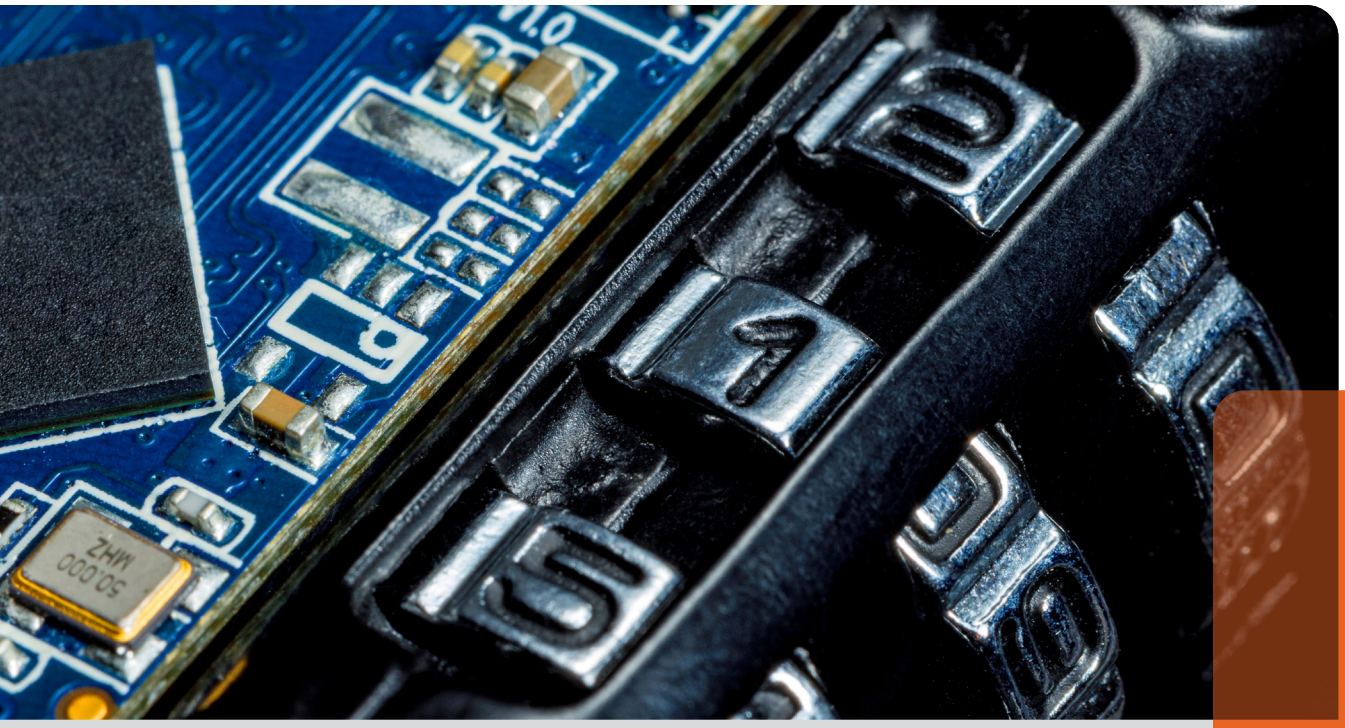
International
Comparative
Legal Guides



Data Protection

2024

11th Edition

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

glg Global Legal Group

Expert Analysis Chapters

Q&A Chapters

Indonesia

ATD Law in association with Mori Hamada & Matsumoto


Abadi Abi Tisnadisastra


Prayoga Mokoginta

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**"). 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/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.

While the PDP Law has been in effect since its enactment on 17 October 2022, we are still in its two-year transitional period until 17 October 2024. The full enforcement of the PDP Law is currently still subject to the issuance of implementing and technical regulations. The Indonesian Government is currently drafting the PDP Law's implementing regulation, and the draft of such regulation was circulated on 31 August 2023 for public discussion ("**RPP PDP**"). Based on the publicly available version, the RPP PDP will provide extensive elaboration and guidelines on certain aspects stipulated 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 lastly amended by Law No. 1 of 2024 ("**EIT Law**"), Government Regulation No. 71 of 2019 on the Operation of Electronic System and Transaction ("**GR 71/2019**"), Minister of Communication and Informatic ("**MOCI**") Regulation No. 5 of 2020 on the Organization of Private Electronic System as amended by MOCI Regulation No. 10 of 2021 ("**MOCI 5/2020**") and MOCI Regulation No. 20 of 2016 on Data Protection in Electronic System ("**MOCI 20/2016**").
b. Law No. 36 of 1999 on Telecommunication (as amended).
c. Law No. 7 of 1992 on Banking (as amended).
d. Law No. 17 of 2023 on Health ("**Health Law**").
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. 22 of 2023 on Consumer and Public Protection in The Financial Services Sector ("**OJK Consumer Protection Regulation**"), 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, which apply to protection of consumers' personal data within the financial services sector;
b. the Bank Indonesia ("**BI**") Regulation No. 3 of 2023 on BI Consumer Protection ("**BI Consumer Protection Regulation**") and its implementing regulation, namely Members of the Board of Governors Regulation No. 20 of 2023 on the Implementation Procedure of BI Consumer Protection, 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. 3 of 2024 on Organization of Financial Sector Technological Innovations, 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?

