Comparative Guide

Data Privacy and Cybersecurity

Indonesia & Singapore Law

Prepared by:

Nusantara Legal Partnership

CLYDE&CO CLASIS SINGAPORE
A joint law venture

Indonesia

Marshall Situmorang and Audria Putri | Nusantara Legal Partnership

Data Privacy and Cybersecurity Comparative Guide

A. Definition and Scope of Data Privacy and Cybersecurity

Data Privacy

1. **Is there any specific definition of "*personal data*" in your jurisdiction? Do the prevailing laws provide distinction between personal data and sensitive personal data?**

   Personal data is defined as *"a certain personal data that is stored, maintained, kept true and its confidentiality is protected"* (Art. 1 (1) of Minister of Communications and Informatics ("**MoCI**") Regulation No. 20 of 2016 on Personal Data Protection within the Electronic System ("**MoCI Regulation 20/2016**")). However, the applicable laws and regulations on personal data protection in Indonesia do not provide any specific definition of "*sensitive personal data*" and are silent on these matters.

   Therefore, there is no clear distinction between "*personal data"* and "*sensitive personal data"*.

2. **What is the scope of "*personal data*" pursuant to the relevant laws and regulations in your jurisdiction?**

   Indonesian prevailing laws do not provide any specific scope of personal data. There are merely provisions under MoCI 20/2016 as outlined above.

   The concept of data privacy is interpreted as a part of the privacy right, which, pursuant to Law No. 11 of 2008 as amended by Law No. 19 of 2016 ("**EIT Law**"), is defined as:

   a. the right to enjoy a private life and be free from all kinds of disturbances;
   b. the right to communicate with other persons (without being spied on);
   c. the right to supervise the access to information on his/her personal life and data (Elucidation of Art. 26 (1) of EIT Law).

   In addition to the above, Personal Data Protection Bill **("PDP Bill")** sets out a more specific scope of personal data:

(i) General personal data consists of a person's full name, gender, citizenship, religion, and/or combined personal data to identify a person;
(ii) Specific personal data, which consists of, among other things, information on a person's health, biometric data, political view, etc. (Art. 3 (1), (2), and (3) of PDP Bill).

However, PDP Bill has not been enacted up to the publication of this comparative guide.

3. **Who are the relevant stakeholders (i.e., data processor, controller, etc.) under the data protection regime in your jurisdiction?**

Stakeholders of data protection under the Indonesian prevailing laws include: (i) personal data user; and (ii) Electronic System Operator **("ESO")**, each of which has different obligations. Please note that the current prevailing laws and regulations for personal data protection do not specifically stipulate data processor and data controller, but merely the party collecting and processing personal data and the relevant data subject. PDP Bill, however, provides specific definitions of data processor and data controller.

With regard to ESOs, Art. 2 of Government Regulation **("GR")** No. 71 of 2019 on Administration of Electronic Transactions and Systems **("GR 71/2019")** stipulates two categories of ESOs, namely (i) public ESO and, (ii) private ESO.

Public ESOs include state administrator agencies and other agencies as formed by virtue of laws and/or appointed by the relevant agencies. Meanwhile, private ESOs include individuals, business entities, and the public that run portals, websites, or online applications on the internet, regulated or supervised by the Minister of Communication and Informatics, and/or the institutions based on the relevant regulations.

Cybersecurity

4. **Is there any specific definition of "*cybersecurity*" in your jurisdiction? Do the prevailing laws provide distinction between "*data protection*" and "*cybersecurity*"?**

Cybersecurity in Indonesia is governed by EIT Law and GR 71/2019, but they provide no specific definitions or terms on cybersecurity itself. A bill on cybersecurity was once proposed, but it was eventually rejected and failed to be enacted in 2019.

Based on EIT Law and GR 71/2019, the general concept of cybersecurity provisions focuses on cyber incidents including prohibitions of hacking, denial of service, phishing and identity theft, as well as cybercrimes.

5. **What are the subjects of cybersecurity? Does cybersecurity apply to certain industries and types of information?**

The government has established an institution that oversees cybersecurity and encryption namely, the National Cyber and Crypto Agency/ *Badan Siber dan Sandi Negara* **("BSSN")**, which functions include but not limited to identification, detection, protection, monitoring of the implementation of technical policies regarding cybersecurity in e-commerce protection, cyber-attacks, and/or cyber incidents in Indonesia.

In addition to the above, the government stipulates protection over certain strategic information of these sectors: (i) Government Administration; (ii) Energy and Mineral Resources; (iii) Transportation; (iv) Finance; (v) Health; (vi) Information and Communication Technology; (vii) Food; (viii) Defense; and (ix) other sectors as determined by the President.

