Data Protection in Indonesia: Overview

by Agus Ahadi Deradjat, Mahiswara Timur, Nina Cornelia Santoso, Dhan Partap Kaur, and Edmund Khovey, ABNR Counselors at Law, with Practical Law Data Privacy & Cybersecurity

Country Q&A | Law stated as at 01-Sep-2025 | Indonesia

A Q&A guide to data protection in Indonesia.

This Q&A guide gives a high-level overview of the data protection laws, regulations, and principles in Indonesia, including the main obligations and processing requirements for data controllers, data processors, or other third parties. It also covers data subject rights, the supervisory authority's enforcement powers, and potential sanctions and remedies. It briefly covers rules applicable to cookies and spam.

To compare answers across multiple jurisdictions in our Global Guides product, visit the *Global Guides Data Protection Country Q&A Tool*.

Regulation

Legislation

1. What national laws regulate the collection, use, and disclosure of personal data?

Law No. 27 of 2022 on Personal Data Protection (PDP Law) (in Indonesian) is the primary law governing any acts related to the processing of personal data, including the collection, use, and disclosure of personal data in Indonesia. The PDP Law is largely modelled on the EU *General Data Protection Regulation ((EU) 2016/679)* (GDPR), which is often considered the benchmark for personal data protection worldwide, demonstrating Indonesia's commitment to bringing its data protection legislation into line with global industry standards.

The PDP Law came into force on 17 October 2024, but some aspects of its provisions and enforcement are unfinalized because its implementing regulations have not been issued. The Indonesian government has since been working on the *Draft Implementing Regulation for Law No. 27 of 2022 on Personal Data Protection* (Draft GR PDP) (Indonesian only), which is intended to provide further guidance on the PDP Law's implementation and enforcement, but as of the date of this Q&A, there is no clear timeline for its finalization.

In addition to the PDP Law, the *Ministry of Communication and Digital Affairs* (MOCD) has issued the *Guidelines for Filling Assessment Tools in the Implementation of Personal Data Protection* (Guidelines) (Indonesian only). The Guidelines provide

guidance on complying with the PDP Law and offers more detailed explanations on the scope of the contractual relationship between data controllers and data processors.

The PDP Law provides for the creation of a new, independent, data protection authority which will be in charge of issuing guidelines and enforcing the PDP Law. Until this new authority is formed and operational, the MOCD remains responsible for primary oversight and regulation of data protection in Indonesia under the PDP Law.

Scope of Legislation

2. To whom do the laws apply?

The *PDP Law* applies to every person (individual or corporation), public entity, and international organisation that performs legal acts either:

- Within Indonesia.
- Outside of Indonesia but which have legal consequences either:
  - in Indonesia; or
  - for data subjects or Indonesian citizens residing outside of Indonesia.

(Article 2(1), PDP Law.)

The PDP Law specifically regulates the following parties involved in the processing of personal data:

- **Data controllers.** A data controller is any person, public entity, or international organization that acts individually or collectively to determine the purpose and controls the processing of personal data.
- **Data processors.** A data processor is any person, public entity, or international organization that acts individually or collectively to process personal data on behalf of the data controller.
- **Data subjects.** A data subject can be any natural person to whom personal data is attributed. The PDP Law does not, however, extend its protections to data subjects who are deceased. Data subjects cannot be legal entities.
- **Third parties.** The PDP Law does not specifically define this term (unlike the GDPR). However, where personal data is processed for and on behalf of a data controller, that person should generally be considered a third party and in that case should be supervised by the data controller.

(Article 1(4), (5), and (6), PDP Law.)

Because the PDP Law's definition of data subject is limited only to individuals (natural persons), a deceased data subject's personal data would be handled according to sectoral regulations, which are outside of the scope of this Q&A.

3. What personal data does the law regulate?

The *PDP Law* defines personal data as data related to an individual (natural person), whether identified or identifiable, independently or in combination with other information, whether directly or indirectly, through an electronic or non-electronic system (Article 1(1), PDP Law). Article 4(1) of the PDP Law provides a non-exhaustive list of matters considered to be general and specific personal data. Accordingly, any definition of personal data should be broadly interpreted and may include any other types of data that can be used to identify an individual, including individualized data that can be combined with other information and may be used to identify a person.