Currently, 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 MOCI.

Pursuant to GR 71/2019 and MOCI 20/2016, the 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.[1]

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 disposal.
- "**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 information and 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.[2]
- "**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 disposal, 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.
- "**Transfer**"
  Transfer means the assignment, disclosure or making available personal data, both electronically and non-electronically, from one party to another entity.

3 Territorial and Material 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. The PDP Law also applies 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.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Yes, data processing conducted by individuals for personal or household purposes are not subject to the PDP Law. As a reference, the RPP PDP provides that such activities include: (i) data processing activities that are not part of professional and/or commercial activity; and/or (ii) data processing activities that are not intended for the public.

4 Key Principles

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

- **Lawful, fair and transparent**
  This principle requires data processing activity to be carried out in such a 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 to be conducted in accordance with such purposes. Data processing purposes shall be specified, explicit and legitimate.
- **Data minimisation**
  Data collection must be limited to personal data that are relevant to what is necessary for the informed purpose.
- **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 compliance can be demonstrated.

The PDP regulatory framework through the RPP PDP will further elaborate on several minimum requirements of technical and organisational measures that, in several cases, must be implemented by organisations to ensure adherence to these principles. An example within the RPP PDP requires organisations to implement a data retention policy to ensure lawful retention. Another example would be for organisations to periodically assess collected personal data in terms of its relevancy to the purpose of data processing, to ensure data minimisation.

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**
  A data subject is entitled to obtain information on the identity, lawful ground, purpose of request and use of personal data, and accountability of the party requesting the personal data.
- **Right of access to data or copies of data**
  A data subject is entitled to access and obtain a copy of their personal data.
- **Right to complete, update, and/or rectification of errors or inaccuracies**
  A 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 terminate processing, deletion, and/or disposal of data**
  A data subject has the right to terminate, delete and/or dispose of their personal data, in accordance with applicable laws and regulations.
- **Right to restrict processing**
  A data subject may suspend or restrict data processing proportional to the purpose of data processing.
- **Right to data portability**
  A data subject may 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 withdraw consent**
  A data subject is entitled to withdraw their submitted consent to the data processing.
- **Right to object against automated decision-making**
  A data subject is entitled to object to automated decision-making and profiling that has legal or significant effects on them.
- **Right to file a lawsuit**
  A data subject has the right to file a lawsuit and receive compensation over the violation of their processed personal data.
- **Right to complain to the relevant data protection authority(ies)**
  The Indonesian DPA may receive complaints/reports of personal data protection incompliance; a data subject is entitled to complain to the relevant authority in respect of a data protection violation.

The PDP regulatory framework through the RPP PDP would further elaborate on means for which organisations may fulfil the exercise of these rights, along with grounds on which organisations may refuse to fulfil a data subject request for these rights. An example within the RPP PDP requires organisations to implement a compensation policy pursuant to data subjects' right to file a lawsuit. Another example provides that organisations may refuse the right to object against automated decision-making if it can demonstrate the absence of legal impact or significant impact and the existence of excellent system accuracy and system mitigation to avoid impact on data subjects.

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 law.

6 Children's Personal Data

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

The processing of children's personal data requires the consent of their parent or guardian. As a reference, the RPP PDP requires organisations to verify the consent granted by such children's parent or guardian. Further, based on the EIT Law, ESOs shall provide: (i) information on the minimum age limit of users of its products or services; (ii) a verification mechanism for child users; and (iii) a mechanism for reporting abuse of products, services and features that violate or potentially violate children's rights. Although the age threshold for minors in Indonesia is stipulated differently under different laws and regulations, the RPP PDP stipulates that a child is an individual who is under 18 years old and unmarried.

