CII owners must submit an initial report of the cybersecurity incident to the Commissioner within 2 hours after becoming aware of the occurrence of the incident and provide supplementary details within 14 days after the submission of the initial report.

The CS Amendment Bill will expand the cybersecurity events to be reported by CII owners to include:

(d) prescribed cybersecurity incidents in respect of any computer or computer system under the owner's control, even where it is not interconnected with or does not communicate with the CII; and

(e) prescribed cybersecurity incidents in respect of any computers or computer systems under the control of a supplier to the owner that is interconnected with or communicates with the provider-owned CII.

Further, there will be reporting obligations imposed on designated providers responsible for third-party-owned CII, as well as owners of STCCs, ESCIs, and major FDI service providers.

At the time of writing, the specific cybersecurity incidents, which are reportable for these new categories, have yet to be prescribed.

D) OUTSOURCING AND CROSS-BORDER TRANSFERS

International Data Transfers

20. Does the PDPA impose requirements in relation to the transfer of data to other jurisdictions? What are the ways in which these requirements may be met?

Organisations transferring data overseas will need to comply with section 26 of the PDPA, i.e. organisations need to ensure that the personal data transferred overseas is accorded a standard of protection that is comparable to the protection under the PDPA.

Under the Personal Data Protection Regulations ("**PDP Regulations**"), the transferring organisation must take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA.

"Legally enforceable obligations" include the following obligations which are imposed on the recipient under:

(a) Any law;
(b) Any contract requiring the recipient to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the PDPA and specify the countries and territories to which the personal data may be transferred under the contract;
(c) Any binding corporate rules that require every recipient of the transferred personal data that is related to the transferring organisation to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the PDPA; and which specifies:
    - the recipients of the transferred personal data to which the binding corporate rules apply;
    - the countries and territories to which the personal data may be transferred under the binding corporate rules; and
    - the rights and obligations provided by the binding corporate rules;
(d) Any other legally binding instrument, including the Asia-Pacific Economic Cooperation Privacy Recognition for Processors System or the Asia-Pacific Economic Cooperation Cross Border Privacy Rules System, which are recognised under the PDP Regulations as one of the modes of transferring data overseas.

Where the transferring party relies on imposing contractual obligations on the recipient to transfer personal data outside Singapore, the transferring party must also specify the countries and territories to which the personal data may be transferred under the contract.

A transferring party is taken to have satisfied the requirement to take appropriate steps to ensure that the recipient is bound by legally

enforceable obligations to provide to the personal data transferred a standard of protection that is comparable to that under the PDPA if:

(a) the data subject whose personal data is to be transferred gives his/her consent to the transfer of his/her personal data, after being provided with a reasonable summary in writing of the extent to which the personal data transferred to those countries and territories will be protected to a standard comparable to the protection under the PDPA; or
(b) the transfer is necessary for the performance of a contract between the organisation and the data subject, or to do anything at the data subject's request with a view to his/her entering a contract with the organisation.

As good practice, however, organisations are encouraged to rely on these circumstances only if they are unable to rely on legally enforceable obligations or specified certifications.

Appointment of Data Processors and Third-Party Vendors

21. What are the requirements and relevant obligations in relation to appointing a data processor to process personal data on behalf of the data controller?

Section 2 of the PDPA defines "*an organisation that processes personal data on behalf of another organisation but does not include an employee of that other organisation*" as a data intermediary (i.e. a data processor).

The PDPA provides that a data intermediary is only subject to the data protection provisions relating to:

(e) the Protection Obligation;
(f) the Retention Limitation Obligation; and
(g) the obligation to notify the data controller of a data breach (see Question 18).

However, a data intermediary remains responsible for complying with all of the obligations under the PDPA in respect of other activities which do not constitute processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing.

With regard to the financial sector, organisations must also comply with the MAS Guidelines on Outsourcing.

22. What obligations does the Cybersecurity Act impose on parties in relation to outsourcing arrangements?

Under the Cybersecurity Code of Practice, the CII owner remains responsible and accountable for the cybersecurity of the CII even if it engages an external party to perform or assist in performing any functions, activities or operations in respect of the CII. The CII owner shall establish processes to maintain oversight over all outsourced functions,

activities or operations, in order to minimise cybersecurity exposure arising from such outsourcing.

The Cybersecurity Code of Practices requires CII owners to include terms in their agreements with the external party to help ensure the cybersecurity of the CII and to reduce or mitigate the impact of any cybersecurity risks associated with the outsourcing. This shall include terms stipulating:

- The type(s) of access that the external party has to the CII, taking into account the CII owner's business requirements and the cybersecurity risk profile of the CII;
- The obligations of the external party to protect the CII against cybersecurity threats and report cybersecurity incidents; and
- The rights of the CII owner to commission an audit of the external party's cybersecurity posture in relation to the outsourced functions, activities or operations; or to require that the external party provide a copy of the audit report should the external party commission its own audit for these purposes.

Furthermore, the CII owner must establish processes for validating the external party's compliance with the terms in the agreement mentioned above and any other terms in the agreement relating to cybersecurity.

The CII owner must also ensure that it is able to renegotiate the terms of its agreements with external parties in the event of new legal or regulatory requirements.

Under the CS Amendment Bill, designated providers responsible for third-party-owned CII will also have to obtain legally binding commitments from such third party to ensure adherence to prescribed standards relating to cybersecurity.

E) ACCOUNTABILITY AND OTHER COMPLIANCE OBLIGATIONS

Data Protection Law - Appointment of Data Protection Officer and Accountability Requirements

23. Is there a requirement to appoint a data protection officer ("DPO")? If so, what is the scope of responsibilities of a DPO and are there any requirements in relation to the DPO's qualifications or experience?

Requirement to appoint a DPO

Section 11(3) of the PDPA requires an organisation to designate one or more individuals to be responsible for ensuring that the organisation complies with the PDPA. This individual is typically referred to as a DPO. Section 11(4) further provides that an individual so designated by an organisation may delegate the responsibility conferred by that designation to another individual.

Scope of Responsibilities of a DPO

An organisation's DPO plays an essential role in how the organisation meets its obligations under the PDPA. The responsibilities of the DPO include:

- working with senior management and the organisation's business units to develop and implement appropriate data protection policies and practices;
- producing or guiding the production of a personal data inventory;
- conducting data protection impact assessments;
- monitoring and reporting data protection risks;
- providing internal training on data protection compliance;
- engaging with stakeholders on data protection matters; and
- generally acting as the primary internal expert on data protection.

Depending on the organisation's needs, the DPO may also work the organisation's data governance and cybersecurity functions. The DPO can also play a role in supporting the organisation's innovation.

DPO's qualifications

While the PDPA does not prescribe the qualifications of a DPO, the PDPC has provided guidance that individual(s) designated by an organisation under section 11(3) should be:

- sufficiently skilled and knowledgeable;
- amply empowered to discharge their duties as a DPO; and
- trained and certified in qualifications such as the Practitioner Certificate for Personal Data Protection (Singapore).

Furthermore, the DPO should ideally be a member of the organisation's senior management team or have a direct reporting line to the senior management to ensure the effective development and implementation of the organisation's data protection policies and practices.

24. Are there other obligations under the PDPA in relation to its data handling processes or compliance with the PDPA?

Under section 12(a) of the PDPA, organisations are required to develop and implement data protection policies and practices. Organisations should develop policies and practices by taking into account matters such as the types and amount of personal data it collects, and the purposes for such collection.

Generally, sections 11 and 12 of the PDPA require organisations to demonstrate that they have taken measures to comply with the PDPA, and developing and implementing data protection policies is one way of demonstrating as such.

Record Keeping of Data Processing Activities

There is no express requirement to maintain records of data processing activities under the PDPA. However, organisations are highly encouraged to maintain such records as a way of demonstrating accountability. While failing to undertake such measures is not itself a breach of the PDPA, it could, in certain circumstances, result in the organisation failing to meet other obligations under the PDPA.

Data Protection Impact Assessments ("DPIAs")

Similarly, there is no express requirement to conduct a data protection impact assessment or similar risk assessment under the PDPA. However, for similar reasons as stated in the preceding paragraph, organisations are highly encouraged to conduct data protection impact assessments in appropriate circumstances, such as when a new system is being developed or implemented.

Cybersecurity Law – Accountability and Compliance Requirements

25. Does the Cybersecurity Act impose obligations in respect of demonstrating that compliance with the law is met?

Under section 15(1) of the Cybersecurity Act, CII owners are required to carry out an audit of the compliance of the CII with the Cybersecurity Act and the applicable codes of practice and standards of performance at least once every two years. The audit is to be carried out by an auditor approved or appointed by the Commissioner.

Additionally, section 15(1) of the Cybersecurity Act requires CII owners to conduct a cybersecurity risk assessment of the CII in the prescribed form and manner at least once a year.

Under the CS Amendment Bill, designated providers responsible for third-party-owned CII will have to obtain a legally binding commitment from such third-party to conduct similar audits and risk assessments as CII owners, among other things (section 14 of the Bill; new section 16J of the Cybersecurity Act).

26. What other key compliance obligations does the Cybersecurity Act impose?

Under Section 16 of the Cybersecurity Act, the Commissioner may conduct cybersecurity exercises for the purpose of testing the state of readiness of CII owners in responding to significant cybersecurity incidents. CII owners must participate in a cybersecurity exercise if directed in writing to do so by the Commissioner. Under the CS Amendment Bill, similar requirements are imposed on designated providers responsible for third-party-owned CII.

Additionally, if there is a change in the beneficial or legal ownership of a CII, the relevant person must inform the Commissioner of the change in

ownership not later than 7 days after the date of that change in ownership (section 13 of the Cybersecurity Act). A designated provider responsible for third-party-owned CII will similarly have to obtain a legally binding commitment from such third party to notify the provider of any change in the beneficial or legal ownership of the CII no later than 7 days (section 14 of the Bill; new section 16H of the Cybersecurity Act).

CII owners, designated providers responsible for third-party-owned CII, owners of STCC, ESCIs and major FDI service providers may also be required to furnish, to the Commissioner, information related to the design, configuration and security of the relevant infrastructure/system or computer or computer system that is interconnected or communicates with such infrastructure/system, among other things.

CONTACTS

LIM Chong Kin

Managing Director, Corporate & Finance Co-head, Data Protection, Privacy & Cybersecurity Co-head, Drew Data Protection & Cybersecurity Academy, Drew & Napier LLC

E:Chongkin.Lim@drewnapier.com

David N. ALFRED

Director and Co-head, Data Protection, Privacy & Cybersecurity Co-head and Programme Director, Drew Data Protection & Cybersecurity Academy, Drew & Napier LLC

E:David.Alfred@drewnapier.com

Anastasia CHEN

Director, Corporate & Finance and Data Protection, Privacy & Cybersecurity, Drew & Napier LLC

E:Anastasia.Chen@drewnapier.com

THAILAND

9. THAILAND

A) OVERVIEW

Legal Framework

1. What are the main laws governing data protection and cybersecurity in Thailand?

The main legislation governing data protection in Thailand is the Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**").

Additionally, there are other sector-specific legislations that contain data protection requirements such as the National Health Act B.E. 2550 (2007) and the Mental Health Act B.E. 2551 (2008) which aim to protect the health-related data of a person; the Notification of the National Broadcasting and Telecommunications Commission Re: Measures to Protect Telecommunications Service Users' Rights Regarding Personal Data, Privacy Rights, and Freedom of Telecommunications which was issued by virtue of the Telecommunications Business Act B.E. 2544 (2001) in 2023 to enhance the protection of telecommunication users' personal data, privacy rights and freedoms; the Credit Business Information Business Act B.E. 2545 (2002) which regulates its members, including the financial institutions, whereby the legislation imposes certain obligations on the use and disclosure of its members' customers' credit data which may also include personal data.

Cybersecurity in Thailand is mainly regulated by the Cybersecurity Act B.E. 2562 (2019) ("**Cybersecurity Act**"). The Cybersecurity Act defines the Critical Information Infrastructure Organisation ("**CII Organisation**") as a state agency or private organisation which has missions or provides critical information infrastructure service in relation to the national security, material public service, banking and finance, information technology and telecommunications, transportation and logistics, energy and public utilities, public health and others as may be prescribed by the National Cyber Security Committee ("**NCSC"**). However, not all such organisations will automatically be deemed as CII Organisations. To determine which of the organisations would be considered as CII organisation, the CII Organisation, the NSCS, along with the competent regulator, are to conduct an assessment based on several criteria such as whether the occurrence of a cyber threat within the organisation could significantly damage the nation's image, severely affect international relations, or disrupt social order or cause harm to individuals' health, safety, and property, disrupt people's livelihoods, or affect the country's economic stability, etc.

According to the Cybersecurity Act, the CII Organisations must protect, manage, and reduce cyber risks by complying with the guidelines of the NCSC and adhering to the duties prescribed in the Cybersecurity Act (e.g. defining the security category for data or information systems and applying the minimum security standard accordingly, reporting of cyber threats, etc.).