B. Governing Authority of Data Privacy and Cybersecurity

Data Privacy

6. **Is there any specific government agency that oversees data privacy legislation in your jurisdiction? Please define what powers and authorities such agency has in the data privacy enforcement?**

Indonesia has **no** specific government agency or independent body overseeing the data privacy legislation given that neither data privacy nor cyber security bills have been passed. Considering data privacy provisions within the scope of EIT Law and MoCI 20/2016, the enforcement of data privacy is supervised by (i) MoCI and several sector-specific authorities, (ii) BSSN; and (iii) an agency under BSSN i.e., Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Center (Id-SIRTII).

MoCI, the main supervisory body, can be supported by Indonesian police in the enforcement of data privacy protection. There are also sector-specific authorities that supervise data protection along with MoCI, e.g., Central Bank of Indonesia for data protection in the banking sector, and the Ministry of Health in the health sector.

BSSN's duty, function, and authority are not limited to data privacy enforcement. They cover a broader scope overseeing the overall matters under EIT Law, including cybersecurity. BSSN carries out the government's duties in the field of cyber and crypto security, focusing on cyber resilience, and resistance against possible attacks by crime organizations on the national level, and those with private interests.

Furthermore, the duty and function of Id-SIRTII mainly focus on supporting the internet growth in Indonesia through various awareness campaigns on securing the technology and information systems, monitoring the potential security incidents, supporting the law enforcement, and providing the relevant technical supports in the interests of the general public.

7. **Can the data protection authority in your jurisdiction cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?**

   MoCI 20/2016 stipulates that MoCI may coordinate with the sectoral supervision and regulatory body to (i) address complaints of data subjects for breaches of personal data protection committed by ESOs; and (ii) impose administrative sanctions for such breaches. MoCI further delegates the authority for the supervision and dispute settlement to the Directorate General of Informatics Application/ *Direktorat Jendral Aplikasi Informatika* (**"Ditjen Aptika"**).

   In this regard, MoCI and BSSN may work with other relevant authorities, for instance, Indonesian police and the intelligence service agencies (**i.e.,** the State Intelligence Agency/ *Badan Intelejen Negara* **(BIN)** and the Strategic Intelligence Agency/ *Badan Intelejen Strategis* **(BAIS))**.

Cybersecurity

8. **Is there any specific government agency that oversees cybersecurity legislation in your jurisdiction? Please define what powers and authorities such agency has in the cybersecurity enforcement?**

   Cybersecurity in Indonesia is supervised by MoCI, BSSN, and Id-SIRTII.

9. **How does the cybersecurity authority cooperate with Data Protection Office ("DPO")? Does your jurisdiction provide certain guidelines for this matter?**

   Indonesia has yet to establish a specific, independent office in-charge of Data Protection. However, MoCI Regulation 20/2016 requires the appointment of a person-in-charge that can be contacted by the relevant personal data owners regarding the management of their personal data.

   Although appointing a DPO is not a requirement, please note that Art. 45 of PDP Bill obliges any data controller or processor to appoint a DPO. This obligation applies to any data controller or processor: (i) who works on data processing to provide public services, (ii) whose main activity requires large-scale, frequent, and systematic monitoring of personal data; and (iii) whose core activity includes processing specific personal data in a large scale, and/or processing personal data related to criminal activity.

C. Regulatory Framework and Registration

Data Privacy

10. **What are the applicable laws and regulations that govern data privacy and personal data protection in your jurisdiction? Please identify further laws on data protection in specific sectors, if any.**

    Data privacy and personal data protections are governed under the following laws and regulations:

    a. EIT Law;
    b. GR 71/2019;
    c. GR No. 80 of 2019 regarding Trading through Electronic System; and
    d. MoCI Regulation 20/2016.

    MoCI Regulation 20/2016 also stipulates that a data owner reserves the right to file a lawsuit for a breach of his/her personal data, in accordance with Art. 1365 of Indonesia's Civil Code/ *Kitab Undang-Undang Hukum Perdata* regulating that any person violating the law is liable for any losses caused by his/her action. The enforcement of data protection refers to Indonesia's Criminal Code/ *Kitab Undang-Undang Hukum Pidana* for the criminal sanction.

    Other relevant sectors also governing the legislation on data privacy and personal data which include the banking, health, and capital market sectors under:

    a. Law No. 36 of 1999 on Telecommunications as amended by Law No. 11 of 2020 on Job Creation;
    b. Law No. 10 of 1992 on Banking as amended by Law No. 10 of 1998;
    c. Law No. 8 of 1995 on Capital Market;
    d. Law No. 36 of 2009 on Health; and
    e. Law No. 14 of 2008 on Disclosure of Public Information.

11. **Are there any exemptions under the data privacy and personal data protection rules in your jurisdiction?**

    The prevailing laws and regulations do **not** provide any exemption with respect to the mandatory registration of ESO.

12. **Do the data privacy applicable laws and regulations apply extraterritorially? If yes, how do DPO and the government exercise such duties?**

Yes. Art. 2 of EIT Law explicitly states that it applies extraterritorially, including to foreign legal subjects regardless of their presence in Indonesia. Therefore, any legal action regarding data protection carried out outside the jurisdiction of Indonesia by Indonesian citizens or legal entities, or foreign citizens or legal entities that have legal consequences in Indonesia shall be subject to EIT Law. Furthermore, Article 50 of PDP Bill also provides that the Indonesian PDP laws shall be applicable to any breach of personal data protection occurring domestically or abroad.

