International
Comparative
Legal Guides

Practical cross-border insights into data protection law

Data Protection 2023

10th Edition

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

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Q&A Chapters Continued

Indonesia


Abadi Abi Tisnadisastra


Prayoga Mokoginta

ATD Law in association with
Mori Hamada & Matsumoto

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The main legislation for personal data protection in Indonesia is Law No. 27 of 2022 on Personal Data Protection ("**PDP Law**"), which was enacted on October 17, 2022. The PDP Law serves as a comprehensive regulatory framework for personal data processing activities, applicable to all types of businesses, industries and organisations, whether private or public.

While the PDP Law applies to all data processing activities, other laws and regulations (see questions 1.2 and 1.3) may provide additional or more stringent provisions for specific types of data processing that fall under the scope of such regulations insofar as they do not contradict with the provisions set out under the PDP Law.

The PDP Law is currently in effect, with a two-year adjustment period for Controllers or Processors, and full enforcement of its provisions is still subject to the issuance of 11 implementing regulations mandated under the PDP Law.

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

Yes, there are several other laws that address personal data in various contexts, among others:

a. Electronic Information and Transaction ("**EIT**") regulatory framework: Law No. 11 of 2008 on EIT as amended by Law No. 19 of 2016 ("**EIT Law**"), Government Regulation No. 71 of 2019 on the Operation of Electronic System and Transaction ("**GR 71/2019**"), and Minister of Communication and Informatics Regulation No. 20 of 2016 on Data Protection in Electronic System ("**MOCI Reg. 20/2016**");
b. Law No. 36 of 1999 on Telecommunication (the "**Telecommunication Law**") as amended by Government Regulation in Lieu of Law No. 2 of 2022 on Job Creation, as stipulated to become a law under Law No. 6 of 2023 (the "**New Job Creation Law**");
c. Law No. 7 of 1992 on Banking as lastly amended by Law No. 4 of 2023 on Financial Sector Development and Strengthening;
d. Law No. 36 of 2009 on Health as amended by the New Job Creation Law and the relevant regulation on medical records; and
e. Law No. 1 of 2023 on Criminal Code, which stipulates criminal acts pertaining to data, e.g., data falsification and data theft.

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

Yes, there are several sector-specific regulations that contain personal data protection provisions, including:

a. the Financial Services Authority ("**OJK**") Regulation No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector and its implementing regulation, namely OJK Circular Letter No. 12/SEOJK.07/2014 of 2014 on the Delivery of Information for Marketing of Financial Products and/or Services (both, "**OJK Consumer Protection Regulations**"), which apply to the protection of consumers' personal data within the financial services sector;
b. the Bank Indonesia ("**BI**") Regulation No. 22/20/PBI/2020 on BI's Consumer Protection and its implementing regulation, namely BI Regulation No. 23/17/PADG/2021 on the Implementation Procedure of BI's Consumer Protection (both, "**BI Consumer Protection Regulations**"), which apply to the protection of consumers' personal data within the payment system sector;
c. the OJK Regulation No. 10/POJK.05/2022 on Information Technology-Based Collective Financing Services which applies to the protection of consumers' data within the peer-to-peer lending sector; and
d. the OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovations in the Financial Services Sector, which applies to the protection of consumers' data within financial-technology sector businesses under the supervision of the OJK.

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

At the moment, Indonesia is in the process of establishing a national data protection authority ("**Indonesian DPA**"), as mandated by the PDP Law. Once established, this authority will be the main authority for: (i) formulation and stipulation of policies and strategies for personal data protection; (ii) supervision on the operation of data protection; (iii) enforcement of violations of personal data protection; and (iv) facilitation of alternative dispute resolution.

In the meantime, the role of personal data protection supervisions is being carried out primarily by the Ministry of Communication and Informatics ("**MOCI**"). Pursuant to GR 71/2019 and MOCI Reg. 20/2016, MOCI is responsible for ensuring compliance towards data protection matters within the EIT

sector, among others, by: (i) coordinating with electronic system operators ("**ESOs**") for cross-border data transfer; (ii) overseeing data breach notifications; (iii) supervising the implementation of personal data protection within the electronic system; and (iv) imposing administrative sanctions for personal data protection violations within the EIT sector.

For specific sectors such as financial services or payment systems, each sectoral supervisory and regulatory body has the authority to regulate and supervise the data-protection-related matters.