Data Protection Law – Scope of Application

2. What is the intended objective or main scope of the PDPA?

Many cases of violations of the right of privacy in relation to personal data that have caused disturbance or damages to data subjects, together with the development of technologies that has increased the ease, convenience and swiftness of the collection, use, and disclosure ("**Processing**" or "**Process**") of personal data in a manner violating such right, have caused damage to the economy overall. The PDPA was therefore enacted to prescribe rules, mechanisms and/or measures regulating personal data protection as a matter of general principles aiming to strengthen and unify personal data protection to align with the global privacy standard and to protect the rights of individuals by imposing obligations on a person or legal entity who Processes personal data of individuals. To achieve its objective in protecting the rights of the data subject (i.e. a living individual who can be identified by personal data, whether directly or indirectly) in relation to his/her personal data and therefore, the PDPA imposes obligations on two key players which are (i) the "**Data Controller**", i.e. a person or legal entity who/which having power to make determination on the Processing of personal data; and (ii) the "**Data Processor**", i.e. a person or legal entity who/which Processes personal data on behalf, or pursuant to the instructions, of the Data Controller.

3. What is the scope of personal data protected under the PDPA?

According to the PDPA, the term "personal data" is defined broadly as any data pertaining to an individual which enables identification of said individual whether directly or indirectly, but excluding data of the deceased person specifically. Therefore, any data that enables the identification of a data subject, whether directly (e.g. full name, email address, etc.) or indirectly (e.g. date of birth, telephone number, workplace and job title, etc.) would fall within the scope of the PDPA which means that the Processing of such data must be carried out in compliance with the PDPA.

The PDPA does not define nor refer to the term "sensitive personal data". However, section 26 of the PDPA provides a list of personal data that are subject to different requirements in terms of legal bases for the Processing and which could result in more severe harm and penalties in case of breach. This list of personal data is substantially similar to the list of the special categories of personal data under the GDPR, i.e. personal data pertaining to ethnicity, race, political opinions, doctrinal, religious or philosophical beliefs, sexual behaviour, criminal records, health records, disability, labour union, genetic data, biometric data, or any other data which may affect the Data Subject in the same manner as prescribed by the Personal Data Protection Committee ("**PDPC**").

4. Who must comply with the PDPA?

The PDPA applies to the Data Controller and Data Processor who/which are in Thailand, regardless of where the Processing activity takes place. The PDPA does have extraterritorial effect which means that its provisions are also enforceable against Data Controller and Data Processor who/which are located outside of Thailand whose Processing activity falls within any of the following scope ("**Extraterritorial Scope**"):

(a) offering of goods or services to the ***data subject in Thailand***, regardless of whether payment is made by the data subject or not; or

(b) monitoring of the behaviour of the data subject ***which takes place in Thailand***.

Cybersecurity Law – Scope of Application

5. What is the intended objective or main scope of the Cybersecurity Act?

The Cybersecurity Act was enacted due to the reasons that nowadays the provision of services or application of the computer network, internet, telecommunication networks or general satellite services are currently under the risk of cyber threat which could then threaten national security and public order of Thailand. Therefore, the Cybersecurity Act was enacted to simultaneously prevent or cope with such cyber threats whereby it determines the characteristics of mission or services that are regarded as fundamental as critical information infrastructure ("**CII**") for both public and private sectors for which there are necessities for such CII to be prevented, coped with and mitigated from the risk of cyber threat, as well as determine the competent authorities responsible to proceed with the relevant task, coordinate between public and private sectors, and establish operational plans and standards to maintain cybersecurity in a united and continuous manner.

The Cybersecurity Act defines "cyber threat" as any unlawful act or operation that is performed through the use of a computer or a computer system or an undesirable program with an intention to cause an act of violence against a computer system, computer data or other relevant data and which is an imminent danger causing damage to or affecting the functionality of a computer, a computer system or other relevant data.

6. Who must comply with the Cybersecurity Act?

The CII Organisation must comply with the Cybersecurity Act. Please refer to responses to Question 1 for more details.

Data Protection Authority, Enforcement and Appeals

7. Which are the key authorities that administer and enforce the PDPA? What powers do the key authorities have under the PDPA?

The PDPC is the authority responsible for the administration and enforcement of the PDPA, including to issue notifications or rules for the execution of the PDPA and perform any other acts as prescribed by the PDPA such as to designate the Expert Committee which will be responsible for considering and handling complaints in relation to the personal data, and making determination on the imposition of administrative penalties. The Expert Committee also has the power to request any person to make a statement of fact.

Furthermore, the competent official under the PDPA shall have the following duties and powers:

(1) to request the Data Controller, the Data Processor, or any person, in writing, to provide information or submit any documents or evidence in connection with the actions or offences under the PDPA; and

(2) to investigate and gather facts, and report to the Expert Committee, in the event that the Data Controller, the Data Processor, or any person, has committed an offence or caused damage due to their violation of or non-compliance with the PDPA or notifications issued in accordance with the PDPA.

Non-compliance with or violation of the PDPA could result in the following penalties and/or liabilities:

(1) **Civil Liability**: Where the non-compliance with or violation causes damage to the data subject, the Data Controller or the Data Processor shall compensate the injured data subject with the actual damages. In certain cases, the court may also order that punitive damages of not exceeding twice the amount of actual damages be compensated.

(2) **Administrative Penalties**: The administrative fine ranges from not exceeding THB 1 million to not exceeding THB 5 million, depending on the offence committed. As described above, the Expert Committee is empowered to make a decision on the imposition of administrative penalties. In the event that the Expert Committee considers the offence to be a non-severe offence, the Expert Committee may impose other administrative measures rather than an administrative fine (e.g. issuance of warning, order to rectify the act, order to suspend the Processing, etc.). On the other hand, if the Expert Committee determines that the offence committed is a severe offence or where the offender fails to comply with certain orders of the Expert Committee, an administrative fine will then be imposed.

(3) **Criminal Penalty**: Use, disclosure or transfer of sensitive personal data in violation of the PDPA with specific intent (e.g. in a manner that is likely to cause another person to suffer any damage, impair his or her reputation, or expose such other person to be scorned, hated, or

humiliated, etc.), could be subject to criminal penalties of imprisonment for a term not exceeding 6 months to not exceeding 1 year and/or fine not exceeding THB 500,000 to not exceeding THB 1 million. Note that for the criminal penalties, if the offence is committed due to the act or omission of the legal entity's director, manager or person responsible for its operation, such director, manager or person responsible for its operation shall also be held liable for such offence.

8. **Is there an avenue for appeal against an enforcement decision made under the PDPA?**

The PDPA does not provide an avenue for appeal against an enforcement decision made under the PDPA. Nonetheless, a person is generally entitled to appeal against the administrative order pursuant to the Administrative Procedure Act B.E. 2539 (1966) and the Act on Establishment of Administrative Courts and Administrative Court Procedure B.E. 2542 (1999).

Cybersecurity Authority, Enforcement and Appeals

9. **Which are the key authorities that administer and enforce the Cybersecurity Act? What powers do the key authorities have under the Cybersecurity Act?**

The NCSC is the regulator responsible for enforcing the Cybersecurity Act and supervising cybersecurity matters – for example, to stipulate the minimum standard related to the computer, computer system; to delegate the control and supervision; to issue rules, objectives, duties, authorities and frameworks regarding the maintenance of the cybersecurity for the regulators or the CII Organisations, etc.

To carry out the duties and responsibilities of the NCSC, the Cybersecurity Act stipulates that the Cybersecurity Regulation Committee ("**CRC**") is to be designated to perform certain functions, including for the purpose of handling and mitigating damage from a serious cyber threat, the Cybersecurity Act empowers the CSSC to order, only to the extent necessary for the prevention of the cyber threat, owners, possessors, or users of computers or computer systems, or administrators of computer systems who are reasonably believed to be connected with the cyber threat or who are affected by the cyber threat, take certain actions such as to exercise surveillance of computers or computer systems in a particular period of time; to gain access to computer data or computer systems, or other data relating to the related computer systems, only to the extent necessary to prevent the cyber threat, etc.

In preventing, coping with, or mitigating the risks from critical level cyber threats, the CRC has the power to order a Competent Official, only to the extent that it is necessary to prevent the cyber threat, to carry out certain acts such as to enter a place to examine, if there is a cause to believe that there is a computer or computer system related to the cyber threat or is affected from the cyber threat; to access the computer data, computer system, or other data related to the computer system, copy, or

filter/screen information data or computer program which there is reason to believe is related to or affected by the cyber threat, etc.

10. Is there an avenue for appeal against a decision made under the Cybersecurity Act?

Yes. Under Section 69 of the Cybersecurity Act, the order may be appealed only if the case where the cyber threat is considered a non-serious cyber threat.

A non-serious cyber threat means a cyber threat posing a significant risk to the extent of causing a computer system of a CII Organisation or public services to become less efficient.

B) DATA PRIVACY AND DATA GOVERNANCE OBLIGATIONS

Obligations Relating to Collection, Use, Disclosure and/or Processing of Personal Data (Data Privacy)

11. What are the legal bases for processing personal data?

Consent is generally required for the Processing of personal data, unless the Processing falls under the exceptions to the consent requirement as follows:

(a) it is for the achievement of a purpose relating to the preparation of the historical documents or the archives for public interest, or for a purpose relating to research or statistics;

(b) it is for preventing or suppressing a danger to a person's life, body or health;

(c) 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;

(d) it is necessary for the performance of a task carried out in the public interest by the Data Controller;

(e) it is necessary for legitimate interests of the Data Controller or any other persons or legal entities; or

(f) it is necessary for compliance with a law to which the Controller is subjected.

Note that for consent to be considered as valid and binding upon the data subject, consent request must be made in accordance with the requirements under the PDPA – for example, the consent request must be clearly distinguished from other parts, use plain language, be in a form which is easily accessible and understandable, not be conditional upon the entering into a contract or provision of service which is not relevant or necessary, etc.

12. Does the PDPA impose other requirements for the collection and processing of personal data?

Processing of Personal Data for New Purpose

The PDPA generally prohibits the Processing of personal data for purposes which have not been notified to the data subject, except:

i. Where the Processing of personal data for new purpose requires consent, the data subject must be informed of the new purpose, and consent from the data subject must be obtained.

ii. Personal data can be Processed for a new purpose if such new purpose is permitted by applicable law or the PDPA.

Notification Requirement

The Data Controller must notify the data subject of the following information before or at the time of collection of his/her personal data ("**Notification Requirement**"):

(a) Purposes of the collection, use, and disclosure of the personal data;

(b) Circumstances where the data subject is required to give personal data in order to comply with the law, or a contract, or where there is a necessity to give personal data in order to conclude a contract, including possible consequences for not giving personal data under said circumstances;

(c) Types of personal data that will be collected;

(d) Retention period, or if a specific retention period cannot be set, the expected retention period according to the data retention standard;

(e) Types of persons/entities that the personal data will be disclosed to;

(f) Information and contact details of Data Controller and, where applicable, local representative and/or data protection officer; and

(g) The rights of the data subject under the PDPA.

13. Does the law impose separate or additional requirements in relation to specific categories of personal data (e.g. sensitive personal data)?

Yes. For sensitive personal data, explicit consent is generally required, unless the Processing falls within any of the following:

(a) it is to prevent or suppress a danger to life, body or health where the data subject is not capable of giving consent due to whatsoever reasons;

(b) it is carried out in the course of legitimate activities with appropriate safeguards by foundations, associations or any other not-for-profit bodies;

(c) it is information that is disclosed to the public with the explicit consent of the data subject;

(d) it is necessary for the establishment, compliance, exercise or defence of a legal claim;

(e) it is necessary for compliance with a law to achieve purpose with respect to: (a) preventive medicine or occupational medicine, the assessment of working capacity of the employee, medical diagnosis, the provision of health or social care, medical treatment, the management of health or social care systems and services; (b) public interest in public health (e.g. protecting against cross-border dangerous disease); (c) employment protection, social security, national health security, social health welfare of the entitled person; (d) it is for the scientific, historical, or statistic research purposes, or other public interests or (e) the substantial public interest, by providing suitable measures to protect the fundamental rights and interest of the data subject.

Obligations Relating to Care of Personal Data (Data Governance)

14. What obligations does the PDPA impose in relation to the care of personal data?

Accuracy Obligation

Section 35 of the PDPA requires the Data Controller to ensure that the personal data remains accurate, up-to-date, complete, and not misleading.

Purpose Limitation Obligation

Section 22 of the PDPA requires that the collection of personal data shall be limited to the extent of necessity for the lawful purpose of the Data Controller.

Retention Limitation Obligation

Section 37(3) of the PDPA imposes the obligation on the Data Controller to implement monitoring systems to delete or destroy Personal Data at the end of the retention period or at the time stipulated by the PDPA (e.g. when the personal data is no longer necessary or relevant for the purposes for which it has been collected, when the data subject exercises the right to withdraw consent, etc.).

Data Subject Rights

15. What rights do data subjects have under the PDPA?

Subject to the conditions and requirements under the PDPA, the data subjects are entitled to the following rights:

(a) **Right to Access** - The right to request to have access to personal data, and to request the disclosure of how personal data has been acquired by the Data Controller without consent.

(b) **Right to Data Portability** - The right to request to have personal data in the format which is generally readable and usable by automatic tools or devices and which can be disclosed and used by automatic means, and to request that personal data in said format be transmitted to another Data Controller.