The provision was built on the concept where the misuse of information technology for electronic information and transactions might, in the future, threaten and harm the interests of Indonesia, which might be detrimental to the nation's (i) economic interests, (ii) protection of strategic data, (iii) dignity, (iv) defense and state security, (v) sovereignty, citizens, and (vi) legal entities. Given the authority over DPO has yet to be established, MoCI shall be the authority that oversees and responsible for coordinating with the ESOs in cross-border, personal data transmissions.

13. **Is the registration of data controllers and processors mandatory in your jurisdiction? If <u>yes</u>, how is the registration procedure completed, and what are the consequences for failing to conduct the registration?**

In general, Indonesia's prevailing regulations do not specifically distinguish a data controller from a data processor. Both are recognized as ESOs. Pursuant to GR 71/2019, any public or private ESO, located onshore or offshore, is obliged to conduct ESO registration to MoCI **("ESO Registration")** through the OSS system prior to conducting any business activity.

The required documents for ESO Registration are (i) registration form including the corporate documents, tax identification number of the company, contact person; and (ii) supplemental documents i.e., general information regarding the electronic system including the system's profile, URL website, IP address, descriptions on the system's functions and business process, and the ESO's statement of willingness to conduct the personal data protection.

Failure to comply with the mandatory ESO registration will be subject to administrative sanctions in the form of warning letters, administrative fine, temporary suspension, access termination, and/or removal from MoCI's list.

Cybersecurity

14. **Is there any specific laws and regulations that govern cybersecurity for data privacy and personal data in your jurisdiction?**

As outlined in Points 4 and 5 above, Indonesia has no specific regulation on cybersecurity for data privacy and personal data. But EIT Law, GR 71/2019, and MoCI Regulation 20/2016 stipulate general provisions on data protection, including cybersecurity for data privacy and personal data.

15. **Is there any specific threshold on the number of personal data subjects that requires a certain level of cybersecurity system?**

There is **no** specific provision regarding this matter.

D. Data Processing

---

16. **What are the recognized, legitimate grounds of personal data processing in your jurisdiction?**

The lawful basis for personal data processing in Indonesia is to obtain consent from the relevant data subject. Such data processing should be carried out in accordance with the specific purposes, expressly elaborated during the data obtainment. Therefore, the use of electronic information involving any personal data must be made with the approval of the relevant person and only for the specified purposes.

Nevertheless, there are certain exceptions where the lawful basis may be waived if: (i) the disclosure of personal data is for law enforcement purposes; and (ii) the personal data interception is for the legitimate interest of the ESO as the data controller. The laws allow the legitimate interest basis as long as the relevant ESO adheres to the prevailing laws and regulations.

17. **What are the key requirements (*such as notification or consent from the personal data subject*) when processing personal data in your jurisdiction?**

Please refer to our response in Point 16 above.

18. **Are there other requirements, restrictions, and best practices that should be considered when processing personal data in your jurisdiction?**

As outlined in Point 16 above, the purposes of data processing shall be restricted and clearly expressed during the time of data collection. Therefore, ESOs are not allowed to process any data that is not in the scope of processing purposes stated in the data subject's consent form.

In addition, GR 71/2019 stipulates that the management, processing, and/or retention of the electronic system and data for ESO in the public sector shall be done within the Indonesian territory. The exemption of this provision is available if the required retention technology is not available domestically. This clearly

provides that any data processing done by a Public ESO is still subject to the data onshoring requirements.

Another provision worth considering is the Personal Data retention period. MoCI Regulation 20/2016 stipulates that the retention period of personal data is five years. In this instance, any obtained data should be retained for, at least, five years, from the last date it is used by the data subject.

E. Data Transfer

19. **What are the requirements that apply to a transfer of data to third parties?**

There is no specific requirement on this matter. However, it is important to note that a transfer of personal data is prohibited without the consent of the data subject.

20. **Are there restrictions that apply to a transfer of data abroad? Are there any exemptions on this matter?**

MoCI Regulation 20/2016 requires any cross-border transfer of personal data to fulfill the following requirements:

a. Submission of a notification regarding the intended transfer of Personal Data abroad, containing, at least, information on: (i) the country of destination; (ii) the name of recipient; (iii) the date of transfer, and (iv) the purpose of transfer.
b. A request for advocacy if required; and
c. Submission of report on the result of such cross-border transfer,

Additionally, no personal data may be transferred abroad unless the receiving country has been declared to have the equivalent protection standard by the Minister of Trade.

21. **Do the prevailing law and regulations on cybersecurity provide certain requirements for a local data transfer? If yes, do they require certain methods or procedures for a data transfer?**

We note that no certain methods or procedures specifically apply to local data transfers apart from the principles discussed in Points 19 and 20 above.