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 data processing activities.

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 do so is subject to an administrative sanction in the form of blocking access to the electronic system by the MOCI.

For notification/registration/approval relating to cross-border/international personal data transfer, please see question 12.1 below.

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)?

To obtain an ESO registration certificate, an organisation is required to submit several documents and information which, among others, are 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)?

Pursuant to MOCI 5/2020, any changes on the information submitted for an ESO registration certificate must be notified to the MOCI.

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 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 (available in the Indonesian language 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 are met cumulatively:

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.

A DPO may be appointed from within or outside 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. Further, the RPP PDP provides that the appointment of a DPO must consider the structure, size and need of the organisation.

A more detailed provision on the appointment of a DPO will be further regulated by a technical regulation that will be issued by the Indonesian DPA.

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 the PDP Law in the form of: (i) written warning; (ii) temporary suspension of data processing activity; (iii) erasure or destruction of personal data; and/or (iv) an administrative fine with the maximum amount of two per cent of annual income against the violation variable.

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?

Although the PDP Law does not expressively stipulate such matters, the RPP PDP provides that organisations must ensure

that a DPO shall not be dismissed or penalised in performing their duties in accordance with applicable rules and regulations.

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

The PDP regulatory framework does not expressly stipulate this matter. However, pursuant to the RPP PDP, we may anticipate that technicalities of the DPO, including the appointment of a single DPO for multiple entities, would be further regulated by a technical regulation that will be issued by the Indonesian DPA.

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. Based on the RPP PDP, we anticipate that the qualification of a DPO would be regulated under a technical regulation that will be issued by the Indonesian DPA.

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

A DPO is responsible for:

a. informing and providing advice to the controller or the processor in order to comply with the provisions of 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.

Additionally, the RPP PDP expands that a DPO must cooperate with internal parties responsible for data security by providing recommendation and supervision on appropriate technical and organisational security measures and assess their work performance.

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

The PDP regulatory framework does not expressly stipulate this matter. However, we anticipate this matter to be regulated under a technical regulation that will be issued by the Indonesian DPA.

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; however, pursuant to the RPP PDP, the contact information of the DPO must be informed to the data subject.

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?

While the requirements to have an agreement (when an organisation engages a processor) is only implied in the PDP Law, it is required under the RPP PDP, which provides the minimum clauses to be included, such as:

a. the scope of personal data processing conducted by the processor on behalf of the controller;
b. the method of personal data processing;
c. the time period of the personal data processing;
d. the mechanism for supervision, audit and inspection;
e. the involvement of another processor, if any; and
f. the appointment of a communication officer.

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 that specifically regulates electronic direct marketing in Indonesia.

In terms of personal data protection aspects, electronic direct marketing activities are subject to the PDP Law and the EIT regulatory framework – for example, adhering to personal data protection principles, processing personal data based on lawful grounds, and so on.

In specific sectors, more stringent rules may apply in the sending of electronic direct marketing. Under the BI Consumer Protection Regulations, the sending of direct marketing can only be carried out from Monday to Saturday, outside public holidays and between 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. Further, before a financial service company may use personal data indirectly collected from third parties, it must obtain a written statement from the third party that it has obtained consent to share the personal data to such financial service company and inform the consumer on the source of data collection.

Content-wise, any marketing activities must comply with Indonesian Consumer Protection Law and the Indonesian Advertising Code of Ethics 2020.

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-consumer 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, question 10.1 also applies 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 sector, respectively.

Since the Indonesian DPA, once established, will take charge of supervising personal data protection compliance, we anticipate that it will also perform supervision over the personal data protection aspects of marketing activities and will coordinate supervision with existing sectoral regulatory bodies.

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 the EIT Law, as well as the PDP Law, if such activities were carried out without proper lawful ground for the processing of data of the data subjects.

In practice, entities may share data by concluding a data-sharing arrangement, given 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, etc.

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 the 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.

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.