(c) **Right to Object** - The right to object to the Processing of personal data in certain cases, for example, where the Data Controller processes personal data for the performance of a task carried out in the public interest, for direct marketing purposes, or it is necessary for the exercising of official authority vested in Data Controller.

(d) **Right to Suspend** - A data subject has the right to request that the use of personal data be suspended under certain circumstances such as where the personal data is no longer necessary for the purposes for which it has originally been collected; where a data subject requested to exercise the right to rectification, and Data Controller is in the process of examining such request, etc.

(e) **Right to Withdraw Consent -** A data subject has the right to withdraw consent at any time and the data subject must be able to withdraw consent as easily as when giving consent. If there is a consequence from withdrawing the consent, such consequence must also be notified to the data subject. The withdrawal of consent would not affect the lawfulness of the Processing of personal data which has been carried out by the Data Controller prior to such withdrawal.

(f) **Right to Erasure -** A data subject has the right to request the Data Controller to erase, destroy, or de-identify personal data in certain circumstances such as when the personal data is no longer necessary for the purposes for which it was Processed, when a data subject has withdrawn their consent for the Processing of personal data, and the Data Controller cannot rely on any legal bases other than consent; when a data subject has exercised their right to object to the Processing of his/her personal data for direct marketing purposes; when the Processing of personal data is not lawful, etc.

(g) **Right to Rectification** - A data subject has the right to request that his/her personal data be rectified so that it would be accurate, up-to-date, complete, and not be misleading.

(h) **Right to Lodge Complaint** - A data subject has the right to lodge a complaint to the Office of the PDPC if the data subject opines that the

Data Controller or Data Processor, including their employees and personnel, violates or fails to comply with the PDPA.

C) SECURITY OBLIGATIONS AND DATA BREACH NOTIFICATION

Protection of Personal Data

16. What security obligations are imposed in relation to the processing of personal data?

Under the PDPA, the Data Controller is required to implement appropriate security measures to protect personal data which must at least meet the minimum standard stipulated by the PDPC under the Notification re: the requirement of security measures for Data Controllers B.E. 2565 (2022) ("**Notification on Security Measure**"). Furthermore, the Data Controller must require its Data Processor to implement appropriate security measures as prescribed by the Notification on Security Measure.

The security measures must be periodically reviewed by the Data Controller when it is necessary, or when the technology has changed in order to efficiently maintain the appropriate security and safety.

Obligations under the Cybersecurity Act

17. What are the security obligations under the Cybersecurity Act?

As described in responses to Question 1, according to the Cybersecurity Act, the CII Organisations must protect, manage, and reduce cyber risks by complying with the guidelines of the NCSC and adhering to the duties – for example, to: (i) implement its own guideline pertaining to cybersecurity which must be in accordance with guidelines issued by the NCSC; (ii) inform the National Cyber Security Agency ("**NCSA**") of the name of its practitioner level and management level officers, including the name and contact information of owners, possessors, and monitoring persons of computer systems; (iii) to conduct cyber risk assessment by both internal investigators and external investigators, etc.

According to the Notification of the CSSC Re: Guidelines on Code of Practice and Standard Framework for Maintaining Cybersecurity for Government Agencies and CII Organisations, a code of practice and a framework standard for the cybersecurity maintenance prepared by CII Organisation must include the following:

(a) Cyber security audit plan;
(b) Assessment of cybersecurity risks;
(c) Cybersecurity incident response plan;
(d) Response measures when cyber threats are detected; and
(e) Cybersecurity resilience and recovery.

Notification of Security Incidents and Data Breaches

18. Are there notification requirements to notify regulatory authorities and affected data subjects of a data breach? What are the timelines for such notification?

Definition of Data Breach Incident – The Notification of the PDPC Re: Rules and Procedures for the Data Breach Notification ("**Data Breach Notification**") defines "data breach incident" as any breach of security that leads to loss, or unauthorised or unlawful access, use, change, alteration, or disclosure of Personal Data, whether such breach occurs intentionally, willfully, by negligence, without authorisation or unlawfully, computer crime, cyber threat, any mistake, accident, or any other reasons.

Data Breach Assessment – The Data Breach Notification stipulates that when the Data Controller has been notified of the data breach incident or become aware of the data breach incident or the suspected data breach incident, the Data Controller is to, among others, carry out the assessment to determine whether the information is reliable as well as the assessment of the risk of the data breach incident.

According to the Data Breach Notification, the below factors are to be taken into consideration when assessing the risk of the data breach incident:

(a) The nature and the type of data breach incident;

(b) The nature, type, and volume of personal data involved;

(c) The nature, type, and status of the affected data subject (e.g. minor, disability, incompetent or quasi-incompetent person, or vulnerable persons);

(d) The severity of the consequences of the data breach incident on the affected data subject, and the effectiveness of the measures taken to prevent the data breach incident;

(e) The impact of the data breach on the operation of the business or the public;

(f) The storage system of personal data involved and relevant security measures including organisational measures, technical measures, and physical measures; and

(g) The legal status of the Data Controller (i.e. individual or a corporate entity), including the scale and nature of its business.

Timeline to Notify the Office of the PDPC – Without delay and, as far as feasible, within 72 hours upon becoming aware of the data breach incident, unless the data breach incident does not have a risk of affecting the rights and freedom of individuals.

Timeline to Notify the Data Subject – Where the data breach incident has a high risk of affecting the rights and freedoms of individuals, the Data Controller must notify the Office of the PDPC as described above ***and*** must also notify the data subjects of such incident, together with the remedial actions, without delay.

Data Processor – The Data Processor must notify the Data Controller of the data breach incident without delay and, as far as feasible, within 72 hours upon becoming aware of such incident.

For Data Controllers, the notification to the Office of the PDPC and the data subjects must contain the contents stipulated by the Data Breach Notification.

19. Are there notification requirements in relation to other cybersecurity events? What are the timelines for such notification?

In the event that a cyber threat is expected to occur, the CII Organisation shall take action in inspecting its relevant data, computer data and computer systems to assess whether the cyber threat has actually occurred.

If the inspection reveals that the cyber threat has occurred or is expected to occur, the CII Organisation shall take action to prevent, handle and reduce cyber threat risks in accordance with the internal code of practice and framework standard for cybersecurity maintenance and promptly notify such cyber threat incident to the NCSA and its regulator. There are currently no further guidance or regulation on the types of information which must be notified.

D) OUTSOURCING AND CROSS-BORDER TRANSFERS

International Data Transfers

20. Does the PDPA impose requirements in relation to the transfer of data to other jurisdictions? What are the ways in which these requirements may be met?

With regard to the cross-border transfer of personal data, the PDPA generally permits the cross-border transfer of personal data by the data controller to a destination country or international organisation that has adequate personal data protection standards ("**Whitelisted Countries**") as prescribed by the PDPC. Currently, the PDPC has not yet announced the list of Whitelisted Countries. In determining which destination country and international organisation will be regarded as Whitelisted Countries, it must be taken into consideration as to whether the destination country or international organisation has legal measures or mechanisms regarding personal data protection that are consistent with the personal data protection laws of Thailand, particularly in relation to the obligations of the Data Controller to implement appropriate security measures and personal data protection measures which enables the enforceability of the data subject's rights, as well as the effective legal remedies.

Cross-border transfer of personal data is also permitted if personal data is transferred under any of the following circumstances:

(a) Where the law so prescribes;
(b) Where the consent of the data subject is obtained after the data subject has been informed about the insufficient personal data protection standards of the relevant destination country or international organisation;
(c) Where it is necessary to comply with the contract under which the data subject is a contracting party;
(d) Where it is an act that is compliant with the contract between the Data Controller and other persons, or legal entities, for the interests of the data subject;
(e) For vital interests; or
(f) For public interests.

In addition to the above, the PDPA also permits the cross-border transfer of personal data where personal data will be transferred within the same group of undertakings in order to jointly operate the business ("**Affiliated Entities**"), provided that a personal data protection policy for the cross-border transfer of personal data among Affiliated Entities ("**Binding Corporate Rules**") has been examined and certified by the Office of the PDPC. Or where there are no Whitelisted Countries or Binding Corporate Rules, cross-border transfer of personal data is permitted if appropriate safeguard is implemented pursuant to the notification of the PDPC – for example, adoption of the ASEAN Model Contractual Clauses for Cross Border Data Flows; the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries which are issued by virtue of the GDPR, subject to the conditions stipulated by the notification of the PDPC.

Legal grounds for the cross-border transfer of personal data and lawful bases for the Processing of personal data are two different things. In other words, having the lawful basis to Process personal data does not entitle the Data Controller to transfer personal data outside of Thailand as to transfer such data, one of the above-listed legal grounds must be satisfied. On the other hand, having the legal ground to transfer personal data outside of Thailand does not render the Data Controller to be able to conduct any other Processing activity as to do so, there must be a legal basis (e.g. consent, legitimate interest, contractual necessity, etc.).

The notifications of the PDPC on the cross-border transfer of personal data came into effect on March 23, 2024. With the notifications now fully enforceable, the Office of the PDPC has begun accepting Binding Corporate Rules for review. Data controllers and data processors intending to adopt Binding Corporate Rules as a means for transferring data to offshore affiliates or group companies must initiate the Binding Corporate Rules submission process promptly.

Appointment of Data Processors and Third-Party Vendors

21. What are the requirements and relevant obligations in relation to appointing a Data Processor to process personal data on behalf of the Data Controller?

Pursuant to the provisions of the PDPA, the Data Processor is obligated to perform the following duties and obligations:

(a) To undertake activities related to Processing of personal data pursuant to instructions or act on behalf of the Data Controller, unless such instruction violates laws or provisions of the PDPA;
(b) To implement appropriate security measures to prevent unauthorised or unlawful loss, access, use, alteration or disclosure of personal data;
(c) To promptly notify the Data Controller of data breach incidents within 72 hours upon having become aware of said breaches; and
(d) To prepare and maintain a record of processing activities in accordance with the criteria and procedures to be prescribed by the PDPC.

Note that the PDPA requires that there must be an agreement between the Data Controller and Data Processor to ensure that the Data Processor Processes personal data in accordance with its obligations under the PDPA. The PDPC may issue subordinate regulation on the provisions to be included in such agreement at a later stage which shall be closely observed.

22. What obligations does the Cybersecurity Act impose on parties in relation to outsourcing arrangements?

According to the Notification on Code of Practice, for the purpose of third-party management, the CII Organisation must include the cybersecurity requirements in its agreement with the third party to reduce the risks associated with access to the storage, communications, and any operations regarding critical information infrastructure.

Additionally, the following requirements shall be taken into consideration:

(a) Types of third-party permitted to access agency critical service assets of CII Organisation according to the business needs and cybersecurity risk profiles;

(b) Obligation to CII Organisation from cyber threats;

(c) Risks related to service and product supply chains; and

(d) Rights of CII Organisation to examine the cybersecurity of external service providers.

E) ACCOUNTABILITY AND OTHER COMPLIANCE OBLIGATIONS

Data Protection Law - Appointment of Data Protection Officer and Accountability Requirements

23. Is there a requirement to appoint a data protection officer ("DPO")? If so, what is the scope of responsibilities of a DPO and are there any requirements in relation to the DPO's qualifications or experience?

Requirement to Appoint a DPO

According to section 41 of the PDPA, it is mandatory for the Data Controller and Data Processor to appoint a Data Protection Officer ("**DPO**") if (i) the Data Controller or Data Processor is a state agency as prescribed by the PDPC; (ii) the activities of the Data Controller or Data Processor in relation to the Processing of the personal data require "*regular monitoring of the personal data or the system*" by reason of "*having large-scale personal data*" as prescribed by the PDPC; or (iii) the core activity of the Data Controller or Data Processor is the Processing of sensitive personal data.

The information and details of the DPO must be notified to the Office of the PDPC and the data subject. Note that the notification of the PDPC on the notification of the DPO has become effective since December 13, 2023.

Scope of Responsibilities of a DPO

The responsibilities and duties of the DPO are as follows:

(a) Give advice to the Data Controller/Data Processor, including the employees or contractors of the Data Controller/ Data Processor, with respect to compliance with the PDPA;

(b) Inspect the operation of the Data Controller/Data Processor, including the employees or the contractors of the Data Controller/ Data Processor with respect to the Processing of personal data, for the purpose of compliance with the PDPA;

(c) Coordinate and cooperate with the Office of the PDPC, in the case where any issue arises in respect to the Processing of the personal data in conjunction with the requirements stipulated under the PDPA; and

(d) Keep confidential the personal data which is known, or acquired, during the course of the performance of his duties.

DPO's Qualifications

According to the PDPA, qualifications of the DPO may later be prescribed – for example, that the DPO must pass the requisite tests, etc.

24. Are there other obligations under the PDPA in relation to its data handling processes or compliance with the PDPA?

Development of Policies and Processes

There is no specific provision that requires the organisation to develop and implement data protection policies and practices. To ensure compliance, organisations should establish internal policies and processes detailing the collection, use, disclosure, and safeguarding of personal data as per legal requirements. These policies and processes should cover various aspects of data protection.