2 Definitions

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

- "**Personal Data**"
  Personal data means any data related to identified or identifiable individuals, separately or in combination with other information, directly or indirectly, through an electronic or non-electronic system.
- "**Processing**"
  Processing includes activities of data acquisition, collection, analysis, storing, rectification, update, display, announcement, transfer, dissemination, disclosure, erasure and/or destruction.
- "**Controller**"
  Controller means any person or corporation, public institution and international organisation acting individually or jointly that determine the purposes and have control over personal data processing activities.
- "**Processor**"
  Processor means any person or corporation, public institution and international organisation acting individually or jointly in processing personal data on behalf of the Controller.
- "**Data Subject**"
  Data subject means an individual whose data are associated with.
- "**Sensitive Personal Data**"
  The PDP Law categorises personal data into general data and specific (sensitive) data, which includes:
  a. health and information data;
  b. biometric data;
  c. genetic data;
  d. criminal records;
  e. children's data;
  f. personal financial data; and/or
  g. other data in accordance with provisions of laws and regulations.
- "**Data Breach**"
  Data breach means failure to protect a person's personal data in terms of confidentiality, integrity and availability of the personal data, including security breaches, whether intentional or unintentional, leading to destruction, loss, alteration, disclosure or unauthorised access to the data which are being transferred, stored or processed.
- "**Profiling**"
  Profiling means an activity of identifying a person, including, but not limited to: work history; economic condition; health; personal preferences; interests; reliability; behaviour; location; or movement of the data subject.

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?

Yes, the PDP Law has an extraterritorial coverage. Pursuant to Article 2 of PDP Law, the provisions under the PDP Law apply to processing activities outside Indonesian jurisdiction that have legal effect or consequence: (i) within Indonesian jurisdiction; and/or (ii) towards Indonesian data subjects outside Indonesia.

4 Key Principles

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

The PDP Law sets out several key principles in personal data protection, namely:

- **Lawful, fair and transparent (the "Lawfulness")**
  This principle requires data processing activity to be carried out in such manner that is lawful, fair and transparent. The Lawfulness principle essentially requires data processing activities to be carried out based on the appropriate lawful grounds, namely: (i) lawful consent; (ii) performance of a contract; (iii) legal obligation; (iv) vital interests; (v) duties for public interest; and/or (vi) legitimate interests.
- **Purpose limitation**
  This principle requires the purpose of data processing to be informed and the data processing shall be conducted in accordance with such purposes. Data processing purposes shall be specified, explicit and legitimate.
- **Data minimisation**
  This principle requires the data processing activity to use data that are adequate, relevant and limited to what is necessary for the informed purposes.
- **Accuracy**
  This principle requires the processed data to be accurate and up to date.
- **Integrity, security and confidentiality**
  This principle requires the protection of the processed data against unauthorised or unlawful processing activity, including unauthorised access, unauthorised disclosure, unauthorised alteration, misuse, loss or damage of data.
- **Lawful retention**
  This principle requires the destruction or erasure of the personal data if the retention period ends or it is requested by the data subject, in accordance with the applicable laws and regulations.
- **Ensuring data subjects' rights**
  In carrying out data processing activities, the rights of data subjects must be taken into account and complied with, in accordance with the applicable laws and regulations.
- **Accountability**
  This principle requires the processing activities to be carried out in a manner that is accountable and can be demonstrated.

5 Individual Rights

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

- **Right to obtain information**
  The data subject is entitled to obtain information on the identity, legal basis, purpose of request and use of personal data, and accountability of the party requesting the personal data.
- **Right to complete, update and/or rectify errors or inaccuracies**
  The data subject is entitled to complete, update and/or rectify errors or inaccuracies of their personal data in accordance with the purpose of data processing.
- **Right to access data or copies of data**
  The data subject is entitled to access and obtain a copy of their personal data, in accordance with the applicable laws and regulations.
- **Right to terminate the processing, deletion or disposal of data**
  The data subject is entitled to delete or destroy their personal data in accordance with the applicable laws and regulations.
- **Right to withdraw consent**
  The data subject is entitled to withdraw their submitted consent to the data processing.
- **Right to object against automated decision-making**
  The data subject is entitled to object to automated decision-making and profiling that has legal or significant effects on them.
- **Right to restrict processing**
  The data subject is entitled to postpone or restrict data processing proportional to the purpose of data processing.
- **Right to file a lawsuit**
  The data subject is entitled to file a lawsuit and receive compensation over the violation of their processed personal data.
- **Right to obtain, use or transfer their data**
  The data subject is entitled to obtain, utilise and transfer their personal data to another Controller, insofar as the system may communicate safely in accordance with the principles provided under the PDP Law.
- **Right to complain to the relevant data protection authority(ies)**
  The data subject is entitled to complain to the relevant authority in respect of a data protection violation.