Cross-border data transfer (outside Indonesia) can be carried out under the existence of transfer mechanism/tools ("**Transfer Tools**") as follows:

a. If the recipient country has an equivalent or higher standard of personal data protection (adequate countries), it will be assessed by the Indonesian DPA pursuant to the RPP PDP.
b. In case the previous condition is not met, the transferor must ensure the existence of an adequate and binding personal data protection instrument. Based on the RPP PDP, this may be in the form of (i) an agreement between the transferor and recipient country; (ii) a Standard Contractual Clause ("**SCC**") that will be issued by the Indonesian DPA; or (iii) a Binding Corporate Rule for a group of companies that must be approved by the Indonesian DPA.
c. In case the previous conditions are not met, the transferor must obtain the data subjects' consent. This may only be applicable in limited circumstances as the RPP PDP imposes strict conditions on the use of consent for the transfer of personal data overseas.[3]

Furthermore, the EIT regulatory framework adds another requirement in conducting cross-border data transfer through

an electronic system. Article 22 of MOCI 20/2016 requires 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, which in practice is submitted annually using the form provided by the MOCI.

It should be noted that certain sectors may have more stringent requirements for international data transfer. For example, the Health Law requires that the transfer of personal data in health information system may only be conducted for a specific and limited purpose and based on approval of the central government, which will be further elaborated in the implementing regulation of the Health Law.

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 Transfer Tools 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 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

The PDP Law does not govern this matter. However, if we refer to the RPP PDP, such data transfer impact assessment must be carried out by organisations who wish to conduct international data transfer. Please note that the RPP PDP stipulates that further elaboration on data transfer impact assessment will be provided in the technical regulation that will be issued by the Indonesian DPA.

12.5 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.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

To date, the Indonesian DPA has not yet been established, and as such no guidance has been issued on this matter. However, the RPP PDP provides the clauses that must be governed under the SCC: (i) basis of data processing; (ii) clause on personal data protection; (iii) notification obligation on data breach; and (iv) obligation to conduct due diligence on the recipient of personal data transfer.

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 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 reported party – while at the same time provide a protection towards the confidentiality of the whistle blower.

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 principles and rules set forth by the PDP Law and the EIT Law, 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.

As a reference, the RPP PDP further provides that organisations must produce clear and concise information within the area covered by the CCTV, indicating the operation of such devices as well as the contact information of the person in charge of operating the CCTV. Such information must be placed in the entrance of a closed space or in an easily readable/accessible position.

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. Generally, it is permitted if it complies with personal data protection 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, etc.

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 employment contract or legitimate interest. However, it may be difficult to obtain lawful consent that is freely given in an employment–employer relationship. In practice, employers are commonly 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 uncommon, such rights and obligations may include the requirement of conducting 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 attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

There are no provisions that prohibits an employer from processing an employee's attendance in office. Such purposes are permitted so long as they are carried out in accordance with personal data protection regulations as with any other personal data processing activities.

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. This shall be achieved through:

a. preparing and implementing organisational and technical measures to protect personal data from disruption in the data processing;
b. determining the security level of personal data by considering 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.

As a reference, the RPP PDP further elaborates that in terms of security of personal data, organisations shall establish organisational technical measures and determine the level of security by considering the nature and the risk of personal data. Further, organisations are required to conduct gap analysis between the formulated organisational technical measures and the actual implementation of the measures.

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.

If 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. 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 the PDP Law, the notification shall contain the following items:

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

Under the RPP PDP, a data breach notification is exempted if it does not result in the disclosure of personal data. Based on the RPP PDP, the notification timeframe is no later than three days after the organisation discovers the data breach certainly, properly and reasonably based on internal documentation of the organisation. Further, the RPP PDP adds a condition for the obligation to also notify the public of data breach, i.e., when the controller cannot ensure that the data subject can directly receive the data breach notification.

Under the EIT regulatory framework, there is a requirement for the ESO to notify any security incident to the law enforcement authorities and relevant ministry/supervisory, pursuant to 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 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 question 16.2.

16.4 What are the maximum penalties for personal 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.

In regard to the calculation of administrative fines, the RPP PDP provides that the violation variables in determining the fine are, among others: (i) the duration of the violation; (ii) negative impact of the violation; (iii) scale of the organisation's business; and (iv) the organisation's ability to pay the fines.

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 order an organisation to take corrective measures as a follow up to supervisory measures.
(c) **Authorisation and Advisory Powers:** The Indonesian DPA oversees 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 legal provisions:** The Indonesian DPA is authorised to impose administrative sanctions, including fines for incompliance with personal data protection regulations.
(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, 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 recent data breach incidents in Indonesia (public and private institutions), 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 on disclosure of personal data to foreign law enforcement or governmental bodies?

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.