F. Rights of Data Subject

22. **What are the rights of data subject in connection to personal data processing? Are there any exemptions to such rights? Please elaborate.**

The rights of a data subject pursuant to Art. 26 of MoCI Regulation 20/2016 are as follows:

a. the right to confidentiality of his/her personal data;
b. the right to access data alternation, supplementation, as well as renewal. This right should include the access to historical record of his/her personal data already transferred to the ESO;
c. the right to delisting, a data subject exercising this right is required to submit a petition to the relevant district court. If the petition is granted, the court decision should become the basis to request a delisting of the irrelevant electronic information and/or document to the ESO (under GR 71/2019);
d. the right to request the erasure of his/her personal data; and
e. the right to file a complaint in the dispute settlement for the failure to get the needed protection to maintain the confidentiality of his/her Personal Data.

In addition to the above, PDP Bill also provides that the personal data controller must ensure the implementation of the "*right to be forgotten*".

23. **Is there any procedure for data subjects to exercise their rights in your jurisdiction?**

There is no specific procedure under the prevailing laws, but there are legal provisions as discussed in this article.

24. **What remedies are available to data subjects in case of a breach of their rights?**

EIT Law provides the right for a data subject to file claim of monetary damages to the relevant ESOs by providing evidence of the actual damages due to the transpired security breach.

G. Data Protection Officer

25. **Is the appointment of a Data Protection Officer ("DPO") mandatory in your jurisdiction? If <u>yes</u>, what are the consequences of failing to appoint the officer?**

The prevailing laws do not stipulate mandatory appointment of a DPO, nor consequences for failing to conduct such appointment. The laws, however, require ESOs to provide accessible contacts to data subjects. The term DPO was introduced in PDP Bill.

26. **What are the key responsibilities of a DPO in your jurisdiction?**

The current prevailing laws do not stipulate this matter, given that PDP Bill has not been passed.

Nonetheless, PDP Bill provides the following key responsibilities of a DPO:

(i) informing and advising the personal data controller or processor to comply with the prevailing laws and regulations;
(ii) supervising and ensuring the relevant data controller's or processor's compliance with PDP law and the privacy policy related to the assignment, including taking the responsibility, raising the awareness, providing the training for the related parties in the personal data process, and conducting the audit;
(iii) providing the advice in the evaluation on the impact of personal data protection, and monitoring the performance of the personal data controller and/or processor; and
(iv) coordinating the relevant stakeholders and acting as the liaison officer in managing issues related to personal data processing, including providing the consultancy on risk mitigation and/or other matters.

H. Data Breach

27. **Is it mandatory to provide a notification in the event of a data breach? If <u>yes</u>, who must be notified (<u>i.e.</u>, the data protection authority, the data subject, etc.) and what kind of information must be provided?**

Indonesian prevailing laws and regulations requires an ESO experiencing a data breach to immediately notify the relevant personal data subject and authorities, then go through the process in the following details:

a. **Relevant Authorities:** An ESO experiencing a data breach is obliged to notify the owner of the leaked data, and later on, file a complaint to the Directorate General of Informatics Application of MoCI. This complaint is intended to resolve a possible dispute caused by the data breach.

b. **Personal Data Subject:** The notice of breach to the Data Subject should include the following information:

- the reasons and causes of the data breach;
- the notice of breach can be submitted electronically provided that the Data Subject has agreed to such submission method during the collection of his/her Personal Data;

- the confirmation that the Data Subject will receive a report if the data breach leads to a potential loss; and
- the written report submitted to relevant Data Subject within 14 days after the occurrence of the breach.

28. **Are companies required to share details of actual or potential cybersecurity threats, or other cyber-intelligence information, with industries or other stakeholders? If yes, what kind of information must be shared?**

No requirements have been imposed on companies in this sense. The prevailing laws only require the ESOs to notify the relevant parties in the event of data breaches as explained in Point 27.

29. **How would a breach of data protection be handled by the authority? Can such breach lead to administrative sanctions or criminal penalties?**

Administrative and criminal sanctions can be imposed on persons committing unlawful acts, which include but not limited to all activities that violate the provisions of the prevailing laws and regulations on data protection and cybersecurity, carried out in bad faith. These sanctions are regulated by EIT Law, and other relevant regulations.

The applicable administrative sanctions are as follows:

a. MoCI Regulation 20/2016 provides the following sanctions:
   (i) verbal warnings;
   (ii) written warnings;
   (iii) suspension of business activities; or
   (iv) announcement of the breacher in MoCI's website.

b. GR 71/2019 provides the following sanctions:
   (i) written warnings;
   (ii) administrative penalty;
   (iii) suspension of business activities;
   (iv) termination of access to the electronic system; or
   (v) expulsion of the relevant platform as registered ESO.