Record of Processing Activities ("ROPA")

The Data Controller must prepare and maintain a ROPA, consisting of the required information, in writing or in an electronic form, and to have the ROPA available for examination by the data subject and the PDPC when requested. For the Data Controller which is classified as a small or medium-sized enterprise under the notification of the PDPC, it does not need to maintain the full ROPA, but is merely obligated to maintain the record of the rejection of the data subject's request to exercise certain rights under the PDPA such as the right to access.

The Data Processor is also obligated to maintain the ROPA, consisting of the required information, in writing or in an electronic form, and to have the ROPA available for examination by the Data Controller and the PDPC when requested.

Data Protection Impact Assessment ("DPIA")

The PDPA currently does not have any explicit provision that the DPIA be conducted.

Others

- For Data Controllers and Data Processors that are not located in Thailand but are subject to the Extraterritorial Scope of the PDPA, they must appoint a representative in Thailand, in writing, without any limitation to liability in relation to the Processing of personal data, except where the Processing does not Process sensitive personal data and engage in large-scale Processing of personal data.

- As there are certain subordinate regulations which have yet to be issued, and the PDPC becomes more active in enforcing the PDPA, it is advisable to closely observe any further developments on the PDPA to ensure that organisations will stay in compliance with the PDPA.

Cybersecurity Law – Accountability and Compliance Requirements

25. Does the Cybersecurity Act impose obligations in respect of demonstrating that compliance with the law is met?

The CII Organisation must conduct risks assessment involving cybersecurity maintenance and carry out an audit of the compliance of cyber at least once a year and prepare a summary report on the operations to the Office of NCSC within thirty days from the date of completion of an audit.

26. What other key compliance obligations does the Cybersecurity Act impose?

The CII Organisation is required to prepare a code of practice and a framework standard for cybersecurity maintenance in line with the policy and plan on cybersecurity which shall at least consist of the following matters:

(a) the plan for the inspection and assessment of risks involving cybersecurity maintenance by an assessor, an internal auditor, or a third-person independent auditor at least once a year; and

(b) the plan for the handling of cyber threats.

Please also refer to the responses to Question 17.

CONTACTS

Nopparat LALITKOMON

Partner, Head of Data Privacy and Cybersecurity
Tilleke & Gibbins

E:Nopparat.l@tilleke.com

Gvavalin MAHAKUNKITCHAREON

Senior Associate
Tilleke & Gibbins

E:Gvavalin@tilleke.com

Napassorn LERTUSSAVAVIVAT

Associate
Tilleke & Gibbins

E:Napassorn.l@tilleke.com

VIETNAM

10. VIETNAM

A) OVERVIEW

Legal Framework

1. What are the main laws governing data protection and cybersecurity in Vietnam?

The main law governing data protection in Vietnam is Decree No. 13/2023/ND-CP on Personal Data Protection ("**PDPD**"). The PDPD is the first comprehensive regulation on personal data protection. Prior to its adoption, privacy obligations were scattered in different laws and relied heavily on general laws like the civil code.

Additionally, there are other sector-specific legislation that contain data protection requirements. Several main laws include:

- Law on Network Information Security No. 86/2015/QH13 ("**LNIS**") which primarily focuses on information protection within network information systems;
- Law on Information Technology No. 67/2006/QH11, which stipulates the obligations of entities regarding the collection, processing, use, storage, and provision of personal data in a network environment;
- Law on Protection of Consumer Rights No. 19/2023/QH15 which includes provisions aimed at protecting the personal data of consumers; and
- Law on Electronic Transactions No. 20/2023/QH15 which forbids, among other things, the illegal collection, provision, use, disclosure, display, spreading, trade of data messages;
- Law on Credit Institutions No. 32/2024/QH15 which contains provisions mandating the confidentiality of information of credit institutions' clients;
- Law on Telecommunications No. 24/2023/QH15 which stipulates the protection of private information of telecommunications service users and private information transmitted through public telecommunications networks;
- Law on Medical Examination and Treatment No. 15/2023/QH15 which includes provisions for the protection of patients' information and the confidentiality of medical records;

Regulations regarding Cybersecurity in Vietnam are scattered throughout numerous legal instruments, including laws and guiding decrees/circulars. However, the main law primarily governing cybersecurity practices in Vietnam is the Law on Cybersecurity No. 24/2018/QH14 ("**Law on Cybersecurity**"). Another relevant law is the LNIS, which, in addition to addressing personal data protection as mentioned above, addresses information system security.

Data Protection Law – Scope of Application

2. What is the intended objective or main scope of the PDPD?

The PDPD entered into force on 1 July 2023 to regulate the processing and protection of personal data. It provides the definition of personal data and categories thereof, and the principles for the processing of personal data. The PDPD also recognises the rights of data subjects regarding their personal data and imposes personal data protection obligations to relevant agencies, organisations and individuals.

The PDPD creates obligations on the different data handlers, whose roles are defined as follows:

- data controllers are organisations that decide the purposes and means of the personal data processing
- data processors are organisations that process data on behalf of the controller under a contract or agreement with the controller, and
- third parties are any organisation other than the data controller, and the data processor that is permitted to process personal data.

3. What is the scope of personal data protected under the PDPD?

“Personal data” as defined by the PDPD refers to electronic information in the form of symbols, letters, numbers, images, sounds, or equivalences associated with an individual or used to identify an individual. Information that helps to identify a specific individual is further clarified as information generated from an individual’s activities that, when combined with other data and stored information, can identify a particular person.

The PDPD splits personal data into two different categories — basic personal data and sensitive personal data.

However, the PDPD does not provide a definition of basic personal data. Instead, it lists types of information considered as basic personal data, including name, date of birth, gender, nationality, personal photos, phone number, identification number, marriage status, history of one’s cyberspace activities, and so on. It further clarifies that any personal data not considered as sensitive personal data shall be considered as basic personal data.

Sensitive personal data, on the other hand, is defined as personal data in association with individual privacy which, when being infringed, will directly affect such individual's legal rights and interests. The PDPD also provides a list of sensitive personal data, which includes political and religious views, health status and personal information as recorded in medical records (excluding information about the blood type), racial or ethnic origin, genetic data related to an individual's inherited or acquired genetic characteristics, individual’s own biometric or biological characteristics, information about an individual’s sex life and sexual orientation, criminal records, customer information of credit institutions/foreign bank branches/payment intermediary service

providers, location data and other personal data requiring specific protection as prescribed by law.

4. Who must comply with the PDPD?

The PDPD has extraterritorial effect and applies to entities in all sectors that engage in the processing of personal data in Vietnam. This includes Vietnamese agencies, organisations and individuals; foreign authorities, entities and individuals in Vietnam; Vietnamese agencies, organisations and individuals that operate in foreign countries; and foreign agencies, organisations and individuals that directly process or are involved in processing personal data in Vietnam.

Cybersecurity Law – Scope of Application

5. What is the intended objective or main scope of the Law on Cybersecurity?

The intended objective of the Law on Cybersecurity is to protect national security and public order in cyberspace; and to clarify the responsibilities of relevant agencies, organisations and individuals.

6. Who must comply with the Law on Cybersecurity?

The application scope of the Law on Cybersecurity is very broad and covers almost all organisations and individuals engaging in activities in cyberspace. This also includes foreign entities active in the Vietnamese cyberspace (i.e. whose website or online application is made available to customers in Vietnam).

Data Protection Authority, Enforcement and Appeals

7. Which are the key authorities that administer and enforce the PDPD? What powers do the key authorities have under the PDPD?

The primary regulator having authority to develop, administer and enforce the PDPD is the Department of Cyber Security and Hi-Tech Crime Prevention ("**A05**") – under the Ministry of Public Security ("**MPS**").

The A05/MPS generally holds significant power in relation to data protection in Vietnam. Some of their notable duties and powers are as follows:

- Assist the Government in implementing the state management of personal data protection, which may include the implementation of personal data protection activities, the protection of data subjects' rights, and the development and operation of the National Information Portal on personal data protection.
- Receive impact assessment dossiers, forms, and information on personal data protection and assess the results of personal data protection activities of relevant agencies, organisations and individuals.

- Inspect, examine, resolve complaints and denunciations, and handle violations of the regulations on personal data protection.

Upon receiving notifications, complaints, denunciations, or when there is suspicion or discovery of individuals or organisations violating the law, A05/MPS is entitled to conduct an investigation and audits of businesses to ensure compliance with regulatory requirements. Relevant stakeholders have the obligation to cooperate with the regulator and to provide information to serve the investigation and to handle violations of the regulations on personal data protection.

There are currently no sanctions for PDPD violations. Up to this point in time, there has been no enforcement of the PDPD considering the lack of penalties or remedies. However, this will soon change as the authorities are developing a new decree on administrative sanctions for cybersecurity violations ("**Draft Sanction Decree**"). The last publicly available version of the Draft Sanction Decree included both (i) sanctions and (ii) remedial measures:

Potential Sanctions (currently, in a draft form):

For every violating act committed by organisations, the violator may be subject to a warning or fine. The administrative fine can be up to VND 1,000,000,000 (approx. USD 40,000) or, for serious violations (such as disclosing and misplacing personal data or cross-border transfer of 5 million data subjects who are Vietnamese citizens; or repetition of illegal data trading), up to 5% of the violating enterprise's turnover of the immediately preceding fiscal year in the Vietnamese market.

Depending on the nature and severity of the non-compliance, the violator can also be subject to one or more additional sanctions, which can include: withdrawal of the right to use business licenses for 1 - 24 months; suspension of personal data processing for 1 - 3 months; suspension of operations for a period from 1 - 24 months.

Potential Remedial measures (currently, in a draft form):

Violators can be subject to one or more remedial measures, which can include: forcible compliance; forcible destruction or unrecoverable deletion of personal data; forcible return of illegal profits obtained from the violations; public apology in mass media.

Please note that the above information regarding sanctions is provided for indicative purposes only. The Draft Sanction Decree is still at the drafting stage. Thus, the information hereunder could be impacted by future developments and alteration of the Draft Sanction Decree before its official enactment.

8. Is there an avenue for appeal against an enforcement decision made under the PDPD?

The PDPD does not provide regulations for the appeal or for filing complaints against enforcement decisions related to personal data protection. However, in principle, if an organisation or individual

disagrees with a decision or action taken by a state agency (for example, if they believe that an administrative penalty issued by A05 is incorrect), they have the right to file a complaint against that administrative action or decision as stipulated in the Law on Complaints No. 02/2011/QH13 of the National Assembly dated November 11, 2011 ("**Law on Complaints**"). A complaint against an enforcement decision made under the PDPD can be submitted to the A05/MPS. The initial resolution period should not exceed 30 days from the date of the complaint filing acceptance. In addition, businesses can initiate an administrative lawsuit in court against the administrative decision or act of MPS/A05 according to the provisions of the Administrative Procedure Law.

Cybersecurity Authority, Enforcement and Appeals

9. Which are the key authorities that administer and enforce the Law on Cybersecurity? What powers do the key authorities have under the Law on Cybersecurity?

A05/MPS is the regulatory authority responsible for the administration and enforcement of the Law on Cybersecurity.

Under the Law on Cybersecurity, the authorities hold broad powers toward the cybersecurity sector, notably including:

- Assist the Government in developing and proposing strategies, guidelines and policies; promulgate and guide the enforcement of legal documents on cybersecurity.
- Inspect, examine, resolve complaints and denunciations, and handle violations of regulations on cybersecurity; or coordinate with other authorities in handling violations in cases it is under the management scope of many agencies.
- Prevent and take actions against the use of cyberspace for activities that violate sovereignty, national interests or national security, as well as those that disrupt public order, and combat cybercrime.

Similar to the investigation powers under the PDPD, upon receiving notifications, complaints, denunciations, or when there is suspicion or discovery of individuals or organisations violating the Law on Cybersecurity, A05/MPS is also able to conduct inspection. The scope of investigation may vary on case-by-case basis, including but not limited to the collection of digital data; or entering into premises to conduct network security checks on information systems.

The authorities also have the power to impose data localisation requirements and to require the establishment of a branch or representative office in Vietnam for foreign violators engaged in the following fields: telecommunications services; storage and sharing of data in cyberspace; provision of national or international domain names for service users in Vietnam; e-commerce; online payment; payment intermediaries; services of connection and transportation in cyberspace; social media and social communication; online games; services of provision, management, or operation of other information in cyberspace in forms of messages, calls, video calls, emails, online chatting.

As the Draft Sanction Decree also covers the penalties for violations of the Law on Cybersecurity, please refer to our answers in Question 8 for further information.

10. Is there an avenue for appeal against a decision made under the Law on Cybersecurity?

The Law on Cybersecurity does not provide regulations for appeals or for filing complaints against enforcement decisions related to cybersecurity. In this regard, organisations or individuals can use the recourse provided under the Law on Complaints and the Administrative Procedure Law. Please refer to our answers to Question 8 for further information.