Based on the level of impact of processing on the data subject, the PDP Law classifies personal data into two categories:

- **General personal data.** This typically encompasses a person's:
  - full name;
  - gender;
  - nationality;
  - religion; or
  - marital status.
- **Specific personal data.** This refers to any personal data which, if processed, may result in a greater impact on the data subject, including discriminatory treatment and greater harm. Specific personal data typically encompasses information such as:
  - Health data or information;
  - *biometric data*;
  - *genetic data*;
  - criminal records;

- children's data;
- personal financial data; and
- other data in accordance with the laws and regulations.

(Article 4(1), PDP Law.)

4. What acts are regulated?

Article 16(1) of the *PDP Law* provides that personal data processing can include:

- Acquisition and collection.
- Processing and analysis.
- Storage.
- *Rectification* and update.
- Display, publication, transfer, dissemination, or disclosure.
- Deletion or destruction of personal data.

Accordingly, the PDP Law is meant to regulate the full scope and cycle of personal data handling (from collection, through to use, and then the eventual deletion of the data). The PDP Law does not regulate any processing beyond this scope.

5. What is the jurisdictional scope of the rules?

The *PDP Law* applies:

- Within Indonesia to every person, entity or organization that engages in personal data processing regardless of their citizenship.
- To anyone engaging in data processing outside the jurisdiction of Indonesia, when the processing has legal consequences:
    - inside Indonesia; or
    - for a data subject who is an Indonesian citizen outside Indonesia.

(Article 2, PDP Law.)

6. What are the main exemptions (if any)?

Article 2(2) of the *PDP Law* specifically states that it does not apply to personal data processing by individuals carrying out a private or household activity.

Certain data subject rights do not apply when processing is carried out for certain circumstances (see *Question 13*).

Notification

7.Is notification or registration with a supervisory authority required before processing data?

Notification, registration, or authorization may be required in certain circumstances. For information on the supervisory authority's notification, registration, or authorization requirements, see *Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Indonesia: Question 2* and *Question 3*.

Main Data Protection Rules and Principles

Main Obligations and Processing Requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

In Indonesia, personal data must be processed according to the following principles:

- **Lawfulness, fairness, and transparency.** Personal data must be collected in a restricted and specific, lawful, fair, and transparent manner, according to the explicit, lawful, and pre-determined purpose for which it is being processed.
- **Purpose limitation.** Personal data may only be processed for the purposes shared with the data subject at the time of collection.
- **Data subject rights.** The *PDP Law* requires data controllers to provide data subjects with certain rights, which must include a right of right of access, correction, and deletion (see *Question 12* and *Question 13*).
- **Accuracy.** Personal data must be processed in a manner that is accurate, complete, not misleading, and can be accounted for.
- **Security.** Personal data must be processed in a manner that is secure from unauthorised access, unauthorised disclosure, unauthorised modification, misuse, destruction, or removal. For details of security requirements, see *Question 15*.
- **Notification.** Data subjects must be notified both when their data is to be processed and when there has been a failure to protect their personal data. For details of breach of notification requirements, see *Question 16*.
- **Storage limitation.** Personal data must be destroyed or deleted either at the end of the retention period, or following a data subject's request, unless otherwise stipulated by any applicable laws and regulations.
- **Accountability.** Personal data must be processed in an accountable and clearly demonstrable manner.

(Article 16(2), PDP Law.)

To satisfy the respective accuracy and accountability obligations above, the *Draft GR PDP* requires data controllers to:

- Implement internal procedures to guarantee the accuracy, completeness, collection, and verification of the data, as well as ensuring that the data collected remains as up to date as possible.
- take measures to facilitate, in accordance with the applicable laws and regulations, the data subject's right to:

- complete, update or fix any mistakes/inaccuracies contained within the data;
- lodge a complaint with the data controller in relation to any automatic decision-making carried out based on the data, including any *profiling*, which has had a significant effect (whether legal or non-legal) on the data subject;
- delay or limit the processing of any personal data when in proportion to the purpose of the data processing.