As we are reaching the end of the two-years transitional period of the PDP Law (by October 2024), we should anticipate the improvement of the enforcement of personal data protection by the Indonesian Government that has been soft 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). Accordingly, organisations have been more vigilant in complying with PDP obligations, such as appointing DPOs and implementing best practices.

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

The Indonesian Government is in its final stages of drafting the RPP PDP, which would greatly clarify and deepen data protection obligation under the PDP Law. The draft of the RPP PDP was issued for public discussion in August 2023. The RPP PDP will stipulate a comprehensive set of rules on what organisations must do to comply with the PDP Law. As per March 2024, the RPP PDP is in the stage of being discussed in inter-ministerial meetings between the MOCI and other ministries/government agencies that supervise different sectors in preparation of harmonisation. Inter-ministerial meetings will be due to end by April 2024, and the RPP PDP is expected to be issued in the first semester of 2024.

Endnotes

1 Referencing the RPP PDP, when the Indonesian DPA is established, it will have the authority to coordinate supervision with such sectoral supervisory and regulatory bodies.

2 As a reference, the RPP PDP stipulates that other data may be considered as specific data if its processing may result in discrimination, material/immaterial losses or other unlawful impacts to the data subject.

3 Consent may be used under the conditions that: (i) it is a non-recurring data transfer; (ii) it is involving only a limited data subject; (iii) the transfer is required to fulfil a purpose that does not set aside the rights of the data subject; and (iv) the organisation has assessed the risk and informed the data subject and the Indonesian DPA.

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
Treasury Tower 2F, SCBD, Lot 28 District 8
Jl. Jend. Sudirman Kav. 52-53, Senayan, Kebayoran Baru
Jakarta Selatan, Jakarta 12190
Indonesia

Tel: +62 811 183 700
Email: abadi.t@mhm-global.com
LinkedIn: www.linkedin.com/in/abaditisnadisastra

Prayoga Mokoginta has a strong passion in 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 focus on Personal Data Protection). He is a member of the Association of Indonesian Personal Data Practitioner and International Association of Privacy Professionals.

ATD Law in association with Mori Hamada & Matsumoto
Treasury Tower 2F, SCBD, Lot 28 District 8
Jl. Jend. Sudirman Kav. 52-53, Senayan, Kebayoran Baru
Jakarta Selatan, Jakarta 12190
Indonesia

Tel: +62 821 2528 8330
Email: prayoga.m@mhm-global.com
LinkedIn: www.linkedin.com/in/noor-prayoga-mokoginta-015875aa

ATD Law is an Indonesian law firm with a focus on corporate commercial work serving local and international clients, having strategic alliance and affiliation with a top-tier Japanese firm, Mori Hamada & Matsumoto (MHM), with offices in China, Japan, Myanmar, Singapore, Thailand and Vietnam.
ATD Law offers a full range of corporate commercial practices, including mergers & acquisitions, foreign direct investment, banking & finance, real estate, employment, capital markets and other corporate practices. Our lawyers in particular have been highly recognised by national and international clients, particularly in the fields of technology-media-telecommunication (TMT) and financial technology, as well as personal data protection and data privacy legal services. We are also highly qualified in providing services in real estate, employment, capital market and other corporate practices.
As a firm, ATD Law strives to adopt well-grounded and practical solutions to a wide array of legal issues. We are passionate about maintaining an international standard quality of legal services for our clients. We aspire to be the "Firm of Choice" for our clients and to contribute to the wider society as part of our role as legal practitioners.
With MHM's extensive regional network and ATD Law's experience in advising clients in Indonesia, the alliance is forged to leverage its resources and expertise in providing a distinctive and excellent service for all our clients.

www.atdmhm.com

ATD Law
in association with
Mori Hamada & Matsumoto

International Comparative Legal Guides

The **International Comparative Legal Guide** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Data Protection 2024 includes two expert analysis chapters and 31 Q&A jurisdiction chapters covering key issues, including:

- Relevant Legislation and Competent Authorities
- Definitions
- Territorial and Material Scope
- Key Principles
- Individual Rights
- Children's Personal Data
- Registration Formalities and Prior Approval
- Appointment of a Data Protection Officer
- Appointment of Processors
- Marketing
- Cookies
- Restrictions on International Data Transfers
- Whistle-blower Hotlines
- CCTV
- Employee Monitoring
- Data Security and Data Breach
- Enforcement and Sanctions
- E-discovery/Disclosure to Foreign Law Enforcement Agencies
- Trends and Developments

The International Comparative Legal Guides are published by: glg Global Legal Group