Indonesia


Denny Rahmansyah


Raoul Aldy Muskitta

SSEK Indonesian Legal Consultants

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal law governing data protection in Indonesia is Law No. 11 of 2008 regarding Electronic Information and Transactions (April 21, 2008), as amended by Law No. 19 of 2016 (November 25, 2016) ("**Electronic Information Law**"). In addition to the Electronic Information Law, rules governing personal data protection are also found in Government Regulation No. 71 of 2019 regarding the Implementation of Electronic Systems and Transactions (October 10, 2019) ("**GR 71**") and Minister of Communication and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data (December 1, 2016) ("**MOCI Reg. 20**"). The Electronic Information Law, GR 71, and MOCI Reg. 20 are hereinafter collectively referred to as the "**PDP Regulations**".

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

The PDP Regulations are the primary regulations governing the protection of personal data in Indonesia.

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

Law No. 36 of 2009 regarding Health (October 13, 2009) stipulates that, in principle, every person is entitled to the confidentiality of their personal health information that has been provided to or collected by healthcare providers.

Financial Services Authority (*Otoritas Jasa Keuangan* or "**OJK**") Regulation No. 1/POJK.07/2013 regarding Financial Consumer Protection (August 6, 2013), as last amended by OJK Regulation No. 18/POJK.07/2018 (September 10, 2018) ("**OJK Reg. 1**"), prohibits financial service providers from disclosing customer data and/or information to third parties, unless they receive written consent from the customer or are required to make such disclosure by law. Where a financial service provider obtains the data and/or personal information of a person or a group of persons from a third party, it is required to obtain written confirmation from the third party that the person or group of persons has agreed to the disclosure.

Law No. 36 of 1999 regarding Telecommunications (September 8, 1999) prohibits the tapping of information transmitted through telecommunications networks. Telecommunications service operators must maintain the confidentiality of any information transmitted and/or received by a telecommunications subscriber through a telecommunications network and/or telecommunications service provided by the respective operator.

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

The Minister of Communication and Informatics ("**MOCI**") is responsible for monitoring and regulating data protection. Additionally, certain other government agencies may oversee data protection for their respective sectors, such as the OJK for financial service providers and the Ministry of Health for healthcare providers.

2 Definitions

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

- "**Personal Data**"
  The definition of personal data has evolved throughout the enactment of the PDP Regulations. MOCI Reg. 20 defines personal data as certain personal data that is stored and/or cultivated, with its accuracy maintained and confidentiality protected. GR 71 further defines personal data as any data relating to a person that is identified and/or is self-identifiable, or is combined with other information, directly or indirectly, through electronic and non-electronic systems.
- "**Processing**"
  The definition of processing is found in GR 71 and includes (a) obtainment and collection, (b) processing and analysis, (c) storage, (d) reparation and renewal, (e) display, announcement, transfer, dissemination, or disclosure, and/or (f) erasure or deletion. MOCI Reg. 20 does not define processing but requires the obtainment of consent from data subjects for (a) obtainment and collection, (b) processing and analysis, (c) storage, (d) display, announcement, transfer, dissemination, or disclosure, and (e) deletion.
- "**Controller**"
  The PDP Regulations do not provide a clear definition of controller or their role and responsibilities. The PDP Regulations instead refer to an Electronic System Provider ("**ESP**") as the party controlling and managing the use of personal data. Please see our discussion of ESPs below. Certain provisions in GR 71 refer to the term "Personal

Data controller" in the context of lawful bases to process personal data, in addition to consent. Unfortunately, GR 71 does not further define controller. Please see our response to 4.1.

- "**Processor**"
  The PDP Regulations do not recognise the concept of processor. The PDP Regulations instead refer to an ESP as the party controlling and managing the use of personal data. Please see our discussion of ESPs below. Unlike controllers, the PDP Regulations make no reference to processors.
- "**Data Subject**"
  The PDP Regulations do not define data subject. Rather, they use the term personal data owner. Please see the definition of Personal Data Owner below.
- "**Sensitive Personal Data**"
  The PDP Regulations do not recognise the concept of sensitive personal data.
- "**Data Breach**"
  The PDP Regulations do not define data breaches, although they do accommodate certain reporting and dispute resolution mechanisms pertaining to data breaches. Please refer to our discussion of data security and breaches in Section 15 below.

Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")

- "**ESPs**"
  The PDP Regulations define an ESP as a person, state administrator, business entity, or community that provides, manages, and/or operates an electronic system, individually or jointly, to or for electronic system users for their own or another party's benefit. ESPs are further divided between Private Scope ESPs and Public Scope ESPs, as further defined below.
- "**Personal Data Owner**"
  MOCI Reg. 20 defines Personal Data Owner as the individual to which personal data is attached.
- "**Electronic Systems**"
  The PDP Regulations define Electronic Systems as a series of devices and electronic procedures that function to prepare, collect, process, analyse, store, display, announce, transmit, and/or disseminate electronic information (which includes personal data).
- "**Private Scope ESPs**"
  GR 71 defines Private Scope ESPs as individuals, business entities, and communities that provide electronic systems.
- "**Public Scope ESPs**"
  GR 71 defines Public Scope ESPs as state administrative agencies, legislative, executive, and judicial institutions at the central and regional government level and other agencies which are formed by virtue of laws and regulations, and institutions appointed by state administrative agencies. The latter refers to institutions providing an electronic system with a public scope on behalf of the appointing state administrative agency. GR 71/2019 excludes Public Scope ESPs that have a regulatory and supervisory authority in the financial sector.
- "**Electronic Certificates**"
  As defined by GR 71, an Electronic Certificate contains a digital signature and identity that shows the legal status of the parties in an electronic transaction and is issued by an Electronic Certification Provider.
- "**Electronic Certification Provider**"
  Electronic Certification Provider is a legal entity that functions as a trustworthy party and which issues and audits Electronic Certificates.

3 Territorial Scope

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

Article 2 of the Electronic Information Law provides that it has an extraterritorial scope if the actions of individuals outside of Indonesia have a legal implication within the territory of Indonesia or if they adversely affect Indonesian interests. On a plain reading of the above provision, the Electronic Information Law may apply to breaches of personal data outside of Indonesia to the extent the effect concerns the personal data of Indonesian data subjects. However, we have not seen the government apply the PDP Regulations to entities outside of Indonesia.

4 Key Principles

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

- **Transparency**
  The PDP Regulations do not expressly identify transparency as a key principle, but the principle of transparency is reflected in certain obligations that apply to ESPs. For example, ESPs must notify data subjects of data breaches within 14 days after the discovery of such breach. We further elaborate on this requirement below.
- **Lawful basis for processing**
  The PDP Regulations mandate the obtainment of consent for any processing of personal data. In addition to consent, GR 71 stipulates other lawful bases other than consent for processing personal data, which are: (1) processing an individual's personal data in order to satisfy the obligations of a contract or to fulfil the request of such personal data owner when concluding an agreement; (2) the fulfilment of the legal obligation of the personal data controller in line with the applicable laws and regulations; (3) guarding the vital interest of the personal data owner; (4) performing the legal obligation of the personal data controller; (5) performing the obligation of a public service personal data controller in the interest of the public; and (6) satisfying another valid interest of the personal data controller and/or the personal data owner. Note, however, that the wording used in the relevant clause regarding lawful bases is rather ambiguous and may be interpreted to mean that consent is still required despite the existence of these lawful bases.
  As we explain above, although GR 71 uses the term "data controller" to define the above lawful bases, it provides no further guidance on the legal obligations of the data controller or their role and responsibilities. Moreover, GR 71 and the PDP Regulations do not define data processors or distinguish them from data controllers. Therefore, we understand that "data controllers" above primarily refer to ESPs.
- **Purpose limitation**
  MOCI Reg. 20 provides that one of the key forms of personal data protection is that the processing of personal data must be in accordance with the original purpose of its processing. Further, GR 71 provides that ESPs must disclose the purpose of their processing of personal data to the data subjects.