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

The PDP Law does not expressly regulate this matter. However, in general, collective redress or class action is recognised under Indonesian regulatory framework.

6 Children's Personal Data

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

Under the PDP Law, the processing of children's personal data requires the consent of their parent or guardian. However, it is important to note that the age threshold for minors is stipulated differently under different laws and regulations in Indonesia.

7 Registration Formalities and Prior Approval

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

In general, the PDP Law does not require organisations to register or notify any governmental body for the processing activities of personal data.

However, if an organisation (Indonesian or offshore) processes personal data through an electronic system (i.e., website or application), such organisation can be considered as an ESO – and accordingly, is subject to obtain an ESO registration certificate under the EIT regulatory framework. Failure to conduct this registration is subject to an administrative sanction in the form of blocking access to the electronic system by the MOCI.

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

In order to obtain an ESO registration certificate, as mentioned in question 7.1, an organisation is required to submit several documents and information, among others related to the personal data that will be processed in the electronic system and information on the location of the data server. Substance-wise, the submission process only requires general information on the aforementioned items.

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

See question 7.1 above.

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

See question 7.1 above.

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

See question 7.2 above.

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

See question 7.1 above.

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

This is not applicable to our jurisdiction.

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

Any changes on the information submitted for an ESO registration certificate must be notified to the MOCI pursuant to Article 5 of MOCI 5/2020.

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

This is not applicable to our jurisdiction.

7.10 Can the registration/notification be completed online?

The ESO registration certificate process is completed online through an Online Single Submission ("**OSS**") system, an integrated electronic system for the implementation of licensing in Indonesia.

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

The list of registered domestic and foreign ESOs can be accessed through the following link https://pse.kominfo.go.id/home (in Bahasa Indonesia only).

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

There is no specific timeline for the ESO certificate registration process. However, in practice, it may take around one to three business days.

8 Appointment of a Data Protection Officer

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

An organisation is required to appoint a DPO if the following conditions apply:

a. the data processing is carried out for the interest of public services;
b. the nature, scope and/or purpose of the Controller's core activities require regular and systematic monitoring of personal data on a large-scale basis; and
c. the core activities of the Controller consist of large-scale processing activities of sensitive personal data and/or personal data relating to criminal activities.

An organisation may appoint the DPO from within or outside of the organisation, such as a consultant or lawyer, as long as such appointment is made based on professional qualities, expert knowledge, practice of personal data protection and the ability to fulfil the tasks.

It is important to note that the more detailed provisions on a DPO will be further regulated in the PDP Law's implementing regulation in the form of a Government Regulation.

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

Violation on the DPO appointment obligation is subject to an administrative sanction stipulated under Article 57 of the PDP Law, in the form of: (i) a written warning; (ii) temporary suspension of the data processing activity; (iii) erasure or destruction of personal data; and/or (iv) an administrative fine in the maximum amount of two per cent of annual income or annual receipt of the violation variable (subject to another implementing regulation of the PDP Law on sanction).

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

The PDP Law does not expressively stipulate whether a DPO is protected from disciplinary measures or other employment consequences in respect of their role as DPO. This matter may be further regulated in the to-be-issued PDP Law's implementing regulation on the DPO.

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

The PDP Law does not expressly stipulate this matter – although, this item may be further regulated in the to-be-issued PDP Law's implementing regulation.

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

The appointment of a DPO must consider professionalism, expert knowledge, data protection experience and ability to fulfil the duties. Furthermore, based on the MOCI Handbook of PDP Programme for DPOs issued in 2022 ("**DPO Handbook**"), the to-be-issued PDP Law's implementing regulation on the DPO will regulate a required certification for a DPO.

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

Pursuant to Article 54 of the PDP Law, a DPO is responsible for:

a. informing and providing advice to the Controller or the Processor in order to comply with the provisions of the PDP Law;
b. monitoring and ensuring compliance with the PDP Law and the policies of the Controller and Processor;
c. providing advice on assessing the impact of personal data protection and monitoring the performance of the Controller and the Processor; and
d. coordinating and acting as a liaison for issues related to the processing of personal data.