B) DATA PRIVACY AND DATA GOVERNANCE OBLIGATIONS

Obligations Relating to Collection, Use, Disclosure and/or Processing of Personal Data (Data Privacy)

11. What are the legal bases for processing personal data?

With the PDPD, Vietnam adopted a consent-centric approach to personal data protection (i.e. by default, consent is required for the processing of personal data). The exceptions to consent are limited to the following cases which shall be interpreted restrictively:

- In emergency situations where it is necessary to process relevant personal data to protect the life or health of the data subject or others;
- Where the disclosure of personal data is in accordance with the law;
- When the processing of data is done by competent state agencies in the event of a state of emergency on national defence, security, social order and safety, major disaster, or dangerous epidemic; or when there is a threat to security and national defence but not to the extent where it is necessary to declare a state of emergency; or to prevent and combat riots, terrorism, crimes and violations of the law;
- To fulfil the contractual obligations of the data subject with relevant agencies, organisations and individuals as prescribed by law; or
- To serve the activities of state agencies as prescribed by sector-specific laws.

To be clear, the definition of “personal data processing” under the PDPD is extensive and encompasses any activities that impact personal data, including, among others, collection, use, deletion, analysis, and disclosure of personal data.

Further, the PDPD imposes prescriptive requirements for the consent to be valid. Consent must be voluntarily made based on the data subject’s full understanding of (i) the type of personal data to be processed; (ii) the purposes of the personal data processing; (iii) the entities authorised to process personal data; and (iv) the data subject’s rights and obligations. Consent must be expressed in a clear and specific manner, either in writing, by voice, by ticking a consent box, by text message, by selecting

consent technical settings, or via another positive action that demonstrates the same. Consent must be made for each purpose, meaning that multiple purposes require multiple positive actions for the data subjects to be able to consent to one or more of them. Tacit consent is not recognised, and silence or non-response is not considered as consent. The data subjects may provide partial or conditional consent. Moreover, consent must be expressed in a format that can be printed out or reproduced in writing, including in electronic or verifiable formats.

12. Does the PDPD impose other requirements for the collection and processing of personal data?

The PDPD mandates that data subjects must be notified prior to the processing of their personal data. The notification must include the following information: (i) the purposes of the personal data processing; (ii) type of used personal data related to the purposes specified; (iii) method of processing personal data; (iv) details about other organisations and individuals related to the processing purposes; (v) undesirable consequences and damage that may occur; and (vi) starting and ending time. Additionally, like the consent, the notification also must be expressed in a format that can be printed out or reproduced in writing, including in electronic or verifiable formats. The prior notification is required in all cases, except in the following cases:

- The data subject knows and fully consents to the contents specified in the list of mandatory notification contents above before permitting the collection of their personal data in accordance with the PDPD;
- The personal data is processed by the competent state agency with a view to serving operations by such agency as prescribed by law.

Moreover, the PDPD sets out a list of principles which are further detailed under Question 14. A key point to note regarding limitation to processing is the explicit prohibition of the sale and purchase of personal data in any form, unless otherwise provided by law.

A key requirement under the PDPD is the obligation to establish a Personal Data Processing Impact Assessment Dossier ("**DPIA**"), using a statutory form. The DPIA shall be submitted to the A05 within 60 days from the processing, and shall be kept and remain available at all times to serve inspection and evaluation by the MPS. This obligation is imposed on data controllers and data processors alike, applying to any controller from the time it starts processing personal data and to any processor from the time it starts processing personal data under a contract with a controller.

For data controllers, the DPIA includes: (i) contact details of the data controller; (ii) name and contact details of the Data Protection Department ("**DPD**") and Data Protection Officer ("**DPO**"); (iii) processing purposes; (iv) types of data processed; (v) those who receive/ access the data; (vi) cases of cross-border transfer; (vii) duration of processing and estimated timing of deletion (if any); (viii) description of security measures; (ix) assessment of impact of the processing; undesirable consequences and damage that may occur, with measures to mitigate or eliminate them.

For data processors, the DPIA includes: (i) contact details of the data processor; (ii) name and contact details of the DPD and DPO; (iii) description of the processing and types of data processed; (iv) duration of processing; estimated timing for deletion (if any); (v) cases of cross-border data transfer; (vi) brief description of security measures; (vii) undesirable consequences and damage that may occur, with measures to mitigate or eliminate them.

13. Does the law impose separate or additional requirements in relation to specific categories of personal data (e.g. sensitive personal data)?

The protection measures applicable to the processing of sensitive personal data are more stringent than those for the processing of basic personal data, and will notably trigger: (i) the mandatory appointment of a DPO and of a DPD and (ii) the requirement for explicit information regarding the processing of sensitive personal data to be included in the notice and, when applicable, the consent form.

Obligations Relating to Care of Personal Data (Data Governance)

14. What obligations does the PDPD impose in relation to the care of personal data?

The PDPD outlines eight principles which shall guide personal data protection. Amongst these principles are included obligations relating to the care of personal data.

Accuracy Obligation
Personal data must be updated and supplemented to align with processing purposes, implying that all relevant entities involved in the processing are responsible for ensuring data accuracy. The PDPD also creates the obligation for data subjects to provide complete and accurate personal data when consenting to provide their personal data.

Data Minimisation Obligation
The collection of personal data must be limited to what is appropriate and relevant to the scope and purposes of the processing.

Purpose Limitation Obligation
Personal data must only be processed for the purposes that have been registered and declared by the data controller, the data processor, and the third party.

Retention Limitation Obligation
Personal data should be stored only for a period appropriate to the processing purposes, unless otherwise provided for by law.

Integrity, Confidentiality and Security Obligation
Personal data shall be protected and secured throughout the processing. This entails protection from violations of data protection regulations,

prevention of data loss, destruction or damage caused by incidents, and the implementation of appropriate technical measures.

Data Subject Rights

15. What rights do data subjects have under the PDPD?

The PDPD recognises 11 data subject's rights, including the right to be informed, the right to consent, the right to access, the right to withdraw consent, the right to delete data, the right to restrict data processing, the right to data provision, the right to object to data processing, the right to complain and denounce and/or initiate lawsuits, the right to claim compensation for damages, and the right to self-defence. Details are as follows:

Right to be informed

Data subjects have the right to be informed of the processing of their personal data, unless otherwise provided for by law.

Please refer to Question 12 for further information regarding the data subjects' notification requirements.

Right to consent

Data subjects have the right to give consent to the processing of their personal data, unless otherwise provided for by law.

Please refer to Question 11 for further information regarding the data subjects' consent requirements.

Right to access

Data subjects have the right to access their personal data to view, rectify or request rectification of the same, unless otherwise provided for by law.

If individuals cannot directly rectify their data due to technical or other reasons, they can request the data controller to do so. If rectification is not feasible, the data controller must inform the individual within 72 hours of receiving the request.

Right to withdraw consent

Data subjects have the right to withdraw their consent at any time, unless otherwise stipulated by law. Withdrawing consent does not affect the legality of prior processing based on that consent. Similarly to the format requirement for the consent to be valid, the consent withdrawal must also be expressed in a format that can be printed and reproduced in writing, including in electronic or verifiable format. The data controllers must inform the data subject about the potential consequences of withdrawal. Upon withdrawal, all processing must cease and the data controller must notify entities it shared the related data with to also cease their processing.

Right to delete personal data

Data subjects have the right to delete or request deletion of their personal data in the following circumstances:

- If the data subject no longer finds the data necessary for the originally consented purposes and accepts any consequences resulting from the deletion;
- If the data subject withdraws its consent;
- If the data subject objects to the processing and the data controller does not have any other valid grounds to continue the processing; or
- If the data is being processed for purposes other than those initially consented to, or if the processing violates regulations or laws;

Upon such requests, the deletion of all personal data collected by the data controller must be completed within 72 hours, unless otherwise provided for by law.

However, the data controller can reject the request in the following cases:

- When deletion is prohibited by law;
- When the data is processed by the competent state agencies to serve their activities as prescribed by law;
- When the data has been disclosed as prescribed by law;
- When processing is necessary for legal requirements, scientific research, or statistical purposes as per the law;
- In the event of a state of emergency on national defence, security, social order and safety, major disasters, or dangerous epidemics; when there is a threat to security and national defence but not to the extent where it is necessary to declare a state of emergency; or to prevent and combat riots, terrorism, crimes and violations of the law; or
- When responding to emergency cases that threaten the life and health or the safety of the data subject or others.

Right to restrict data processing

Data subjects have the right to restrict the processing of their personal data, unless otherwise provided for by law.

Upon receiving a request from a data subject, restrictions on processing must be implemented within 72 hours and shall apply to all personal data covered by the request, unless otherwise required by law.

Right to data provision

Data subjects have the right to request the data controller to provide them with a copy of their personal data, unless otherwise provided by law. The provision request must be submitted in Vietnamese using a statutory form. Upon receipt of a valid request for the provision of personal data, the data controller must notify of the time limit, location,

form of providing personal data; actual costs for printing, copying, photographing and sending information via postal and facsimile services (if any) and payment methods and terms to provide the personal data. The data controller must provide the personal data within 72 hours of the request, unless otherwise provided by law.

Right to object to processing

Data subjects have the right to object to the data controller's processing of their personal data to prevent or restrict (i) the disclosure of personal data or (ii) the use of personal data for advertising and marketing purposes, unless otherwise provided for by law. The data controller must comply with the data subject's request within 72 hours of receipt, unless otherwise provided for by law.

Right to complain, denounce and/or initiate lawsuits

Data subjects have the right to complain, denounce and/or initiate lawsuits as prescribed by law.

Right to claim damage

Data subjects have the right to claim damages as allowed by law in cases of personal data protection regulation violations, unless otherwise agreed by the parties or unless otherwise prescribed by law.

Right to self-defence

Data subjects have the right to self-defence according to regulations in the Civil Code, other relevant laws and the PDPD, or request competent agencies and organisations to implement civil right protection methods according to regulations of the Civil Code. This includes the right for the data subjects whose rights are violated to request, amongst other things, the termination of the violation, request a public apology, request the performance of civil obligations, request compensation for damages.

C) SECURITY OBLIGATIONS AND DATA BREACH NOTIFICATION

Protection of Personal Data

16. What security obligations are imposed in relation to the processing of personal data?

The PDPD prescribes general security obligations imposed in relation to the processing of personal data, including the obligation to implement appropriate management and technical measures (which shall be adopted from the beginning and throughout the processing), to adopt internal regulations on personal data protection; and to carry out cybersecurity inspections on systems, means, and equipment used for processing personal data both before the processing begins and before permanently deleting or destroying devices that contain personal data. These obligations are not further defined under the PDPD.

The LNIS also requires organisations processing personal information to develop and implement appropriate management and technical measures to protect the processed personal data, and comply with standards and technical regulations on ensuring network information security. Amongst applicable technical standards, organisations have the obligation to establish a plan to protect data integrity, use secured storage methods, and make backups through an independent storage system or media. In the event of a network information security incident, the organisations must take remedy and stoppage measures as soon as possible.

Obligations under the Law on Cybersecurity

17. What are the security obligations under the Law on Cybersecurity?

Under the Law on Cybersecurity, information system administrators are responsible for applying technical measures to prevent and stop cyber-attacks and acts related to cyber-attacks. In the case of an attack, they have the obligation to cooperate with the cybersecurity authorities in tracing the origin of the attack and collecting evidence thereof, to filter information serving the attack and provide such information and documents to the authorities.

Under the Law on Cybersecurity, service providers in cyberspace have the responsibility to warn their users about the risks related to using their services in cyberspace and to provide instructions on risk minimisation. They are also responsible for implementing different cybersecurity measures to ensure security during the information collection process and prevent the risk of data disclosure, leakage, damage or loss. They also have the obligation to develop plans for prompt response to cybersecurity incidents, leak or loss of data and prevent weaknesses, vulnerabilities, malicious codes, network infiltration and other security risks, and must cooperate with the authorities to protect cybersecurity.

The Law on Cybersecurity has a very broad application scope as discussed above and includes other security obligations relating to the monitoring of the information on cyberspace, to the regular review and inspection of the systems' cybersecurity, and to the general mandatory cooperation with the cybersecurity authorities.

Notification of Security Incidents and Data Breaches

18. Are there notification requirements to notify regulatory authorities and affected data subjects of a data breach? What are the timelines for such notification?

Yes.

In Vietnam, there are 3 main laws imposing notification obligations in case of data breach, namely (i) PDPD, (ii) Law on Cybersecurity, and (iii) LNIS. In addition, other sector-specific laws may also impose notification obligations.

PDPD

Under the PDPD, the requirement for the data controller to notify is not limited to data breaches, but is imposed for any violations of the PDPD. Under the PDPD, the data controller has the obligation to notify the A05/MPS within 72 hours of any violations of personal data protection regulations. Clearly put, this obligation does not only apply to data breaches but to all types of violations related to personal data protection. In case of delay or late notification, justification reasons must be provided. The notification must be completed in Vietnamese using a statutory form provided under the PDPD notably including the following mandatory contents:

- A description of the nature of the violation;
- Contact details of the employees, organisations, or individuals responsible for data protection;
- A description of potential consequences and damages;
- A description of measures taken to handle and mitigate the harm caused by the violation.

Meanwhile, the data processor only has the obligation to notify the data controller of any violations of the personal data protection regulations as soon as possible.

Please note that the PDPD does not require any notification to the affected data subjects.