- Document any inaccuracies or incompleteness in relation to the data.
- Implement protective measures in relation to verifying the data, to ensure accuracy and prevent the data subject from being subject to harm.
- Implement mechanisms and quality standards to ensure the data is processed in a manner that is complete and accurate.

Data controllers are generally required under the PDP Law to supervise both data processors and third parties involved in processing personal data under its control. This supervision requirement is further detailed in the *Draft GR PDP* and includes general requirement to establish an agreement that stipulates the relevant parties' rights and obligations in relation to the processing activity**.** For more on a controller's obligations when engaging data processors, see *Question 17*.

The PDP Law requires data controllers and data processors to appoint a Data Protection Officer (DPO) when:

- The data controller is carrying out the processing for the public interest.
- The data controller's main activities are of a nature, scope, and purpose that requires large-scale, frequent, and systematic monitoring of personal data.
- The data controller's main activities involve large-scale processing of specific personal data or personal data in relation to criminal offences.

(Article 53, PDP Law.)

To standardise DPO competencies, Indonesia's Minister of Manpower issued *Decree No. 103 of 2023* (Indonesian only), setting National Competency Standards for Personal Data Protection. These standards guide authorities in developing qualifications, training, and certification for DPOs.

For more information on the circumstances under which organizations must appoint a data protection officer, see *Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Indonesia: Question 4* and *Question 5*.

9. Is the consent of data subjects required before processing personal data?

The Indonesian *PDP Law* requires data subjects to explicitly consent to processing unless a controller can rely on a different legitimate basis for the processing (Article 20, PDP Law; see *Question 10*). Consent can be written or recorded electronically or non-electronically (Article 22, PDP Law).

Should consent be relied upon as a lawful basis for processing, the data controller must provide a consent form to the data subject, which must explain:

- The legality of processing.
- The purpose of processing.
- The types and relevance of personal data to be processed.
- The retention period of the documents containing personal data.
- The details of the information being collected.
- The period of processing.
- The data subject's rights.

(Article 21, PDP Law.)

Explicit Consent

Consent must be provided in a manner that involves the data subject expressly opting into the processing. The data subject's opt-in cannot be made implicitly, hidden, or based on errancy (oversight), duress, or deception. Consent must also be given in the Indonesian language, although a dual language format, such as in both English and Indonesian language, is also acceptable. The Draft Government Regulation on the Implementation of the PDP Law (Draft GR PDP) provides that consent will be deemed to be validly given when it satisfies all of the following elements:

- **Explicit.** The consent must not be hidden or based on any oversight, negligence, or duress on the part of the data subject.
- **Opt-in.** The data subject must provide their consent in a manner that requires affirmative action, instead of an implied opt-in or opt-out.

- **Informed.** The request for the data subject's consent must be accompanied by specific and clear information in relation to the goals and purposes of the processing.
- **Unambiguous.** The notice that consent is being obtained from the data subject must not be misleading and must be consistent with data subject's reasonable expectations.

(Article 55(1) a, Draft GR PDP; section 1.2.a., Guidelines.)

Data subjects are entitled to withdraw their consent anytime (Article 9, PDP Law and see *Question 13*).

Consent by Minors and Persons with Disabilities

The PDP Law requires consent from a child's parental or legal guardian before processing is permitted (Article 25, PDP Law).

The PDP Law classifies all data relating to children as specific personal data but does not specify what the age limit is for a data subject to be considered a child. The *Draft GR PDP* has defined children as being, for the purposes of the PDP Law, "individuals who are below 18 years and unmarried." However, other non-data protection related laws define children as both:

- Individuals below the age of 21 who have not been legally married are not competent to conclude an agreement (*Indonesian Civil Code*).
- Individuals below the age of 18 (*Law No. 23 of 2002 on Child Protection* (as amended, most recently by Law No. 17 of 2016)).

Before processing personal data of persons with disabilities, data controllers must obtain consent from the person with disabilities or their guardian (Article 26, PDP Law).