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

The PDP Law does not expressly stipulate this matter – although, this item may be further regulated in the to-be-issued PDP Law's implementing regulation on the DPO.

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

The PDP Law does not expressly stipulate this matter – although, this item may be further regulated in the to-be-issued PDP Law's implementing regulation on the DPO.

9 Appointment of Processors

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

The PDP Law only stipulates contractual requirement when the processing activity is carried out by two or more Controllers. However, as a good governance to protect the interest of the parties, it is advisable to have a written agreement to govern the relationship between the Controller and Processor. Furthermore, the DPO Handbook provides that the relationship between Controller and Processor shall be made in a written form which stipulates, among other things, the:

a. data subjects, duration, characteristics and purpose of the data processing activity;
b. personal data classification;
c. data subject's category;
d. rights and obligations of the supervisor;
e. Processor's authority to only process personal data based on documented instruction from the Controller;
f. Processor's warranty to ensure the confidentiality of the processed data;
g. Processor's warranty to undertake every necessary action to secure the data processing;
h. Processor respects the conditions for using another Processor;
i. Processor undertakes to help the Controller by implementing proper technical and organisational actions;
j. Processor undertakes to ensure the compliance to any obligations provided by the applicable laws and regulations related to PDP;
k. upon the Controller's choice, the Processor must delete or return all personal data to the Controller after the end of the completion of services related to the data processing and delete existing copies unless there are laws requiring the personal data to be stored;
l. Processor provides all compliance information required by the Controller; and
m. Processor allows and contributes to audit conducted by the Controller.

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

See question 9.1 above.

10 Marketing

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

There is no regulation which specifically regulates electronic direct marketing in Indonesia.

In terms of personal data protection aspects, electronic direct marketing activities are generally subject to the PDP Law and the EIT regulatory framework – for example, adhering to the personal data protection principles, complying with the relevant rules, processing personal data based on the appropriate lawful grounds, and so on. Meanwhile, content-wise, any marketing activities (including electronic direct marketing) must comply with Indonesian Consumer Protection Law and the Indonesian Advertising Code of Ethics 2020.

However, in specific sectors, more stringent rules may apply to the sending of electronic direct marketing, for example:

a. In the financial services sector (e.g., insurance, banking, fintech and other financial services) and payment system sector, consent is still the main lawful ground to process consumers' personal data.
b. Furthermore, the OJK Consumer Protection Regulations provide that, in the event that a financial service company intends to use the personal data of a data subject that were obtained from third parties, the financial service company must: (i) obtain a written statement that the third parties providing the data had obtained consent to share the personal data to such financial service company; and (ii) inform the potential consumer on the source of collection of the personal data. A similar concept is also adopted under the BI Consumer Protection Regulations.
c. Under the BI Consumer Protection Regulations, the sending of direct marketing can only be carried out from Monday to Saturday, outside public holidays and within 08.00–18.00 local time. The OJK Consumer Protection Regulations also adopted a similar concept, with additional rules, e.g.; (i) stating the purpose of the marketing; and (ii) the content must use simple and plain Indonesian language, contain clear information and include the financial services entity.

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

There is no specific provision under Indonesian laws and regulations that separate business-to-business and business-to-consumers marketing.

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

In general, the provisions set out in question 10.1 also apply to marketing via other means. Indonesia also does not have a specific national opt-out list for direct marketing activities.

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

The PDP Law and the EIT Law both contain extraterritorial provisions. Meanwhile, the Consumer Protection Law applies to foreign business actors outside Indonesian jurisdiction conducting business in Indonesian jurisdiction.

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

The MOCI, as the supervisory authority in the EIT sector, is relatively active in enforcement of breaches of the EIT regulatory framework – including related to electronic direct marketing activities. Similarly, the OJK and BI are also actively supervising the financial services and payment system sectors, respectively.

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

There is no specific provision regulating the purchase of marketing lists from third parties. However, the sale and purchase of marketing lists (which contain data subjects' personal data) may be considered as criminal actions under Article 48(2) *jo.* Article 32(2) of the EIT Law, as well as Article 65 of PDP Law, should be considered if such activities were carried out without the proper lawful ground for the processing of data of the data subjects.

In practice, entities may share data by entering into a data-sharing arrangement, under the conditions that both entities comply with the rules and requirements set forth by applicable laws and regulations – e.g., establishing the appropriate lawful grounds, informing the purposes of processing, and so on.