- **Data minimisation**
  MOCI Reg. 20 provides that ESPs may only use the personal data of data subjects in accordance with the needs of the data subjects. Further, GR 71 provides that ESPs must put in place a mechanism that accommodates the deletion of personal data if it has outlived its relevance.
- **Proportionality**
  The PDP Regulations do not address the proportionality principle.
- **Retention**
  MOCI Reg. 20 provides that ESPs must retain personal data for a minimum period of five years unless stipulated otherwise by sectoral regulations. Data may be retained beyond the five-year period if it is to be used in accordance with its initial purpose.

5 Individual Rights

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

- **Right of access to data/copies of data**
  The PDP Regulations acknowledge the right of data subjects to have adequate access to their personal data. The PDP Regulations also acknowledge the right of data subjects to obtain copies of their personal data submitted to ESPs.
- **Right to rectification of errors**
  The PDP Regulations acknowledge the right of data subjects to alter and renew their personal data, to the extent that such alteration and renewal does not disturb the management of the personal data by ESPs.
- **Right to deletion/right to be forgotten**
  The PDP Regulations acknowledge the right of data subjects to have their personal data deleted. GR 71 provides that the right to erasure applies to personal data: (1) that is acquired and processed without the consent of the personal data owner; (2) for which consent has been withdrawn by the data subject; (3) that is obtained and processed illegally; (4) that is no longer in accordance with the purpose for which it was obtained based on an agreement and/or laws and regulations; (5) whose utilisation has exceeded the period in accordance with an agreement and/or laws and regulations; and/or (6) that is displayed by the ESP and caused a loss for the data subject.
- **Right to object to processing**
  The PDP Regulations do not address the right to object to processing.
- **Right to restrict processing**
  The PDP Regulations do not address the right to restrict processing.
- **Right to data portability**
  The PDP Regulations do not address the right to data portability.
- **Right to withdraw consent**
  GR 71 acknowledges the right of data subjects to withdraw consent for all data processing activities by ESPs.
- **Right to object to marketing**
  The PDP Regulations do not address the right to object to marketing.
- **Right to complain to the relevant data protection authority(ies)**
  MOCI Reg. 20 acknowledges the right of data subjects to complain to MOCI for the failure of an ESP to protect personal data. Data subjects may submit a written complaint to the Directorate General of Application of Informatics ("**DGAI**") at the Ministry of Communication and Informatics ("**Ministry**") within 30 business days from the discovery of the failure to protect the personal data of the data subject. If a violation is found, the DGAI may recommend that MOCI impose certain administrative sanctions on the ESP.

Other key rights – please specify

- **Right to delisting**
  GR 71 acknowledges the right of data subjects to have their personal data removed from search engines provided that they are no longer "relevant", based on a court order. The PDP Regulations do not elaborate on when personal data is considered "irrelevant". Nonetheless, we are of the view that the same rationale as to why data subjects may have their data erased if they withdraw consent should apply here.

6 Registration Formalities and Prior Approval

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

Yes. GR 71 requires both Public Scope ESPs and Private Scope ESPs to be registered with MOCI through the Online Single Submission ("**OSS**") system. This registration must be done before the electronic system can be used. However, as of this writing we have not seen ESPs follow this registration requirement in practice, nor has it been enforced by the Ministry. Unlike Public Scope ESPs, which can only process electronic data (including personal data) within the territory of Indonesia, Private Scope ESPs may carry out data processing activities outside of Indonesia, provided they ensure the effectiveness of oversight by the Ministry or other relevant government agencies. Further, certain coordination requirements apply to Private Scope ESPs transferring data outside of Indonesia, as we further elaborate in our response to question 11.1 below. However, this does not entail a notification requirement. Nonetheless, we have also not seen this requirement implemented in practice.

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

The PDP Regulations do not regulate the form of registration and/or notification. In our current view, a general description of the relevant data processing activities should be sufficient.

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

The PDP Regulations also do not go into detail on this matter. As indicated above, they do emphasise the obligation to register with and/or notify the Ministry on a 'per legal entity' basis (i.e., for each ESP).

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

GR 71 provides that ESPs must register with MOCI through the OSS system. We are not aware of any foreign legal entity being required by MOCI to register through the OSS system.

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

The PDP Regulations do not address the details that must be included in the registration/notification.