LNIS

Under the LNIS, network information security incident is “a failure of information or an information system with consequential impacts on its confidentiality, integrity or availability”. If there are signs of a cyber-attack or network information security incident on a data system located in Vietnam, the administrator of the information system (i.e. owner of the data system that is located in Vietnam) has an obligation to notify the supervisory authorities of the incident within 5 days. The notification must be simultaneously sent to the National Coordinating Agency (Vietnam Computer Emergency Response Team, or "**VNCERT**"), the Specialised Incident Response Units (VNCERT, Vietnam Internet Network Information Center, or "**VNNIC**"), internet service providers, other relevant state agencies and members of the concerned incident response network. This notification must include the following information:

- Name and address of the reporting entity or individual;
- Name or domain name, IP address of the affected information system;
- Name and address of the entity or individual operating and the supervisory authority of the affected information system (if applicable);
- Description of the incident and the time it was detected;

- Proposed handling results, recommendations, and any other relevant information (if available).

Like the PDPD, the LNIS also does not require any notification to the affected data subjects.

In addition, LNIS also requires the organisations and individuals using online services (i.e. the users) to promptly notify the service provider or the Specialised Incident Response Units when detecting sabotage or network information incidents. No standard form or timeline has been provided for this type of notification by the users.

Law on Cybersecurity

Under the Law on Cybersecurity, a cybersecurity incident is defined as “an unexpected event in cyberspace (itself defined as a “network of IT infrastructure which includes Internet, communication systems and databases, amongst others”) that threatens national security, public order or the lawful rights and interests of an organisation or individual”. The obligation to notify is imposed on the service provider and is twofold:

(i) Notification to the regulator and the data subjects in the case of cybersecurity emergencies that cause serious effect to the impacted person

When a cybersecurity emergency is detected, organisations or individuals must immediately notify A05/MPS and affected entities/individuals of a data incident. "Cybersecurity emergencies" may include various situations and notably cover cases where the incident causes or is likely to cause “very serious damage” to the legitimate rights and interests of the affected individuals located in Vietnam or threatens human lives in the situation. This obligation applies regardless of the types of services provided or the location of the affected data system. The law does not specifically define what would constitute "very serious damage”. Thus, the current interpretation is based on clarification provided by the A05/MPS.

(ii) Notification to the regulator in the case of cybersecurity incidents, data breaches, leaks, damages, or loss of user information when providing services in cyberspace or of violations of the Law on Cybersecurity

Enterprises providing services in cyberspace are required to immediately notify the A05 of any cybersecurity incidents, data breaches, leaks, damages, or loss of user information.

The administrator of the information system also has the obligation to notify the A05/MPS when detecting violations of the Law on Cybersecurity.

The Law on Cybersecurity does not stipulate the content nor any formality for the notification to the A05.

19. Are there notification requirements in relation to other cybersecurity events? What are the timelines for such notification?

Yes. Other cybersecurity events could be included in the very broad definition of cybersecurity incident under the Law on Cybersecurity, which encompasses all events that occur in cyberspace that may compromise national security, public order, social safety, or the legitimate rights and interests of organisations, individuals, or agencies (Article 2.13, Law on Cybersecurity). Hence, the notification requirements under the Law on Cybersecurity analysed in Question 18 do not only cover data breaches, but also cybersecurity events in general. For example, denial-of-service (DoS) attacks, malware infection, Internet-of-Things (IoT) vulnerabilities can be considered as cybersecurity incidents when they could seriously damage the legitimate rights and interests of agencies, organisations and individuals. In such cases, the notification will be subject to the same requirements as described under Question 18 for the notification obligation pursuant to the Law on Cybersecurity.

D) OUTSOURCING AND CROSS-BORDER TRANSFERS

International Data Transfers

20. Does the PDPD impose requirements in relation to the transfer of data to other jurisdictions? What are the ways in which these requirements may be met?

The cross-border transfer of personal data is broadly defined and includes the act of processing personal data of Vietnamese citizens using servers and/or automated systems located outside of Vietnam. In any such cases of cross-border transfer of Vietnamese citizen's personal data, the transferor (which could be either the data controller or data processor) is subject to certain obligations as below.

Data Transfer Impact Assessment Dossier ("TIA")

The transferor shall prepare a TIA based on a statutory form, which includes: (i) contact information and details of the transferor and the transferee(s); (ii) full name and contact details of an organisation or individual under the transferor involved in transferring and receiving the data; (iii) description and explanation about the objectives of the personal data processing after the personal data is transferred abroad; (iv) description and clarification of the type of personal data to be transferred abroad; (v) description and explanation on the compliance of the regulations on personal data protection under the PDPD, and the detailed personal data protection measures; (vi) assessment on the impact of the personal data processing; undesirable consequences and damage that may occur, and measures for reducing or removing such consequences and damage; (vii) consent of the data subject according to the PDPD with information on the mechanism for feedback and complaint in case of arising problems or requests; and (viii) document that shows binding obligations and responsibilities between the transferor and the transferee(s) for the personal data processing.

The TIA shall be made available at all times for inspection and evaluation by the A05/MPS. In addition, the transferor shall submit an original copy of the TIA to the A05 within 60 days from the processing. The TIA Dossier is not a prerequisite condition for the cross-border transfer of personal data, but this requirement is rather triggered by the cross-border transfer itself. In addition, the TIA only serves as a notification to the authority of the personal data cross-border transfer activities for their post-inspection and shall not be considered as an approval. However, failure to comply with the TIA requirements could lead to the A05/MPS ordering the data transferor to stop transferring the data across the Vietnam border.

Contractual obligations

As per the requirements for the TIA, the transferor and the transferee must ensure that they agree on a clear attribution of obligations and responsibilities related to personal data protection. The authorities did not issue any standard contractual clause templates nor any further guidance as to what must be included in such an agreement for the transfer.

Notification of successful transfers to the A05

After the personal data of Vietnamese citizens is successfully transferred outside of Vietnam, the transferor shall also notify in writing to the A05 about the data transfer and contact details of the organisation or individual in charge of such transfer.

Appointment of Data Processors and Third-Party Vendors

21. What are the requirements and relevant obligations in relation to appointing a data processor to process personal data on behalf of the data controller?

On the one hand, the data controllers shall select appropriate data processors for specific tasks and mandates and shall only work with the data processors that have appropriate protection measures in place.

On the other hand, the data processors have the following responsibilities pursuant to the PDPD:

- Only receive personal data after having a contract or an agreement on data processing in place with the data controller;
- Process personal data in accordance with the contract or the agreement signed with the data controller;
- Fully implement measures to protect personal data as specified in the PDPD and other relevant legal documents;
- Be responsible to the data subject for damages caused by its personal data processing;

- Delete or return all personal data to the Controller after completing the personal data processing;

- Cooperate with the MPS and the state authorities in protecting personal data, providing information for investigation and handling of violations of the law on the protection of personal data.

There are also sectoral requirements imposed on outsourcing data processing, for example:

- **Banking and finance**: Circular No. 09/2020/TT-NHNN of the State Bank of Vietnam ("**SBV**") dated 21 October 2020 prescribing information system security in banking operations dedicates a section on the management of the use of third party's IT services (which may cover data processing), including: (i) general principles for the use of third party's IT services; (ii) requirements for the use of third party's IT services; (iii) criteria for selection of third-party providers of cloud computing services; (iv) service use agreement with the third party; and (iv) organisations' responsibilities in the use of third party's services. Especially, in the case of outsourcing to third parties the administration of certain information systems, including the ones processing customers' information, organisations shall carry out risk assessment and submit their risk assessment report to the SBV.

- **Healthcare**: Circular No. 53/2014/TT-BYT of the Ministry of Health dated 29 December 2014 prescribing the conditions for healthcare operations in cyberspace requires that, in the event of hiring external IT infrastructure, the engaged service provider shall be able to present its incident response procedures. Regarding external human resources, the engaged human resources shall satisfy the relevant professional requirements, and the agreement shall clearly stipulate that the use of healthcare information and/or data related to patients must ensure patients' right to privacy. In case the organisation hires external IT application services, an agreement must be entered into with the service provider with provisions on the commitment to the lawful processing of the information and the parties' contractual responsibilities in case any incidents arise.

22. What obligations does the Law on Cybersecurity impose on parties in relation to outsourcing arrangements?

There is no obligation under the Law on Cybersecurity on parties in relation to outsourcing arrangements.

E) ACCOUNTABILITY AND OTHER COMPLIANCE OBLIGATIONS

Data Protection Law - Appointment of Data Protection Officer and Accountability Requirements

23. Is there a requirement to appoint a data protection officer ("DPO")? If so, what is the scope of responsibilities of a DPO and are there any requirements in relation to the DPO's qualifications or experience?

As mentioned in Question 13, the requirement to appoint a DPO is triggered by the processing of sensitive personal data. In addition to the DPO, the PDPD requires that a DPD be also appointed for personal data protection-related tasks.

There is currently no official guidance regarding specific qualifications requirements for a person to be appointed as a DPO.

In addition, the appointment of the DPD and DPO must be made in the form of a written decision made by the company (i.e. a board resolution or a letter of appointment signed by the company's legal representative and affixed with the stamp of the company) and a copy of this written decision is required to be submitted alongside the DPIA and TIA.

24. Are there other obligations under the PDPD in relation to its data handling processes or compliance with the PDP?

The PDPD sets out the principle of accountability for the data controller for personal data processing, specifying that they shall be responsible for evidencing compliance with the regulations. The data controllers are also responsible for recording and storing logs of personal data processing. However, the PDPD does not clearly specify what constitutes log data of personal data processing activities, the method or the period to store it.

Specific obligations related to policies are addressed under Question 16.

As mentioned under Question 12, data controllers and data processors are required to prepare a DPIA. Such DPIA must be available at all times for inspection and evaluation by the A05/MPS. The same requirement applies to data transferors for the TIA.

Cybersecurity Law – Accountability and Compliance Requirements

25. Does the Law on Cybersecurity impose obligations in respect of demonstrating that compliance with the law is met?

There is no such requirement for demonstration of compliance under the Law on Cybersecurity.

26. What other key compliance obligations does the Law on Cybersecurity impose?

The Law on Cybersecurity imposes mandatory data localisation requirement. This requirement has been further regulated and detailed under Decree No. 53/2022/ND-CP of the Government dated 15 August 2022 elaborating some articles of the Law on Cybersecurity ("**Decree 53**"), where clarifications are provided on the different applications of this requirement on domestic enterprises (i.e. enterprises established pursuant to Vietnamese laws) and foreign enterprises (i.e. enterprises established under another jurisdiction).

Decree 53 specified that only some data is required to be stored in Vietnam, namely: (i) data on personal information of service users in Vietnam; (ii) data generated by service users in Vietnam (i.e. data on information reflecting the process of participating, operating, and using cyberspace of service users and information on devices and network services used for connection with cyberspace in the territory of the Socialist Republic of Vietnam, including: account name for use of services, duration of use of services, credit card information, email address, IP addresses for the latest login and logout, registered telephone number attached to the account or data relevant to the customer's personal data); and (iii) data on the relationships of customers in Vietnam (i.e. data on information reflecting and identifying relationships of service users with other people in cyberspace), including friends, and groups with which the customer connects or interacts (together the "**Regulated Data**").

For domestic companies

A domestic company would be subject to the requirement to store the Regulated Data in Vietnam if it meets the following two conditions:

- It provides services on telecom networks, on the internet or provides value-added services to the customer in Vietnam; and
- The provided services involve the activities of collecting, exploiting, analysing, and processing the Regulated Data.

For foreign companies

Foreign companies would have the obligation to locally store the Regulated Data and/or to establish a branch or representative office in Vietnam if the following four conditions are fully met:

- The company provides one of the following services: (i) telecom services; (ii) services of data storage and sharing in cyberspace; (iii) supply of national or international domain names to service users in Vietnam; (iv) e-commerce; (v) online payment; (vi) intermediary payment; (vii) service of transport connection via cyberspace; (viii) social networking and social media; (ix) online electronic games; (x) services of providing, managing, or operating other information in cyberspace in the form of messages, phone calls, video calls, email, or online chat.. ("**Regulated Services**");
- The service it provides has been used to commit a violation of the Law on Cybersecurity;

- The company has been warned that the services it provides have been used to violate Vietnamese laws and the company has not taken any measures to avoid, deal with, fight against or prevent such breach, or has not complied with a written request from the A05 for coordination in investigating and dealing with a breach of law or an act of neutralising or rendering ineffective the protective cybersecurity measures implemented by the cybersecurity regulator; and

- The company received an official notification demanding such company comply with the Data Localisation requirement in Vietnam and/or establish a branch or representative office.

Upon receiving the official notification in point 4 above, the company has 12 months from the date it received such notice to comply with the Data Localisation requirement.

The minimum period for the local storage is 24 months, which starts from the time the enterprise receives from the MPS a request for storing data and shall last until the request ends. The period for having a branch or representative office in Vietnam will start from the date on which the enterprise receives a request to set up such a branch or representative office and shall continue until the company no longer operates in Vietnam, or no longer provides the Regulated Services in Vietnam.

Moreover, no regulations impose any specific form of local data storage. Therefore, the regulated companies are free to choose the form of storage, and nothing appears to prohibit data mirroring across borders.