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

The maximum criminal penalty for violation of Article 32 of the EIT Law is maximum imprisonment of nine years and/or a fine of IDR 3 billion, while violation of Article 65 of PDP Law is subject to maximum imprisonment of five years and/or a fine of IDR 5 billion.

11 Cookies

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

There are no specific laws and regulations on cookies and/or other identifier technologies. However, insofar that the cookies contain personal data, the use of such technology will be subject to the relevant personal data protection laws and regulations mentioned in this chapter (e.g., the PDP Law, the EIT Law and/or other sectoral regulations as may be applicable).

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

The current applicable regulatory framework does not distinguish between different types of cookies.

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

There is no enforcement in relation to cookies to date.

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

Depending on the type of breaches, any use of cookies and/or other identifier technologies which violate personal data protection rules may be subject to administrative and/or criminal sanctions under the EIT Law and/or the PDP Law.

12 Restrictions on International Data Transfers

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

Pursuant to Article 56 of PDP Law, cross-border data transfer can be carried out if one of the following conditions is fulfilled:

a. the transferor must ensure that the recipient's country has an equivalent or higher standard of personal data protection than the PDP Law;
b. if the above condition in letter a is not met, the transferor must ensure the existence of an adequate and binding instrument (e.g., standard contractual clause); or
c. if the above conditions in letters a and b are not met, the transferor must obtain the data subjects' consent.

Please note that the more-elaborated provisions on cross-border data transfer will be further regulated in the PDP Law's implementing regulation in the form of a Government Regulation.

Furthermore, the EIT regulatory framework adds another requirement in conducting cross-border data transfer through an electronic system. Article 22 of the MOCI 20/2016 require a cross-border data transfer to be reported (before and after the transfer), by submitting information such as: (i) the designated country and recipient; (ii) the date of the transfer; and (iii) the purpose of the transfer. The regulation does not provide a specific time period for the reporting; however, in practice, the report is submitted annually using the form provided by the MOCI.

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

In addition to the conditions mentioned in question 12.1, the cross-border data transfer activities must also be carried out in compliance with the principles and rules set out under the PDP Law, the EIT Law and/or the relevant sectoral regulations (as may be applicable).

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

See question 12.1.

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

To date, there is no guidance issued by the authority on this matter.

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

To date, there is no guidance issued by the authority on this matter.

13 Whistle-blower Hotlines

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

There is no specific law/regulation on corporate whistle blowing. The existing regulatory framework only governs a whistle-blowing process within the context of a formal investigation process, witness protection and mostly related to criminal proceedings. Meanwhile, a corporate whistle-blower system/process is commonly implemented based on internal policy/regulation of the company itself. The scope of a corporate whistle-blower system mainly relates to corruption and/or general compliances.

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

This may be subject to each company's internal policy on a whistle-blower system. However, it is common for the company to encourage the disclosure of the identity of the reportee and the reported party – while at the same time provide a protection towards the confidentiality of the reportee.

14 CCTV

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

In addition to the general personal data protection principles and rules set forth by the PDP Law and the EIT Law, Article 17 of the PDP Law stipulates the use/instalment of CCTV in public places and/or public service facilities to only be carried out under the following conditions (letters b and c are exempted if the purpose is for the prevention of criminal action and law enforcement):

a. for the purpose of security, disaster prevention and/or traffic management or collection, analysis, and regulations of traffic information;
b. display information stating that CCTV has been installed in the area; and
c. not used to identify a person.

Any use/instalment of CCTV in private premises (e.g., an office or meeting room) shall comply with the general principles and rules under the PDP Law and the EIT Law – for instance, establishing the appropriate lawful grounds, adhering to the data minimisation principle, informing the purposes of processing, and so on.

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

See question 14.1.

15 Employee Monitoring

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

There is no specific provision and/or guidelines on this matter. However, in general, employee monitoring is permitted as long as it complies with personal data protection and privacy laws and regulations. In practice, common employee monitoring methods that are implemented are the instalment of CCTV in an office room, monitoring tools used in office devices, and so on.

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

The general applicable requirement under the PDP Law is to establish the appropriate lawful ground to conduct the employee monitoring activities – whether it is based on consent, employment contract or legitimate interest. In practice, employers are commonly seeking consent or providing notice/information at the outset, i.e., when the monitoring tool is first introduced or at the signing of an employment contract.