In addition to the above, criminal sanctions in the form of fines and/or imprisonment are also applicable.

a. fine of IDR 600,000,000 (six hundred million rupiah) to IDR 800,000,000 (eight hundred million rupiah), and/or 4 to 8 years imprisonment for unlawful access;

b. fine of IDR 800,000,000 (eight hundred million rupiah) to IDR 1,000,000,000 (one billion rupiah), and/or 6 to 10 years imprisonment for illegal interception or wiretapping of transmission;
c. fine of IDR 2,000,000,000 (two billion rupiah) to IDR 5,000,000,000 (five billion rupiah), and/or 8 to 10 years imprisonment for unlawful alteration, addition, reduction, transmission, tampering, removal, transfer or concealment of electronic information or record; and
d. fine of IDR 10,000,000,000 (ten billion rupiah) to IDR 12,000,000,000 (twelve billion rupiah), and/or 10 to 12 years imprisonment for unlawful manipulation, creation, alteration, destruction, or damage of electronic information or document with a purpose of creating a certain assumption or conducting other violations in the processing of electronic information or documents.

30. **What other requirements, restrictions, and best practices should be considered in the event of a data breach?**

The government of Indonesia is aiming to complete the enactment of PDP Bill soon. When the bill is enacted into law, stricter provisions on Personal Data Protection and cybersecurity will be enforced. PDP Bill is expected to provide a more comprehensive guideline for personal data protection practitioners.

We still have to wait and see whether PDP Bill will have further changes prior to its enactment.

Nusantara Legal Partnership

Marshall S. Situmorang
marshall.situmorang@nusantaralegal.com

Andhitta Audria Putri
audria.putri@nusantaralegal.com

AIA Central, Level 31, Jl. Jend. Sudirman Kav. 48 A, Jakarta Selatan 12930
+6221 2709 1321
www.nusantaralegal.com

Singapore

Thomas Choo and Zhen Guang Lam | Clyde & Co

Data Privacy and Cybersecurity Comparative Guide

A. Definition and Scope of Data Privacy and Cybersecurity

Data Privacy

31. **Is there any specific definition of "*personal data*" in your jurisdiction? Do the prevailing laws provide distinction between personal data and sensitive personal data?**

Under Singapore's Personal Data Protection Act 2012 (Act 26 of 2012) ("**PDPA**"), "personal data" means data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access.

Although the PDPA does not have a separate category of "sensitive" personal data, it may be gleamed from the enforcement decisions by the PDPC (as defined in Question 36 below) that the PDPC takes a stricter view when considering a case where the personal data compromised is of a sensitive nature.

32. **What is the scope of "*personal data*" pursuant to the relevant laws and regulations in your jurisdiction?**

The following non-exhaustive laws and regulations contain sector-specific provisions relating to data including personal data:

a) Banking Act (Chapter 19): its banking secrecy provisions govern customer information held by banks and "personal data" would be in respect of such customer information.

b) Private Hospitals and Medical Clinics Act (Chapter 248): its provisions govern the confidentiality of medical information and "personal data" would be in respect of such medical information.

33. **Who are the relevant stakeholders (i.e., data processor, controller, etc.) under the data protection regime in your jurisdiction?**

An "individual" under the PDPA (which is the equivalent of a "data subject" under the EU General Data Protection Regulation ("**GDPR**") means a natural person, whether living or deceased.

An "organisation" under the PDPA (which is the equivalent of a "controller" under the GDPR) includes any individual, company, association or body of persons, corporate or unincorporated, whether or not formed or recognised under Singapore law; or resident, or having an office or a place of business in Singapore.

A “data intermediary” under the PDPA (which is the equivalent of a “processor” under the GDPR) means an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation.

Cybersecurity

34. **Is there any specific definition of “*cybersecurity”* in your jurisdiction? Do the prevailing laws provide distinction between “*data protection*” and “*cybersecurity*”?**

“Cybersecurity” is defined under the Cybersecurity Act 2018 (Act 9 of 2018) (“**CSA**”) as the state in which a computer or computer system is protected from unauthorised access or attack, and because of that state the computer or computer system continues to be available and operational; the integrity of the computer or computer system is maintained; and the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained.

Generally speaking, “data protection” relates to the protection of personal data which is governed by the PDPA. Nevertheless, there are overlaps between the two concept given that the PDPA requires organisations to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and the loss of any storage medium or device on which personal data is stored.

35. **What are the subjects of cybersecurity? Does cybersecurity apply to certain industries and types of information?**

The CSA establishes a legal framework for the oversight and monitoring of Critical Information Infrastructures (“**CII**”) in Singapore. CIIs are computer systems directly involved in the provision of essential services and the CII sectors are: Energy, Water, Banking and Finance, Healthcare, Transport (which includes Land, Maritime, and Aviation), Info-communications, Media, Security and Emergency Services, and Government.