CONTACTS

Waewpen PIEMWICHAI

Counsel
Tilleke & Gibbins
E:Waewpen.p@tilleke.com

Mélynda MAHEUX

Associate
Tilleke & Gibbins
E:Melynda.m@tilleke.com

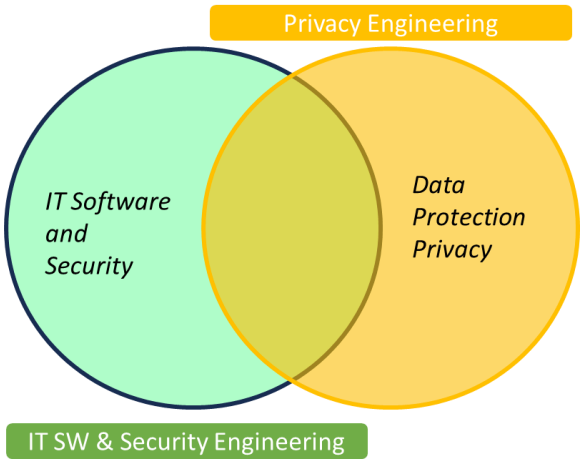
CYBERSECURITY AND PRIVACY ENGINEERING

11. CYBERSECURITY AND PRIVACY ENGINEERING

A) Challenges of Cyber Security and Privacy Engineering

A closer look at the various contributions in this Guide will reveal mostly similar intents regarding personal data protection and privacy, yet the regulatory frameworks and nuances across ASEAN (and globally) do have differences and variations. In contrast, the field of information technology ("**IT**") security (also called cybersecurity) displays a much more homogeneous landscape in general, regionally as well as globally. There are for example internationally accepted standards for IT security, most prominently the long-standing (since 2005) ISO/IEC 27001, and well-known frameworks like *The Open Web Application Security Project* (OWASP)[36] and MITRE ATT&CK[37]. Some of these are certifiable standards, which involve an approved and qualified third-party assessment, in contrast to a mere self-check for legal compliance commonly applied in the data protection domain.

A common misconception equates IT security with the specific data security obligations under countries' data protection laws. In fact, obligations such as those under Singapore's Personal Data Protection Act 2012 ("**PDPA**") and comparable laws in other jurisdictions typically use generic terms like "reasonable security arrangements". They do not explicitly refer to particular standards. Furthermore, they imply not only professional IT software and security design, engineering and testing, but extend to what is referred to as privacy engineering.



While there are indeed commonalities and overlaps between security and data protection/privacy, there are also critical differences, as shown in the figure above (the size of each domain as well as the overlap between them is only illustrative, not to scale for any specific jurisdiction, and may vary substantially from system to system). This has been recognised on the

[36] https://owasp.org/Top10
[37] https://attack.mitre.org

international level: using ISO/IEC 27001 again as example, which has been complemented since 2019 by a specific privacy extension, namely ISO/ICE 27701 *Privacy Information Management System*. Furthermore, a notably revised version of ISO/IEC 27001 was published in 2022, with an explicit inclusion of privacy in the new title *Information security, cybersecurity and privacy protection*. (Side note: The grace period to transition from the previous version ISO/IEC 27001-2013 to the new version ends by October 2025). Similarly, NIST has been aligning its Privacy Framework with the Security Framework. Nothing indicates that one could simply replace the other, rather both are needed, yet can leverage each other. This applies especially in the digital era when systems hardly exist without processing personal data or affecting privacy.

IT security is typically simplified and explained in terms of "CIA", which refers to confidentiality, integrity, and availability of information and systems, Security is sometimes extended to authorisation, audit, non-repudiation, and even more. However, CIA is actually an information-theoretic, high-level concept. Its implementation refers to IT security engineering, and that implementation can vary case by case, e.g. using encryption or access control mechanisms. Similarly, concepts like Data Protection by Design (or Privacy by Design), especially in their original form of the 7 principles created by Ann Cavoukian[38], are high level concepts, the implementation of which refers to privacy engineering, e.g. using Privacy Enhancing and Privacy Preserving Technologies ("**PET**"/"**PPT**"). The 7 principles include but also go beyond IT security considerations.

It therefore stands to reason that it is commonly acknowledged that without good software engineering, no good IT security can be achieved, and without good IT security, strong data protection cannot be ensured. However, we have arguably seen rather little progress in the skills of software and security engineering in general. To illustrate: enforcement decisions by data protection authorities, as well as guides on the typical causes of data breaches, across jurisdictions, are full of findings that attackers (often with little effort) succeeded in finding trivial bugs or exploiting well-known vulnerabilities such as SQL injection and URL manipulation. This seems to fly in the face of statements we may often see in media that threat actors are becoming ever more sophisticated over time. However, this is not to say they are not getting more sophisticated, as many threat actors have created their own attack-business models and services, like RaaS (ransomware-as-a-service), and there have indeed been sophisticated attacks in recent times, for example, the Accellion incident in 2020/2021 where the threat actors targeted a file transfer application that was used by well over 100 companies globally.

Similarly, many cases show a surprising lack of skills and coverage in core software and security testing. For example, it is not uncommon to find that vendors and organisations do not differentiate a vulnerability assessment ("**VA**") well enough from a penetration test ("**PT**"), to the extent that for example in 2022 the Singapore Cyber Security Agency ("**CSA**") created the world's first regime for VA/PT service providers for the Singapore market to be licensed (and this despite the existing framework that pen tester's and organisations which provide such services should be CREST certified).

[38] Available at https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf.

Similarly, it is not uncommon to see a test, which supposedly should include security and data protection aspects, be called a UAT (user acceptance test) instead of the more suitable term security test or SAT (system acceptance test).

All this makes a privacy engineer's life a rather daunting challenge: not only do they need to have a firm grasp of engineering and security, they also need to understand data protection laws and cross-border differences when it comes to personal data, and on top of that they need to evaluate how their organisations may deploy cutting edge privacy-specific technologies, which include exotic sounding solutions like homomorphic encryption, secure multi-party-computing, federated learning and more. Such technologies can be hard to understand fully, and even harder to implement and test, for anyone who does not have a solid experience in engineering and security. Lastly, in the era of smart homes and smart nations, Internet of Things (IoT) devices as well as mobile applications and systems add their own peculiarities in terms of security and privacy. In these domains, we see internationally renewed interest and efforts by regulators to encourage and sometimes enforce third-party product assessments and certifications, instead of the more common process-oriented approaches in privacy and data protection.

B) Guidance for Organisations

Organisations seeking to address the basic security and privacy challenges noted in **(A)** can refer to guidance from the relevant data protection authorities. In Singapore, the PDPC has issued a number of guides and handbooks on this topic. Many of these guides and handbooks are suitable for both a technical and non-technical audience, as they tend to explain things from a practical perspective rather than from the legal, compliance angle. However, it is explicitly stated in these guides that following them alone does not automatically establish compliance with the law. Therefore, at least in the case of PDPA, the PDPC's guides always must be read in conjunction with the PDPA and other sources, such as PDPC's advisory guidelines on the interpretation of the PDPA and PDPC's enforcement decisions. PDPC's guides, advisory guidelines and enforcement decisions are available on its website[39].

The following are some guides issued by Singapore's PDPC.

(i) Guide to Securing Personal Data in Electronic Medium

One of the earliest technical guides in this respect published by PDPC was the *Guide to Securing Personal Data in Electronic Medium*[40], released in May 2015 and updated in January 2017. This guide covered a wide range of common cybersecurity topics and mistakes, including the following:

- ICT security and data breach risks involving personal data
- Governance

[39] www.pdpc.gov.sg

[40] Available at https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/guidetosecuringpersonaldatainelectronicmedium0903178d4749c8844062038829ff0000d98b0f.pdf.

- Security awareness
- Compliance, testing and audits
- Authentication, authorisation and passwords
- Destruction of electronic personal data
- Computer networks
- Personal computers and other computing devices
- Portable computing devices and removable storage media
- Printers, copies, scanners and fax machines
- Databases
- Email
- Websites and web applications
- ICT outsourcing and software products
- Cloud computing

This guide also included checklists of good and enhanced security practices which organisations may consider adopting.

(ii) ***Data Protection Practices for ICT Systems***

In late 2021, PDPC launched a larger framework called *Data Protection Practices for ICT Systems*[41]. This framework includes a revamped guide on data protection practices (integrating most of the previous stand-alone guide) and a separate set of checklists. It further features a new handbook, called *How to Guard Against Common Types of Data Breaches*[42], which identifies and illustrates the five most common gaps in ICT system management and processes, mostly based on PDPC's analysis of its own investigations and breach decisions.

(iii) ***Guide Disposal of Personal Data on Physical Medium***

Another early guide from PDPC, which starkly reminds us that not all is about cyber alone, was the *Guide to Disposal of Personal Data on Physical Medium*[43]. Physical medium therein refers to storage media like drives, USB sticks, DVDs, etc, and, not to forget, print and paper documents. These are often considered temporary storage (especially when 'drafts' of reports or lists are printed) and tend to be treated with less awareness than the 'final' or 'main' version of the data. However, loss of such media as well as exposing oneself to dumpster diving (searching through physical waste or recycling containers for discarded items) are real security and data protection failures, and such material remains covered by regulation. This guide has also been supplemented by the Guide to Data Protection Practices for ICT Systems (see above) since 2021.

[41] Available at https://www.pdpc.gov.sg/help-and-resources/2021/08/data-protection-practices-for-ict-systems.
[42] Available at https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/tech-omnibus/how-to-guard-against-common-types-of-data-breaches-handbook.pdf.
[43] Available at https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/guide-to-disposal-of-personal-data-on-physical-medium-(200117).pdf.

C) Obligations of Data Controllers and Data Processors/Data Intermediaries

Many data protection laws provide for different obligations for data processors ("**DPs**") or data intermediaries ("**DIs**") as compared to data controllers ("**DCs**"). DPs and DIs are, in general, considered to have fewer obligations under several data protection laws. However, when it comes to security and privacy engineering, DPs and DIs are often subject to the same obligation to protect personal data using "reasonable security arrangements" (or similar wording) as DCs. As such, as far as the security of personal data is concerned, there is, in principle, as good as no difference between DPs/DIs on the one hand and DCs on the other. In practice, the scope of "reasonable security arrangements" takes into account the management and operational scope of the parties concerned and hence one party, typically the DC, may have greater responsibility in terms of ensuring that a DP/DI with appropriate experience and technical abilities is engaged to process personal data while the other, the DP/DI, may have greater responsibility in terms of implementing appropriate technical security measures to protect the data. Nevertheless, there can be substantial overlap between the responsibilities of both these categories of organisations, for example, in relation to administrative security measures (such as security policies) and sophisticated DCs often have significant involvement in all aspects of the security of personal data by the DPs/DIs they engage.

While some larger and more sophisticated DCs may have the necessary resources and internal expertise to manage security and privacy issues relating to their DPs and DIs, many organisations do not. In particular, small and medium enterprises ("**SMEs**") may not have the skills and resources to manage IT systems and IT products, and they tend to outsource such activities to vendors. Furthermore, in contrast to DPs and DIs, some vendors may not even be subject to the applicable data protection laws, for example, in cases where the services provided by the vendors does not include direct management or processing of personal data.

In either case, organisations still need to exercise proper oversight and due diligence regarding technical and administrative security measures with respect to their obligations under the applicable data protection laws. In the absence of in-house experts, guides issued by data protection authorities are valuable resources as a starting point and reference for project managers, legal counsels and other teams handling or managing personal data.

CONTACTS

David N. ALFRED

Director and Co-head, Data Protection, Privacy & Cybersecurity, Drew & Napier LLC
Co-head and Programme Director, Drew Data Protection & Cybersecurity Academy

E:David.Alfred@drewnapier.com

Albert PICHLMAIER

Senior Cybersecurity and Privacy Engineer, Data Protection, Privacy & Cybersecurity, Drew & Napier LLC
Senior Learning Technology Designer, Drew Data Protection & Cybersecurity Academy

E:Albert.Pichlmaier@drewnapier.com

DATA BREACH MANAGEMENT ACROSS ASEAN

12. DATA BREACH MANAGEMENT ACROSS ASEAN

A) Data Breach Notification in Context

Data breach notification is increasingly becoming a significant legal obligation that organisations need to be aware of across the jurisdictions they are operating in. However, the full extent of organisations' obligations does not begin, or end, with data breach notification. Instead, it is part of the broader set of obligations organisation may have under data protection law and potentially other laws.

Data protection laws, such as Singapore's PDPA and others in Southeast Asia, include the following obligations for organisations in respect of personal data in their possession or under their control:

- **Protection of personal data**, using reasonable security arrangements (or a similar standard that refers to technical, administrative and physical security measures or controls which an organisation may employ);

- **Accountability for personal data**, including the development of policies and practices that are necessary for the organisation to meet its obligations under the relevant data protection law; and

- **Data breach notification**, which requires organisations to notify the jurisdiction's data protection authority (for example, in the case of Singapore, the Personal Data Protection Commission) and, in some cases, affected individuals, where a data beach meets the stipulated thresholds for notification.