10. If consent is not given, on what other grounds (if any) can processing be justified?

Under the Indonesian *PDP Law*, data subject consent to processing is not required if the controller can justify the processing under one of the following other lawful bases for processing:

- **Contractual necessity.** Data controllers may process data without data subject consent when the data is processed to fulfil an obligation under a contract to which the data subject is one of the parties, or to fulfil a request made by the data subject at the time of entering into the agreement.
- **Legal obligation.** Data controllers may process data without data subject consent when the data is processed for the purpose of fulfilling a legal obligation to which the data controller is subject under applicable Indonesian laws and regulations.

- **Vital interest.** Data controllers may process data without data subject consent when the processing is necessary to protect the data subject's *vital interests*.
- **Public interest.** Data controllers may process data without data subject consent when the data controller processes the data to perform a task for public interests, public services, or for a lawful authority according to Indonesian laws and regulations.
- **Legitimate interest.** Data controllers may process data without data subject consent when T the data is processed to fulfil a legitimate interest after balancing the data controller's purposes and needs against the data subject's rights.

(Article 20, PDP Law.)

To determine the appropriate lawful basis for a certain processing activity, the Guidelines encourage data controllers to conduct a thorough assessment into every processing activity that is and will be performed, to identify:

- The purpose of processing.
- The type of processing that will be performed.
- The types of personal data required for the processing activity.
- The necessity of the personal data relative to the purpose and type of processing.

(Section 1.2.f., Page 31, Guidelines.)

If the assessment's results can be used to justify another lawful basis for processing, the data controller is not obliged to obtain the data subject's consent to process their personal data.

For further information on consent as a legal basis to process data, see *Question 9*.

Special Rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

The *PDP Law* classifies personal data into general and specific personal data, based on the level of impact of processing on the data subject (Article 4(1), PDP Law and see *Question 3*). Specific personal data is generally regarded as sensitive data, as it may result in a greater impact on the data subject if processed. While the PDP Law does not differentiate the treatment of processing of general or specific personal data, processing specific personal data may trigger additional obligations, such as

the need to perform a *data protection impact assessment* (DPIA) or to appoint a *data protection officer* (DPO) (Articles 34 and 53, PDP Law).

Conducting a DPIA requires the data controller or data processor to provide:

- A description of processing activities and the processing purposes, including the data controller's interests in the processing.
- An assessment of the need for, and proportionality between, the processing's purposes and activities.
- A risk assessment for protecting data subjects' rights.
- Details of the measures the data controller has taken to protect data subjects from the processing's risks.

(Article 128(2), *Draft GR PDP*.)

If a DPO is appointed, the data controller must take account of and document suggestions from the DPO when performing the DPIA. The DPIA must be reviewed if there are changes to the risks of processing. The DPIA and the steps taken by the data controller to protect data subjects from the risks of processing must be documented.

For further details of the legal bases to process non-sensitive personal data, see *Question 9* and *Question 10*.

Rights of Individuals

12. What information rights do data subjects have?

As part of the "lawfulness, fairness, and transparency" principle, data controllers must process personal data in a transparent manner. Under the *PDP Law*, transparency requires the data controller to ensure that data subjects are aware of:

- The personal data that is being processed.
- How their data is to be processed.
- Where they can find the related information and communications regarding the processing of their personal data, which should be provided in a form that is easily accessible and readily understandable, and in plain language (Indonesian language).
- (Elucidation of Article 27, PDP Law.)

The PDP Law does not specify the format for providing the notice containing the above information, nor the timing for delivery. However, the Draft GR PDP provides that:

- Data controllers must provide data subject with information on the:
    - legality of processing;
    - purpose of processing;
    - type and relevance of personal data to be processed;
    - retention period of documents containing personal data;
    - information being collected;
    - period during which the data will be processed; and
    - data subject's own rights with regard to the data processing.
- If the personal data is collected directly from the data subjects, the information must be provided prior to the collection or obtainment.
- If the personal data is collected indirectly, the information must be provided at the latest 30 days upon collection.

(Article 76 (1) and 77, Draft GR PDP)

There is no exception to the data controller's requirement to provide notice to data subjects on its intention use and process their data and notify them in accordance with the principles outlined above. For details of information regarding cookies, see *Question 18*.

For details of specific data rights granted to data subjects, see *Question 13*.