B. Governing Authority of Data Privacy and Cybersecurity

Data Privacy

36. **Is there any specific government agency that oversees data privacy legislation in your jurisdiction? Please define what powers and authorities such agency has in the data privacy enforcement?**

The Personal Data Protection Commission (“**PDPC**”) serves as Singapore’s main authority in matters relating to personal data protection. Broadly, the PDPC has the follow powers and authorities:

a) **Powers relating to alternative dispute resolution.** These powers generally relate to the manner by which a complainant and an organisation may by directed by the PDPC to resolve the complainant’s complaint, for example, through mediation or other modes of dispute settlement.

b) **Powers relating to reviews.** These powers enable the PDPC to review an organisation's reply to an access or correction request made by an individual and to confirm the organisation's reply or direct the organisation to take certain action in relation to the individual's request.

c) **Powers relating to investigations.** These powers enable the PDPC to carry out investigations to determine whether an organisation or person is complying with the PDPA and to direct an organisation or person that is not complying to take the appropriate action to ensure its compliance, or to pay a financial penalty.

d) **Powers relating to voluntary undertakings.** These powers enable the PDPC to accept a voluntary undertaking from an organisation or person including an undertaking to take specified action, where the organisation or person has not complied, is not complying or is likely not to comply with the PDPA. Further, if the organisation or person fails to comply with any undertaking, the PDPC may give any direction to ensure compliance with that undertaking

37. **Can the data protection authority in your jurisdiction cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?**

The PDPC is Singapore's main data protection authority. The PDPC has been known to pursue available options for assistance (e.g. assistance relating to its investigations) with the relevant foreign data protection authorities. These are reflected in some of its enforcement decisions in which the PDPC would refer certain issues to foreign data protection authorities. In addition, the PDPC has entered into memorandum of understandings with other jurisdictions including Australia and Hong Kong for the cross-sharing of experience, exchange of best practices, joint research projects and information exchange involving potential or ongoing data breach investigations.

Cybersecurity

38. **Is there any specific government agency that oversees cybersecurity legislation in your jurisdiction? Please define what powers and authorities such agency has in the cybersecurity enforcement?**

The Cyber Security Agency of Singapore ("**CSA**") is the government agency overseeing the CSA. As part of the CSA, the Commissioner of Cybersecurity has the power to investigate and prevent cybersecurity incidents including requiring any person to answer any question concerning a cybersecurity incident or produce any record or document which is in the possession of that person which the relevant incident response officer considers to be related to any matter relevant to the investigation.

39. **How does the cybersecurity authority cooperate with Data Protection Office ("DPO")? Does your jurisdiction provide certain guidelines for this matter?**

The CSA has worked with the PDPC to produce guides on protecting organisations' data from cyber threats, recognising a data breach and developing a data breach management plan. The CSA has also worked with the PDPC to develop a web portal containing a directory of cyber security and data protection service providers in Singapore. The directory serves as a resource for businesses seeking cyber security and data protection solutions and services in Singapore.

C. Regulatory Framework and Registration

Data Privacy

40. **What are the applicable laws and regulations that govern data privacy and personal data protection in your jurisdiction? Please identify further laws on data protection in specific sectors, if any.**

The PDPA is the law governing personal data protection in Singapore. The PDPA governs the collection, use and disclosure of individuals' personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances. For certain laws on data protection in specific sectors, please refer to question 32 above.

41. **Are there any exemptions under the data privacy and personal data protection rules in your jurisdiction?**

The PDPA does not apply to, or applies to a limited extent to, certain categories of personal data. The PDPA does not apply to the following types of data:

a) business contact information, which is defined as an individual's name, position name or title, business telephone number, business address, business email address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes;

b) personal data about an individual that is contained in a record that has been in existence for at least 100 years; and

c) personal data about an individual who has been dead for more than 10 years.

42. **Do the data privacy applicable laws and regulations apply extraterritorially? If <u>yes</u>, how do DPO and the government exercise such duties?**

Although the PDPA is not expressly stated to have extraterritorial effect, the provisions of the PDPA envisage its applicability to organisations outside of Singapore. An "organisation" is defined the PDPA as including any company whether or not formed or recognised under the law of Singapore; or resident, or having an office or a place of business, in Singapore. That being said, it is noted that the relevant government ministry has acknowledged that enforcement against organisations registered and located outside Singapore may be an issue.

43. **Is the registration of data controllers and processors mandatory in your jurisdiction? If <u>yes</u>, how is the registration procedure completed, and what are the consequences for failing to conduct the registration?**

The registration of data controllers and processors is not required in Singapore.

Cybersecurity

44. **Is there any specific laws and regulations that govern cybersecurity for data privacy and personal data in your jurisdiction?**

The PDPA, specifically section 24, requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control in order to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and the loss of any storage medium or device on which personal data is stored.

45. **Is there any specific threshold on the number of personal data subjects that requires a certain level of cybersecurity system?**

While there is no specific threshold on the number of personal data subjects that requires a certain level of cybersecurity system, the PDPC has stated in its guidelines that the amount and type of personal data an organisation holds should be considered in ascertaining whether its information security arrangements are adequate.