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

The sanctions under GR 71 and MOCI Reg. 20 may apply for failure to register/notify where required. GR 71 regulates administrative sanctions for failure to register with the Ministry, which include: (1) written warnings; (2) administrative fines; (3) temporary suspension; (4) termination of access to the ESP's electronic system; and/or (5) blacklisting. MOCI Reg. 20 stipulates the following administrative sanctions: (1) written warnings; (2) administrative fines; (3) temporary suspension; and/or (4) announcement of such failure on the Ministry's website. Although the sanctions under GR 71 and MOCI Reg. 20 differ somewhat, both are equally enforceable by MOCI.

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

There is no fee for an ESP's registration with MOCI through the OSS system. Any registration through the OSS system is in principle free of charge.

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

The PDP Regulations do not address this matter, but we presume that ESP registration with MOCI through the OSS system is done once.

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

No, except for Public Scope ESPs that wish to carry out data processing activities outside of Indonesia. In such case, Public Scope ESPs must prove that the relevant data processing technology is not available in Indonesia and subsequently obtain approval from MOCI.

6.10 Can the registration/notification be completed online?

Yes, as we have explained above, ESP registration is primarily done online through the OSS system.

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

No, there is not.

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

As we are not aware of the requirement to register with MOCI through the OSS system actually being implemented and enforced, we are unsure as to the time required for such registration to be completed.

7 Appointment of a Data Protection Officer

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

The PDP Regulations do not recognise the concept of a Data Protection Officer. Therefore, appointing a Data Protection Officer is not mandatory under Indonesian law. However, MOCI Reg. 20 does require that individuals be informed of the contact details of a designated contact person for enquiries into an ESP's data processing activities. The PDP Regulations do not specifically regulate sanctions for failure to comply with this requirement.

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

Please refer to our response to question 7.1.

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

Please refer to our response to question 7.1.

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

Please refer to our response to question 7.1.

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

Please refer to our response to question 7.1.

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

Please refer to our response to question 7.1.

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

Please refer to our response to question 7.1.

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

Please refer to our response to question 7.1.

8 Appointment of Processors

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

As explained above, the PDP Regulations do not distinguish between data processors and data controllers, and instead use the term ESP. Therefore, there are no requirements pertaining to the appointment of data processors by data controllers.

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

Please refer to our response to question 8.1.

9 Marketing

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

As explained above, OJK Reg. 1 prohibits financial service providers from disclosing customer data and/or information to third parties, unless they receive written consent from the customer or are required to by law. Where a financial service provider obtains the data and/or personal information of a person or a group of persons from a third party, it is required to obtain written confirmation from the third party that the person or group of persons has agreed to the disclosure. The above rules commonly apply to unsolicited ads or marketing communications by email, and to telemarketing telephone calls or text messages.

We are not aware of any other rules pertaining to the sending of electronic direct marketing.

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

The above restrictions only apply in a business-to-consumer relationship. We are not aware of any rules applicable in a business-to-business context.

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

We are not aware of any legislative restrictions other than those discussed in our response to question 9.1.

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

No. The rules under OJK Reg. 1 do not apply extraterritorially.

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

Although the OJK is active in its enforcement of violations committed by financial service providers (e.g., banks, insurance companies, securities companies, etc.), we are not aware of any cases where the OJK has sanctioned financial service providers for violations pertaining to electronic direct marketing.

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

No, the purchase of marketing lists from third parties is not lawful. However, the PDP Regulations and other Indonesian laws do not stipulate sanctions for violations committed by legal entities not considered to be ESPs or financial service providers, or legal entities in other sectors that are subject to sectoral data protection rules. Nonetheless, certain criminal sanctions under the Electronic Information Law may still apply to individuals who commit violations. These sanctions are: (1) fines of IDR600 million to IDR800 million and/or four to eight years' imprisonment for unlawful access; (2) fines of IDR800 million to IDR1 billion and/or six to 10 years' imprisonment for interception/wiretapping of transmission; (3) fines of IDR2 billion to IDR5 billion and/or eight to 10 years' imprisonment for the alteration, addition, reduction, transmission, tampering, deletion, moving, or hiding of electronic information and/or electronic records; (4) fines of IDR10 billion to IDR12 billion and/or 10 to 12 years' imprisonment for the manipulation, creation, alteration, destruction or damage of electronic information and/or electronic documents with a purpose of creating an assumption that such electronic information and/or documents are authentic, and other violations related to the processing of electronic information and/or documents.