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

A company may have to consult the labour union if the company regulation or collective labour agreement requires the company to do so. As a reference, a collective labour agreement is required to include rights and obligations of both the employer and the employees. Although it may not be common, such rights and obligations may include the requirement of conducting a consultation or notifying the labour union for certain specific matters, such as the introduction of employee monitoring initiatives.

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

There is no provision which specifically prohibits an employer from processing an employee's COVID-19 vaccination status – so long as it is carried out in accordance with personal data protection laws and regulations. However, it should be noted that COVID-19 vaccination status may fall under the category of sensitive data stipulated under Article 4(2) of the PDP Law.

16 Data Security and Data Breach

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

The Controller and Processor are required to protect and ensure the security of the processed personal data pursuant to Article 35 of the PDP Law. This shall be achieved through:

a. preparing and implementing operational technical measures to protect personal data from disruption in the data processing;
b. determining the security level of personal data by taking into account the nature and risks of the processed personal data; and
c. using a security system for the processed personal data and/or processing personal data using an electronic system in a reliable, secure and responsible manner.

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

In the event that a data breach occurs, the Controller is required to submit a written notification to the affected data subjects and the Indonesian DPA no later than three days from the occurrence of the data breach, pursuant to Article 46 of PDP Law. In certain circumstances, the data breach shall also be notified to the public if it disturbs public services and/or has a material impact on the public interest. Pursuant to Article 46(2) of PDP Law, the notification shall contain the following items:

a. the disclosed data;
b. the time and reason of the breach; and
c. the remedy measure carried out by the Controller.

Furthermore, there is a requirement for the ESO to notify any security incident to the law enforcement authorities and relevant ministry or supervisory, pursuant to Article 24(3) of GR 71/2019. Such security incident is only applicable in the event of failure or disturbance of an electronic system caused by outsiders and resulting in a serious risk to the electronic system.

In addition, the ESO may electronically notify the data subject upon their consent, pursuant to Article 28 letter c of the MOCI Reg. 20/2016.

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

See our response to question 16.2 above.

16.4 What are the maximum penalties for data security breaches?

Failure in ensuring the security and confidentiality of the processed personal data is subject to the following administrative sanctions:

a. a written reprimand;
b. the temporary suspension of the data processing activity;
c. the erasure or destruction of personal data; and/or
d. an administrative fine in the maximum amount of two per cent of the annual income or annual receipt of the violation variable.

Under the GR 71/2019, violation to the principle of integrity and security is subject to the following administrative sanctions:

a. a written reprimand;
b. a fine;
c. temporary suspension;
d. an access termination; and/or
e. removal from the list.

17 Enforcement and Sanctions

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

a. **Investigative Powers:** The Indonesian DPA is authorised to carry out investigation in relation to a personal data protection breach allegation.
b. **Corrective Powers:** The Indonesian DPA is authorised to impose administrative sanctions of a personal data protection breach.
c. **Authorisation and Advisory Powers:** The Indonesian DPA is in charge of formulation and stipulation of policies and strategies for personal data protection which shall become the guideline for data subjects, Controllers and Processors.
d. **Imposition of Administrative Fines for Infringements of Specified GDPR Provisions:** This is not applicable to our jurisdiction.
e. **Non-compliance with a Data Protection Authority:** The Indonesian DPA may impose administrative sanctions in the event of any incompliances to personal data protection, as mentioned above.

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

Yes, pursuant to Article 57(2) letter b of the PDP Law, temporary suspension of data processing is one of the administrative sanctions that may be imposed because of a personal data protection breach. Such temporary suspension does not require a court order under the PDP Law.

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

As mentioned in question 1.4, while the Indonesian DPA has yet to be established, the MOCI is the primary supervisory authority in connection with data protection issues. In this case, during the series of data breach incidents that happened in Indonesia in 2021–2022 (public and private institutions), the MOCI summoned the relevant institutions to seek clarification on the incidents. However, there are no publicly announced sanctions that were imposed by the MOCI against such relevant institutions.

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

The MOCI, as the current data protection supervisory authority in Indonesia, has the authority to exercise its power against

organisations outside Indonesian jurisdiction since the EIT Law has extraterritorial provision – for example, by imposing administrative sanctions or blocking access to the electronic system operated by such offshore organisation. However, as at the time of writing, we have not seen the MOCI exercise its power against an organisation outside Indonesian jurisdiction due to a personal data protection violation.

Additionally, in theory, the to-be-established Indonesian DPA will also have similar power against offshore organisations due to the extraterritorial provision stipulated under the PDP Law.