13. Other than information rights, what other specific rights are granted to data subjects?

In addition to the right to be provided with certain information (see *Question 12*), data subjects are granted other specific rights under the *PDP Law*, including:

- **Right to rectification.** Data subjects have the right to complete, update, and correct errors or inaccuracies in relation to any personal data regarding themselves, according to the purpose for which the personal data is processed. Data controllers must comply with requests to exercise this right within 72 hours of receiving them. (Article 6, PDP Law.)
- **Right of access.** Data subjects have the right to access and obtain copies of any or all personal data regarding themselves. Data controllers must comply with requests to exercise this right within 72 hours of receiving them. (Article 7, PDP Law.)
- **Right to terminate processing**. Data subjects have the right to terminate the processing, delete, or destroy any or all personal data regarding themselves (Article 8, PDP Law).
- **Right to withdraw consent.** Data subjects have the right to withdraw any previously given consent to personal data processing. Data controllers must comply with requests to exercise this right within 72 hours of receiving them. (Article 9, PDP Law.)
- **Right to object to automated decision-making**. Data subjects have the right to object to any decision-making action that is solely based on automated processing, including *profiling*, which has legal consequences, or has a significant impact, upon them (Article 10, PDP Law).
- **Right to suspend or restrict processing.** Data subjects have the right to suspend or restrict the processing of their data in proportion to the purpose for which the data is being processed. Data controllers must comply with requests to exercise this right within 72 hours of receiving them. (Article 11, PDP Law.)
- **Right to lodge a complaint and seek compensation.** Data subjects have the right to lodge complaints and receive compensation for any data processing violations concerning them (Article 12, PDP Law).
- **Right to data portability.** Data subjects have the right to obtain or use personal data about them from data controllers in a structured, commonly used or readable electronic system format (Article 13, PDP Law).

The PDP Law provides for certain exemptions to a controller's obligation to comply with a data subject's right to request the termination of processing, withdraw consent, object to automated decision-making, suspend and restrict processing, or right to data portability, when such a restriction is:

- In the interests of Indonesia's national defence and security.
- In the interests of law enforcement.
- In the public interest and is within the scope of the administration of the Indonesian state.
- In the interests of supervising the financial sector, monetary sector, or financial system, or ensuring the stability of Indonesia's financial system and is within the scope of the administration of the state.

- For the purposes of statistical and scientific research.

(Article 15, PDP Law.)

For more on data subject information rights, see *Question 12*.

For a comparison chart detailing controllers' notification obligations when experiencing a data breach, see *Quick Compare, Global Data Breach Notification Laws*.

Security Requirements

14. What security requirements are imposed in relation to personal data?

Data controllers and data processors have a legal obligation to both protect and ensure the security of all personal data they process by:

- Preparing and implementing technical and operational measures to protect the personal data from any illegal disruption or other measures which conflict with applicable laws and regulations.
- Determining the security level for the data by taking into consideration the nature of the personal data being processed and the associated risks of processing it.

(Article 35, PDP Law.)

The PDP Law does not specify any specific security requirements, but the *Draft GR PDP* provides some details of the types of technical and operational measures that would be expected to ensure security, including, but not limited to:

- Pseudonymizing and encrypting the data.
- Ensuring that the systems and services used can quickly restore access and make the personal data available in the event of a physical or technical incident.

(Article 131 (2), Draft GR PDP.)

Neither the PDP Law nor the Draft GR PDP mentions specific standards that must be complied with for security. However, in practice, international standards such as *ISO 27001* would suffice.

As a matter of practical implementation, data controllers should:

- Carry out a risk analysis of its processing activities and assess the appropriate level of security that should be implemented.
- Establish an information security and personal data protection policy and ensure that the policy is implemented consistently and continuously.
- Periodically review its information security and personal data protection policies and controls, and improve them if necessary.
- Implement personal data protections through encryption and/or data masking mechanisms.

Indonesian regulations are silent on the specific requirements for securing specific personal data (sensitive data). However, organizations should reasonably expect to deploy additional protection measures to protect sensitive data.