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

For violations committed by ESPs under the PDP Regulations and financial service providers under OJK Reg. 1, sanctions range from a written warning and fines to the limitation of business activities, suspension of business activities, and revocation of business licence. As for criminal sanctions that apply to individuals, please refer to our response to question 9.6.

10 Cookies

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

Please note that the PDP Regulations do not regulate the use of cookies.

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

Please refer to our response to question 10.1.

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

Please refer to our response to question 10.1.

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

Please refer to our response to question 10.1.

11 Restrictions on International Data Transfers

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

As discussed above, the PDP Regulations do not restrict international data transfers, except for Public Scope ESPs. However, MOCI Reg. 20 requires that the transfer of data overseas be done in coordination with the Ministry. This coordination entails:

(1) Reporting the plan to transfer the personal data. At a minimum, the report must include:
   (a) the name of the destination country;
   (b) the name of the receiving party;
   (c) the date of the transfer; and
   (d) the reason/purpose of the transfer.
(2) Requesting the assistance of the MOCI for the transfer (if required).
(3) Reporting the result of the transfer.

However, the Ministry has never provided procedures to implement this coordination with MOCI. To the best of our knowledge, very few business players have, of their own volition, attempted to comply with the coordination obligation. The Ministry has also never sought to enforce the rule, which for the time being is widely disregarded in practice.

MOCI Reg. 20 further stipulates that the transferring entity would need to apply the laws and regulations on the cross-border exchange of personal data. However, since Indonesia has yet to issue any laws or regulations on the cross-border exchange of personal data, it is currently not possible for an ESP to comply with this requirement. As a result, ESPs are not, in practice, required to fulfil this requirement.

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

Obtaining the consent of data subjects, via consent to a privacy policy, is still the most common way to transfer data abroad. Although there are certain lawful bases aside from consent to process personal data, as discussed above, we have not seen their application in practice.

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

Please refer to our response to question 11.1.

12 Whistle-blower Hotlines

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

The PDP Regulations do regulate corporate whistle-blowers. Therefore, there are currently no restrictions on the permitted scope and form of corporate whistle-blower reports.

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

Please refer to our response to question 12.1.

13 CCTV

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

We are not aware of any regulation requiring the prior registration, notification or approval and/or any specific form of public notice for the use of CCTV.

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

Please refer to our response to question 13.1.

14 Employee Monitoring

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

The PDP Regulations do not regulate this matter. We are also not aware of any other regulations on employee monitoring.

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

Considering that the concept of employee monitoring is not recognised under the PDP Regulations or any other Indonesian laws or regulations, and to the extent the employer qualifies as an ESP and processes the personal data of employees, who may be considered to be data subjects, consent is required.

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

The PDP Regulations and Indonesian manpower laws do not regulate this matter.

15 Data Security and Data Breach

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

The PDP Regulations provide that ESPs have the obligation to keep data secure. As we have discussed above, MOCI Reg. 20 mandates ESPs to notify data subjects in writing within 14 days after the discovery of their failure to protect personal data. GR 71 affirms this obligation and further provides that ESPs must have security procedures and infrastructure in place to prevent disruptions, failures and damage within electronic systems. GR 71 does not go into further detail as to the minimum measures required for such security procedures and infrastructure. It simply says that a separate regulation will be issued to govern the minimum cybersecurity measures. To date, no such regulation has been issued.

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

No. Generally, the PDP Regulations do not obligate ESPs to notify either the Ministry or MOCI of a data breach, except for "serious data breaches caused by third parties", as provided by GR 71. Neither GR 71 nor the PDP Regulations provide further guidance on how the above phrase is defined. However, based on our unofficial confirmation with officials from the Ministry, the Ministry expects to be notified of any data breach. To the best of our knowledge, however, there are very few cases where MOCI has demanded to be notified of a data breach. The most recent data breach involved the personal data of approximately 150,000 Indonesian data subjects managed by a large private low-cost airline. Admittedly, the Indonesian entity of the airline did not manage the leaked personal data, and thus was not considered to be an ESP under the PDP Regulations. In a press release dated September 19, 2019, the Ministry did not indicate that it would enforce the sanctions under the PDP Regulations, and simply requested that measures be taken by the airline to protect the personal data of the Indonesian data subjects. A similar sentiment was expressed by the Ministry when the personal data of approximately one million Indonesian data subjects leaked through a major social media platform in 2018. Although the Ministry expressed concern over the leak, it did not conclude whether the leak was in violation of the PDP Regulations and that sanctions thereunder were applicable.