D. Data Processing

46. **What are the recognized, legitimate grounds of personal data processing in your jurisdiction?**

The PDPA adopts a "consent-first" regime. Unless an exception to consent is applicable, organisations are generally required to obtain the consent of an individual before collecting, using and/or disclosing the individual's personal data. Exceptions to the consent obligation are set out in the First and Second Schedules to the PDPA and include the legitimate interests exception and the business improvement exception which were introduced during the amendments to the PDPA which took effect from 1 February 2021.

47. **What are the key requirements (*such as notification or consent from the personal data subject*) when processing personal data in your jurisdiction?**

Under the Consent Obligation, an organisation must obtain the consent of the individual before collecting, using or disclosing his personal data for a purpose.

Under the Purpose Limitation Obligation, an organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances; and where applicable, that the individual has been informed of by the organisation.

Under the Notification Obligation, an organisation must inform individuals of the purposes for which their personal data will be collected, used and disclosed in order to obtain their consent. The organisation's collection, use and disclosure is limited to the purposes for which notification has been made to the individuals concerned.

48. **Are there other requirements, restrictions, and best practices that should be considered when processing personal data in your jurisdiction?**

Where an organisation engages a data intermediary to process personal data on its behalf, the PDPA states that the organisation has the same obligations under the PDPA in respect of personal data processed on its behalf by a

data intermediary as if the personal data were processed by the organisation itself. The organisation remains liable for any breach of the data protection provisions for any processing by a data intermediary on its behalf and for its purposes. As such, it is good practice for an organisation to undertake an appropriate level of due diligence to assure itself that a potential data intermediary is capable of complying with the PDPA.

E. Data Transfer

49. **What are the requirements that apply to a transfer of data to third parties?**

An organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA, i.e. to ensure that organisations provide a standard of protection to transferred personal data that is comparable to the protection under the PDPA.

The Personal Data Protection Regulations 2021 specify the conditions under which an organisation may transfer personal data overseas. In essence, an organisation may transfer personal data overseas if it has taken appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations or specified certifications to provide the transferred personal data a standard of protection that is comparable to that under the PDPA.

Legally enforceable obligations may be imposed in two ways. First, it may be imposed on the recipient organisation under:

a) any law;

b) any contract that imposes a standard of protection that is comparable to that under the PDPA, and which specifies 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 to provide a standard of protection for the transferred personal data that is comparable to that of the PDPA, and which specify (i) the recipients of the transferred personal data to which the binding corporate rules apply; (ii) the countries and territories to which the personal data may be transferred under the binding corporate rules; and (iii) the rights and obligations provided by the binding corporate rules; or

d) any other legally binding instrument.

Second, if the recipient organisation holds a "specified certification" that is granted or recognised under the law of that country or territory to which the personal data is transferred, the recipient organisation is taken to be bound by such legally enforceable obligations. Under the Personal Data Protection Regulations 2021, "specified certification" refers to certifications under the Asia Pacific Economic Cooperation Cross Border Privacy Rules ("**APEC CBPR**") System, and the Asia Pacific Economic Cooperation Privacy Recognition for Processors ("**APEC PRP**") System. The recipient is taken to satisfy the requirements under the Transfer Limitation Obligation if it is receiving the

personal data as an organisation and it holds a valid APEC CBPR certification; or it is receiving the personal data as a data intermediary and it holds either a valid APEC PRP or CBPR certification, or both.

50. **Are there restrictions that apply to a transfer of data abroad? Are there any exemptions on this matter?**

Please refer to the response to question 49 above.

51. **Do the prevailing law and regulations on cybersecurity provide certain requirements for a local data transfer? If yes, do they require certain methods or procedures for a data transfer?**

Please refer to the response to question 49 above.

F. Rights of Data Subject

52. **What are the rights of data subject in connection to personal data processing? Are there any exemptions to such rights? Please elaborate.**

The PDPA provides individuals the rights for request for access to their personal data ("**Access Request**") and for correction of their personal data ("**Correction Request**") that is in the possession or under the control of an organisation.

In addition, the PDPA provides that individuals may at any time withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose by an organisation.

In respect of exceptions to an Access Request, the PDPA provides that an organisation is not required to provide individuals with the personal data or other information in respect of the matters specified in the Fifth Schedule to the PDPA. An organisation is not prohibited from providing information in respect of the matters specified in the Fifth Schedule and may do so if it decides to.

Regarding exceptions to a Correct Request, an organisation is not required to correct or otherwise alter an opinion, including a professional or an expert opinion. In addition, the PDPA provides that an organisation is not required to make a correction in respect of the matters specified in the Sixth Schedule to the PDPA.

53. **Is there any procedure for data subjects to exercise their rights in your jurisdiction?**

The PDPA provides that upon an Access Request by an individual, an organisation must provide the individual with the following as soon as reasonably possible: personal data about the individual that is in the possession or under the control of the organisation; and information about the ways in which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request.