Taken together, the above-mentioned obligations require organisations to develop and implement the necessary policies and internal governance frameworks and controls to ensure appropriate protection of personal data. This would typically include developing and implementing a security incident response plan ("**SIRP**") or data breach management plan ("**DBMP**") to address how the organisation should respond in the event of a security incident or data breach that arises in relation to the organisation's networks, systems, devices and/or data.

While the terms security incident and data breach are sometimes used, in a general sense, to refer to the same type of incident, a distinction may be made that a security incident refers to any incident affecting the security of an organisation's systems, etc, whereas a data breach refers to a security incident where there has been some kind of unauthorised access to the organisation's systems, etc, or loss of data or a device containing data.

The contents of an SIRP or DBMP typically include the following:

- Measures to monitor for the occurrence of security incidents;
- Instructions to the organisation's staff on when and how to report the occurrence of a security incident (including what constitutes a security incident);

- Composition and responsibilities of the security incident response team;
- Steps and measures to respond to a data breach, including measures to contain and assess a data breach; and
- Framework to evaluate the organisation's response to a data breach, including a process to make improvements to its SIRP/DBMP.

An organisation's IT and cybersecurity teams have a critical role to play to ensure that the organisation responds quickly and effectively in the event of a data breach. They typically have a significant range of tasks to perform, often under tight timelines, for example, to prevent further unauthorised access to the organisation's networks and systems, prevent exfiltration (or further exfiltration of data) and remediate the cause(s) of the incident.

The organisation's data protection officer also has an important role to play and this is in ensuring that the organisation assesses whether a data breach is notifiable under the applicable laws in a timely manner.

B) Data Breach Notification Requirements Across ASEAN

In brief, jurisdictions with data breach notification obligations in their data protection law include Indonesia, the Philippines, Singapore, Thailand and Vietnam.[44] For these jurisdictions, in the event of a data breach (as defined under the relevant law), organisations are in general required to notify the jurisdiction's data protection authority within 72 hours or 3 calendar days. In the Philippines, the requirement to notify the data protection authority only applies in relation to sensitive personal data (as defined).

Organisations may also be required to notify affected individuals in the event of a data breach that meets the specified threshold. A similar 72-hour time frame applies in the case of Indonesia and the Philippines. Thailand requires such notifications without undue delay and Singapore requires notification to individuals on or after notifying the PDPC.

C) Data Breach Management and Response in a Regional or Global Context

Organisations that are affected by a data breach must comply with all applicable data breach notification obligations. In this regard, organisations should be mindful of the following:

- While a data protection law typically requires notification to the jurisdiction's data protection authority, the organisation should consider whether to make a police report or notify other agencies. A police report may be appropriate, for example, where a data breach may be suspected to arise from criminal activity within the jurisdiction or there may be misuse of the data exfiltrated for other criminal purposes. Other agencies which may be concerned with the occurrence of a data breach may include the jurisdiction's cybersecurity regulator and sectoral

[44] A similar obligation is expected to be introduced in due course in Brunei's Personal Data Protection Law. Please refer to the relevant chapters of this guide for more details of these jurisdictions laws.

regulators having oversight over the organisation's industry sector. Notifying the relevant authorities can also aid an organisation in managing its response to a data breach and its communications to the affected individuals or other stakeholders.

- In many cases, the exact impact of the data breach may require investigations over a period of time. Nonetheless, where the threshold for reporting a data breach has been met, organisations should meet their notification obligation even though their investigations have not been completed. This is particularly important to bear in mind in jurisdictions where the applicable threshold(s) for notification are relatively low.

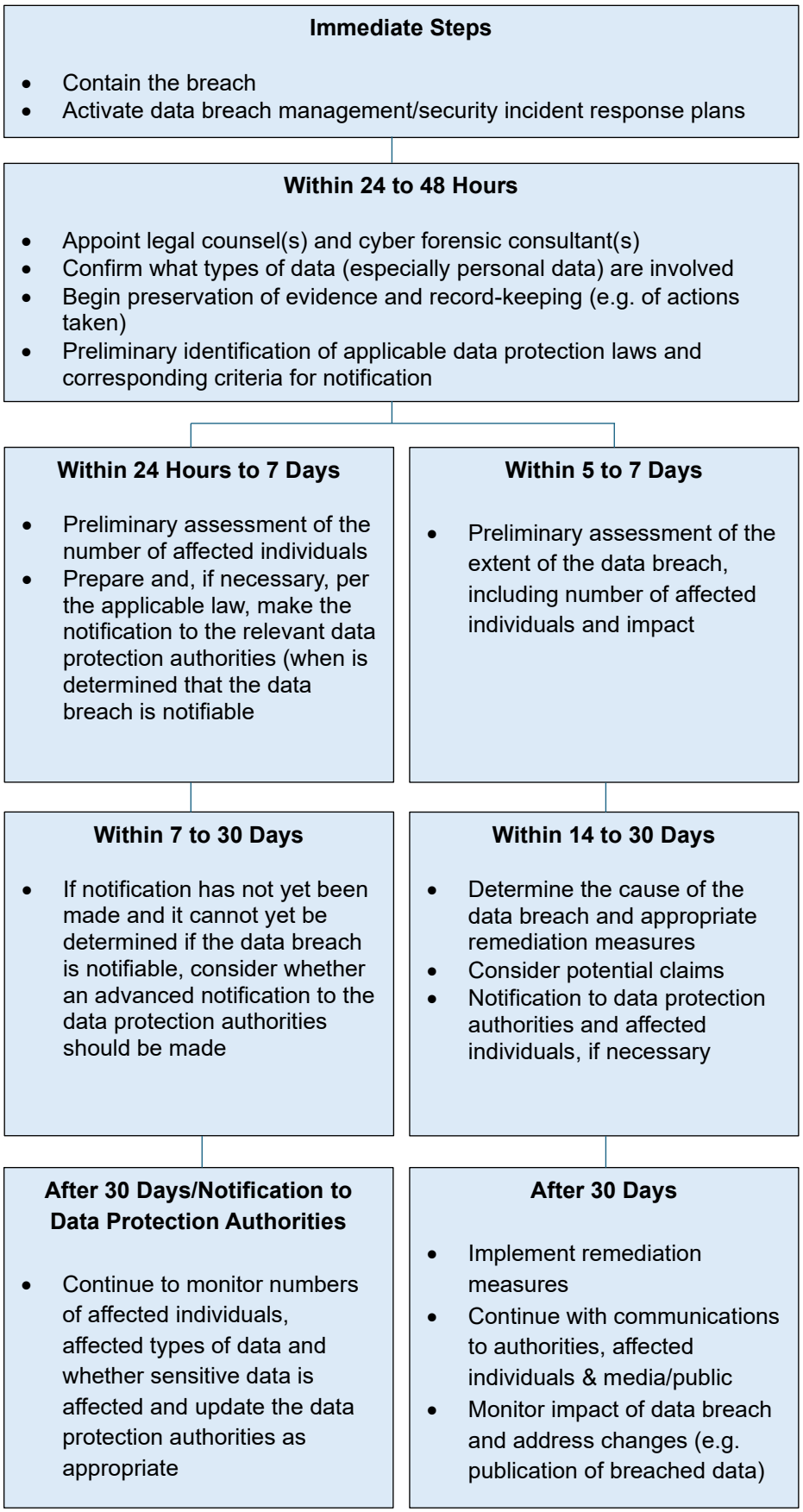
- Amidst the flurry of activities that invariably happens when a data breach is discovered, organisations should also bear in mind that some information they may require to investigate the causes of the data breach may have a limited lifespan, for example, system or firewall logs. Steps should be taken as early as possible to obtain copies of such information and preserve them for the investigation.

- Where an organisation decides to engage an external service provide to aid in analysing and determining the cause(s) of a data breach, they should also consider engaging a law firm to ensure, as far as possible, that the appropriate steps are taken to protect information that should be protected under legal privilege. This will likely give the organisation some breathing room in considering its legal and regulatory response to the data breach and protect its legal and business interests.

- For organisations that hold the personal data of foreign individuals, it should not be assumed that foreign data protection laws do not apply to a data breach in a particular jurisdiction. This is especially, but not solely, the case where personal data of the foreign individuals was originally collected while they were overseas. In this regard, many data protection authorities are concerned that organisations based in another country which collect personal data from individuals within their jurisdiction comply with the relevant obligations of their data protection law.

D) What to Do When a Data Breach Occurs

The following chart illustrates key steps of what an organisation should do in the event of a data breach. Note that these are not prescribed time frames and the circumstances and events may require a different approach. The first two stages are critical in ensuring that the organisation has activated or obtained the necessary resources to support its response to the data breach.


Immediate Steps
Contain the breach
Activate data breach management/security incident response plans
Within 24 to 48 Hours
Appoint legal counsel(s) and cyber forensic consultant(s)
Confirm what types of data (especially personal data) are involved
Begin preservation of evidence and record-keeping (e.g. of actions taken)
Preliminary identification of applicable data protection laws and corresponding criteria for notification
Within 24 Hours to 7 Days
Preliminary assessment of the number of affected individuals
Prepare and, if necessary, per the applicable law, make the notification to the relevant data protection authorities (when is determined that the data breach is notifiable
Within 5 to 7 Days
Preliminary assessment of the extent of the data breach, including number of affected individuals and impact
Within 7 to 30 Days
If notification has not yet been made and it cannot yet be determined if the data breach is notifiable, consider whether an advanced notification to the data protection authorities should be made
Within 14 to 30 Days
Determine the cause of the data breach and appropriate remediation measures
Consider potential claims
Notification to data protection authorities and affected individuals, if necessary
After 30 Days/Notification to Data Protection Authorities
Continue to monitor numbers of affected individuals, affected types of data and whether sensitive data is affected and update the data protection authorities as appropriate
After 30 Days
Implement remediation measures
Continue with communications to authorities, affected individuals & media/public
Monitor impact of data breach and address changes (e.g. publication of breached data)

How to Activate Us

To activate us for data breach issues across ASEAN:

LIM Chong Kin

Managing Director, Corporate & Finance
Co-head, Data Protection, Privacy & Cybersecurity
Co-head, Drew Data Protection & Cybersecurity Academy,
Drew & Napier LLC

E:Chongkin.Lim@drewnapier.com
O: +65 65 6531 4110
M: +65 9011 0100

David N. ALFRED

Director and Co-head, Data Protection, Privacy & Cybersecurity
Co-head and Programme Director, Drew Data Protection & Cybersecurity Academy,
Drew & Napier LLC

E:David.Alfred@drewnapier.com
O: +65 6531 2342
M: +65 9696 7145

Jurisdiction Coverage

Indonesia

Heru MARDIJARTO

Partner
Makarim & Taira S.

E:Heru.mardijarto@makarim.com

Reagan Roy TEGUH

Partner
Makarim & Taira S.

E:Reagan.teguh@makarim.com

Lia ALIZIA

Partner
Makarim & Taira S.

E:Lia.alizia@makarim.com

Malaysia

Timothy SIAW

Co-Head, Technology, Media & Telco
Partner, Intellectual Property
Partner, Healthcare and Life Sciences
Shearn Delamore & Co.

E:Timothy@shearndelamore.com

Janet TOH

Head, Personal Data
Co-Head Technology, Media & Telecommunications
Partner, Intellectual Property
Shearn Delamore & Co.

E:Janet.toh@shearndelamore.com

Philippines

Erika B. PAULINO

Partner
Head, Data Privacy and Security
Martinez Vergara & Gonzalez Sociedad

E:Erika.paulino@mvgslaw.com

Kristine R. BONGCARON

Partner
Co-Head, Data Privacy and Security
Martinez Vergara & Gonzalez Sociedad

E:Kristine.bongcaron@mvgslaw.com

Singapore and Brunei Darussalam

LIM Chong Kin

Managing Director, Corporate & Finance
Co-head, Data Protection, Privacy & Cybersecurity
Co-head, Drew Data Protection & Cybersecurity Academy,
Drew & Napier LLC

E:Chongkin.Lim@drewnapier.com

David N. ALFRED

Director and Co-head, Data Protection, Privacy & Cybersecurity
Co-head and Programme Director, Drew Data Protection & Cybersecurity Academy,
Drew & Napier LLC

E:David.Alfred@drewnapier.com

Anastasia CHEN

Director, Corporate & Finance and Data Protection, Privacy & Cybersecurity,
Drew & Napier LLC

E:Anastasia.Chen@drewnapier.com

Thailand, Vietnam, Cambodia, Laos and Myanmar

Nopparat LALITKOMON

Partner, Head of Data Privacy and Cybersecurity
Tilleke & Gibbins

E:Nopparat.l@tilleke.com

Waewpen PIEMWICHAI

Counsel
Tilleke & Gibbins

E:Waewpen.p@tilleke.com

Jay COHEN

Partner and Director, Cambodia
Tilleke & Gibbins

E:Jay.c@tilleke.com

Yuwadee THEAN-NGARM

Partner and Director, Myanmar
Tilleke & Gibbins

E:Yuwadee.t@tilleke.com

DNA

- Singapore
- Philippines
- Myanmar
- Indonesia
- Cambodia
- Thailand
- Malaysia
- Laos
- Vietnam

www.drewnetworkasia.com

www.linkedin.com/company/drewnetworkasia