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

Yes. Please refer to our response to question 15.1. Please note that the PDP Regulations do not prescribe the form of reporting. MOCI Reg. 20 simply provides that if a data breach occurs, data subjects are entitled to be informed of the cause of the breach and any potential damages.

15.4 What are the maximum penalties for data security breaches?

Please refer to our response to question 9.6.

16 Enforcement and Sanctions

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

Investigatory/ Enforcement Power	Civil/Administrative Sanction	Criminal Sanction
MOCI or other ministries in accordance with the jurisdiction and/or government agencies and institutions.	The PDP Regulations each stipulate different sanctions. The Electronic Information Law regulates criminal sanctions while GR 71 and MOCI Reg. 20 only stipulate administrative sanctions. The administrative sanctions under GR 71 and MOCI Reg. 20 also differ. Nonetheless, the sanctions stipulated thereunder are equally enforceable by MOCI. The administrative sanctions under GR 71 are: (1) written warnings; (2) administrative fines; (3) temporary suspension; (4) termination of access to the ESPs electronic system; and/or (5) blacklisting. The administrative sanctions under MOCI Reg. 20 are: (1) written warnings; (2) administrative fines; (3) temporary suspension; and/or (4) announcement on the Ministry's website. Both MOCI Reg. 20 and GR 71 provide that the above sanctions may be enforced by MOCI or by other ministries and/or government agencies depending on the subject committing the violation, in coordination with MOCI. For example, violations of data protection rules under OJK Reg. 1 shall be enforced by the OJK, in coordination with MOCI.	Not applicable.

Investigatory / Enforcement Power	Civil/Administrative Sanction	Criminal Sanction
The Indonesian National Police	Not applicable.	Sanctions for criminal violations are stipulated under the Electronic Information Law. They are: (1) Fines of IDR600 million to IDR800 million and/or four to eight years' imprisonment for unlawful access; (2) fines of IDR800 million to IDR1 billion and/or six to 10 years' imprisonment for interception/wiretapping of transmission; (3) fines of IDR2 billion to IDR5 billion and/or eight to 10 years' imprisonment for the alteration, addition, reduction, transmission, tampering, deletion, moving, or hiding of electronic information and/or electronic records; and (4) fines of IDR10 billion to IDR12 billion and/or 10 to 12 years' imprisonment for the manipulation, creation, alteration, destruction, or damage of electronic information and/or electronic documents with a purpose of creating an assumption that such electronic information and/or documents are authentic, and other violations related to the processing of electronic information and/or documents.

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

The enforcement of bans under the PDP Regulations falls under the jurisdiction of MOCI, in the form of blacklisting or temporary/permanent suspension of access (i.e. access to the electronic system of the ESP). Neither GR 71 nor MOCI Reg. 20 require a court order for the enforcement of these bans. GR 71 only requires court orders to be obtained if data subjects wish to exercise their right to delisting.

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

Criminal sanctions for breaches of the Electronic Information Law are commonly enforced in Indonesia. However, these mostly involved cases of slander done through electronic systems, and do not concern violations of personal data processing rules. To the best of our knowledge, MOCI rarely enforces the above administrative sanctions.

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

No. As explained above, although the Electronic Information Law provides that it may apply extraterritorially, we have not heard of any case where MOCI or the Ministry has sought to enforce the PDP Regulations extraterritorially.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

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

To the best of our knowledge, we have not heard of foreign e-discover requests being made by foreign law enforcement agencies to ESPs in Indonesia.