18 E-discovery / Disclosure to Foreign Law Enforcement Agencies

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

Indonesian laws and regulations are silent on this matter. However, under the PDP Law, the Indonesian DPA is authorised to cooperate with the personal data protection agency of other countries to settle allegations of cross-border personal data protection violation. Furthermore, the obligation for a Controller to keep the confidentiality of the processed personal data may be exempted for the interest of the law enforcement process. Therefore, a foreign request for disclosure may be exercised insofar as it is for law enforcement purposes.

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

To date, there is no guidance issued by any authority on this matter.

19 Trends and Developments

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

In 2022, Indonesia finally enacted its general data protection law, i.e., the PDP Law. Although the PDP Law has a two years' grace period, we anticipate the improvement of the enforcement of personal data protection by the Indonesian government, which has been quite lax in dealing with personal data protection breaches for the past years, considering the comprehensive provisions set out under the PDP Law as well as the plan to establish a specific data supervisory institution (i.e., the Indonesian DPA).

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

Following the enactment of the PDP Law, the government is currently preparing for the issuance of the implementing regulations by involving public participation in the discussion. There are several provisions under the PDP Law that need more clarity and guidelines to support the enforcement of the PDP Law through the enactment of the implementing regulations, such as: (i) Data Protection Impact Assessments; (ii) DPOs; (iii) data transfer; and (iv) Indonesian DPA establishment.

Abadi Abi Tisnadisastra's practice covers a broad range of corporate and commercial areas, including mergers & acquisitions, restructuring, joint ventures, and foreign investments. He has been involved in numerous cross-border acquisitions and investments in companies from various industries, including banking, financial services, manufacturing, information technology, e-commerce and financial technology (Fintech). He also advises foreign investors on operations, corporate governance and legal compliance, advising, whether at the outset of their investment or in connection with the compliant functioning of their ongoing businesses.
Abi is recognised for his in-depth knowledge of financial services and information technology sectors, having advised local and multinational financial institutions (multi-finance, insurance and venture capital companies), tech players and investors in investing and consolidating operations in Indonesia. He advises clients across the Fintech ecosystem from start-ups to large technology companies, tech investors and financial institutions, as well as industry associations. Abi also counsels clients on data protection, blockchain technology and cryptocurrency.

ATD Law in association with Mori Hamada & Matsumoto
Revenue Tower, Level 20
Jl. Jend. Sudirman Kav. 52–53
DKI Jakarta 12190
Indonesia

Tel: +62 811 183 700
Email: abadi.t@mhm-global.com
URL: www.atdlaw.id

Prayoga Mokoginta has a strong passion for tech-related legal matters. While he handles a variety of areas of legal practice, Yoga mainly focuses his practice on mergers and acquisitions, personal data protection/data privacy, technology, fintech and payment system, e-commerce and general corporate.
He is a licensed lawyer to appear before the Indonesian courts. He holds a Bachelor of Law (S.H.) degree from Gadjah Mada University, Indonesia, and a Master of Laws (LL.M.) degree from Tilburg University (majoring in Law and Technology, with a focus on Personal Data Protection). He is a member of the Association of Indonesian Personal Data Practitioners and the International Association of Privacy Professionals (IAPP). Yoga is also in the process of obtaining a CIPP certification from IAPP.

ATD Law in association with Mori Hamada & Matsumoto
Revenue Tower, Level 20
Jl. Jend. Sudirman Kav. 52–53
DKI Jakarta 12190
Indonesia

Tel: +62 821 2528 8330
Email: prayoga.m@mhm-global.com
URL: www.atdlaw.id

ATD Law in association with Mori Hamada & Matsumoto (MHM) (ATD Law) is an Indonesian law firm with a focus on corporate commercial work serving local and international clients. ATD Law offers a full range of corporate commercial practices, mergers & acquisitions, foreign investments, banking & finances and TMT.
MHM is one of the top-tier firms in Japan, having offices in Japan, Singapore, Thailand, Vietnam, Myanmar and China. MHM's extensive regional network also means the firm is well-placed to advise on cross-border work for regional, as well as international, clients.
With MHM's network and ATD Law's experience in advising Indonesian projects, the firm leverages this synergy to offer its clients the expertise and resources of its regional network.

www.atdlaw.id

ATD Law
in association with
Mori Hamada & Matsumoto

ICLG.com

Current titles in the ICLG series

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

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