With regard to a Correction Request, unless the organisation is satisfied on reasonable grounds that the correction should not be made, it should correct the personal data as soon as practicable; and send the corrected personal

data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction request was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.

54. **What remedies are available to data subjects in case of a breach of their rights?**

An individual may submit a complaint to the PDPC and the PDPC may review or investigate an organisation's conduct and compliance with the PDPA.

G. Data Protection Officer

55. **Is the appointment of a Data Protection Officer ("DPO") mandatory in your jurisdiction? If yes, what are the consequences of failing to appoint the officer?**

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.

Failure to appoint a DPO may result in the PDPC finding the organisation to be in breach of the Accountability Obligation under the PDPA.

56. **What are the key responsibilities of a DPO in your jurisdiction?**

The responsibilities of the DPO often include working with senior management and the organisation's business units to develop and implement appropriate data protection policies and practices for the organisation. In addition, the DPO would undertake a wide range of activities, which may include 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 with (or have additional responsibilities relating to) the organisation's data governance and cybersecurity functions

I. Data Breach

57. **Is it mandatory to provide a notification in the event of a data breach? If yes, who must be notified (i.e., the data protection authority, the data subject, etc.) and what kind of information must be provided?**

The PDPA requires that 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, an assessment of whether the data breach is a "notifiable data breach". If the organisation assesses that the data breach is a notifiable one, it is required to notify the affected individuals and/or the PDPC.

Information to be provided in the organisation's notification to the PDPC must include the facts of the data breach, a chronological account of the steps taken by the organisation after the organisation became aware that the data breach had occurred, and the contact details of at least one authorised representative of the organisation.

Information to be provided in the organisation's notification to the affected individuals should include the facts of the data breach, information on any action by the organisation, whether taken before or to be taken after the organisation notifies the affected individuals to eliminate or mitigate any potential harm to the affected individuals as a result of the notifiable data breach, and the contact details of at least one authorised representative of the organisation.

58. **Are companies required to share details of actual or potential cybersecurity threats, or other cyber-intelligence information, with industries or other stakeholders? If yes, what kind of information must be shared?**

Where an organisation is required to notify a sectoral regulator or law enforcement agency of a data breach under other written laws, the organisation must notify that sectoral regulator or law enforcement agency accordingly. Additionally, it must also notify the PDPC and affected individuals (if required) according to the timeframes for data breach notification under the PDPA. The information to be provided to the sector regulator or law enforcement agency would very much depend on the breach notification requirements set out under other applicable written laws.

59. **How would a breach of data protection be handled by the authority? Can such breach lead to administrative sanctions or criminal penalties?**

In general, the PDPC may commence an investigation either upon receiving a complaint from an individual against an organisation or of its own motion. Where the PDPC receives a complaint or other information that indicates that an organisation has, or may have, contravened the PDPA, the PDPC will first consider whether the matter may be more appropriately resolved by alternative dispute resolution in order to resolve the underlying dispute between the complainant and the organisation.

The PDPC may commence an investigation into the conduct of an organisation if the PDPC considers that an investigation is warranted, based on the information it has obtained (whether through a complaint or from any other source). In deciding whether to commence an investigation, the PDPC will generally consider the following non-exhaustive factors:

a) whether the organisation may have failed to comply, whether intentionally, negligently or for any other reason or cause, with all or a significant part of its obligations under the PDPA;

b) whether the organisation's conduct indicates a systemic failure by the organisation to comply with the PDPA or to establish and maintain the necessary policies and procedures to ensure its compliance;

c) the number of individuals who are, or may be, affected by the organisation's conduct;

d) the impact of the organisation's conduct on the complainant or any individual who may be affected including, for example, whether the complainant or affected individual(s) may have suffered a loss, injury or other damage

as a result of the organisation's contravention of the PDPA or whether they may have been exposed to a significant risk that they may suffer such a loss, injury or damage; and/or

e) whether the organisation had previously contravened the PDPA or may have failed to implement the necessary corrective measures to prevent the recurrence of a previous contravention.

Upon determining that an organisation is in breach of the provisions of the PDPA, the PDPC may direct an organisation or person that is not complying to take the appropriate action to ensure its compliance, or to pay a financial penalty.

60. **What other requirements, restrictions, and best practices should be considered in the event of a data breach?**

The strategy for containing, assessing and managing data breaches would include roles and responsibilities of the employees and data breach management team. Organisations may consider preparing contingency plans for possible data breach scenarios and measures to be taken or run regular breach simulation exercises to better prepare themselves to respond to data breaches in a prompt and effective manner. The PDPC has published a guide on managing and notifying data breaches under the PDPA which can be found on its website.

CLYDE&CO
CLASIS SINGAPORE
A joint law venture

Thomas Choo

Thomas.Choo@clydeco.com

Zhen Guang Lam

Zhenguang.Lam@clydeco.com

Marina Boulevard | Marina Bay Financial Centre Tower 3 | #30 - 03 | Singapore 018982
+65 6544 6500
www.clydeco.com