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

To the best of our knowledge, we are not aware of any guidelines issued by MOCI or the Ministry in response to foreign e-discovery requests.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

As discussed above, the Ministry expressed concern over the leak of the personal data of approximately 150,000 Indonesian data subjects, managed by one of the largest private Indonesian low-cost airlines. We have not heard of enforcement measures being carried out by the Ministry in this case, but we understand that the Ministry has been actively trying to investigate the case and seek mitigation measures. Similarly, and as explained above, the Ministry expressed a similar sentiment when the personal data of approximately one million Indonesian data subjects leaked through a major social media platform in 2018. Although the Ministry expressed concern of such leakage, it did not conclude whether the leakage was in violation of the PDP Regulations and that sanctions thereunder were applicable.

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

The Indonesian House of Representatives (*Dewan Perwakilan Rakyat* or "**DPR**") is currently in the process of finalising the Draft Data Protection Bill (the "**Draft Bill**"), which has been included by the DPR in the National Legislation Program for 2020. The National Legislation Program is a compilation of the top 50 draft bills that the DPR aims to ratify during the current five-year term of DPR members. However, despite being included in the National Legislation Program, there is no certainty as to when the Draft Bill will be passed into law. President Joko Widodo approved the most recent version of the Draft Bill, which was updated in December 2019, on January 24, 2020. In a recent statement, the MOCI, Johnny G. Plate, indicated that the government was "optimistic" that the Draft Bill would be ratified this year.

The current Draft Bill heavily resembles the EU's General Data Protection Regulation ("**GDPR**"). In brief, the Draft Bill is intended to clarify the scope of personal data, the roles and responsibilities of data controllers, data processors and data protection officers, and acknowledges most, if not all, of the rights of data subjects under the GDPR, and the general principles on consent to data processing.

Denny Rahmansyah is managing partner of SSEK Indonesian Legal Consultants. His key practice areas are IT and telecommunications, including extensive experience advising clients on data privacy and data protection regulations in Indonesia, banking and finance, foreign investment, general commercial and corporate law, M&A, real estate and property. Denny has advised several multinationals and Fortune 500 companies on data protection and data privacy issues. Denny was quoted extensively in an article on the data privacy scandal involving Facebook, in which more than one million Indonesian Facebook users were affected, and in an article by *MLex Market Insight*, a subscription-only service that analyses regulatory risk around the world, on Indonesia's draft protection bill.

SSEK Indonesian Legal Consultants
Mayapada Tower I, 14th Floor
Jl. Jend. Sudirman Kav. 28
Jakarta 12920
Indonesia

Tel: +62 21 521 2038
+62 21 2953 2000
Email: dennyrahmansyah@ssek.com
URL: www.ssek.com

Raoul Aldy Muskitta joined SSEK in 2016 after having worked as an assistant researcher at the Center for International Law Studies. Raoul has been involved in a variety of projects at SSEK, with a focus on data protection and data privacy matters, M&A transactions and the establishment of foreign capital investment entities. He also has been involved in a number of legal due diligence projects. Raoul is fluent in English and Indonesian.

SSEK Indonesian Legal Consultants
Mayapada Tower I, 14th Floor
Jl. Jend. Sudirman Kav. 28
Jakarta 12920
Indonesia

Tel: +62 21 521 2038
+62 21 2953 2000
Email: raoulmuskitta@ssek.com
URL: www.ssek.com

SSEK Indonesian Legal Consultants was established in 1992 and has more than 27 years of experience working with clients in Indonesia and helping them achieve their business and investment goals. SSEK is a full-service commercial law firm and works with domestic and global corporates on the largest, most complex projects and transactions across all sectors in Indonesia. The firm's telecommunications and IT practice, which includes its data protection team, advises corporate clients on data protection matters as they relate to the collection, use and storage of data.

SSEK is regularly recognised by independent legal publications as a leading law firm in every major practice area. SSEK is a six-time *Who's Who Legal* Indonesia Law Firm of the Year, has twice been named Indonesia Law Firm of the Year by *Chambers and Partners* and has been an Asian-MENA Counsel Law Firm of the Year every year since 2009.

SSEK combines an unsurpassed insight into Indonesian corporate law with the global outlook of its award-winning lawyers to offer clients innovative and timely solutions to their real-world problems.

www.ssek.com

SSEK
Indonesian Legal Consultants