Processing by Third Parties

15. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

The *PDP Law* does not explicitly require a written data processing agreement when a data controller engages a data processor but the PDP Law does require data processors to follow the data controller's instructions and makes them liable for deviating from those instructions (Articles 51 and 57, PDP Law). Data processors are also required to obtain the data controller's written consent before engaging sub-processors (Article 51(5), PDP Law). According to the provisions of the *Draft GR PDP*, a data processing agreement is explicitly required when a data processor processes data on behalf of a data controller. The Data Processing Agreement must contain, at a minimum:

- The scope of processing to be carried out by the data processor on behalf of the data controller.
- The third party's procedure and methods for processing the data.
- The type of personal data being processed.
- The purpose for processing the personal data.
- The categories of data subjects.
- The period of processing.

- The rights and obligations of the data controller and the data processor.
- Details of the applicable supervision, audit, and inspection mechanisms.
- Provisions for how disputes will be resolved by the parties.
- If agreed, how other data processors will be involved.
- Appointment of a jointly appointed contact person.

(Article 21, Draft GR PDP.)

The data controller remains responsible for ensuring that any personal data processed by a data processor is carried out according to a proper lawful basis (Article 51(3), PDP Law).

Consent from the data subject is generally not required for transfers to third parties, unless there is no other lawful basis to justify such a transfer.

International Transfer of Data

Transfer of Data Outside the Jurisdiction

16. What rules regulate the transfer of data outside the jurisdiction?

Cross-border data transfers are generally permitted under the *PDP Law*.

Under Article 56 of the PDP Law, a data controller may transfer personal data to controllers or processors outside of Indonesia only when:

- **The foreign jurisdiction offers adequate protection.** Data can be transferred on this basis when the foreign jurisdiction receiving the data provides a personal data protection level that is equal or higher than the PDP Law's provisions (Article 56(2), PDP Law). However, the Indonesian government has given no indication of any intention to publish an approved list of such countries. Therefore, whether the level of personal data protection in the recipient country provides equivalent or higher is a matter to be determined by the Ministry of Communication and Digital Affairs (MOCD) (guidance provided in Chapter V Part III of the Draft GR PDP).
- **The data controller secures the transfer with appropriate safeguards.** Data can be transferred when the data controller secures the transfer by implementing adequate and binding personal data protections (typically

standard contractual clauses or *binding corporate rules*). The PDP Law is silent on what would constitute an appropriate safeguard in this context, although it is possible that a data processing agreement would be a sufficient measure to substantiate compliance. Nonetheless, there is no indication as to what provisions such an agreement would need to contain to establish an appropriate safeguard. According to the guidance provided in Chapter V, Part III of the Draft GR PDP, adequate protection of personal data can be ensured through:

- agreements between the sending and receiving countries;
- standard data protection contract clauses;
- binding corporate rules for groups of companies; and
- other data protection instruments acknowledged by the MOCD.

- **Consent is obtained.** Data may be transferred to a foreign jurisdiction that would otherwise be considered to not provide an adequate level of protection and appropriate safeguards are not in use if the data subject provides their specific consent to do so. According to the guidance provided in Chapter V, Part III of the Draft GR PDP, a data transfer to a foreign jurisdiction based on consent may be permitted when:
  - it is a one-time transfer;
  - it involves a limited number of data subjects;
  - it is necessary for specific purposes without overriding data subject rights;
  - the data controller has assessed the risk and implemented appropriate safeguarding measures;

    or
  - the data controller has informed the MOCD and the data subject of the transfer and the urgent legitimate interest fulfilled by such transfer.

The three mechanisms must be assessed and implemented in the above order (for example, if a data controller cannot rely on an adequate-protection basis, they may instead be able to rely on an appropriate-safeguards basis).

In limited circumstances, a data controller may be permitted to transfer data subject to a court decision, tribunal or administrative authority decision issued by a foreign jurisdiction, if there is an underlying international agreement in place with the country requesting the transfer.

The PDP Law does not provide any exemptions to the prohibition on transferring data outside the jurisdiction for affiliates, subsidiaries, or other companies within their corporate group located outside of Indonesia. However, the Draft GR PDP provides that it is possible for groups of companies to establish binding corporate regulations which can be used as a form of appropriate safeguards (Articles 185 and 188, Draft GR PDP). If such regulations are established, they must contain the following minimum elements:

- The receiving data controller or data processor must provide a level of personal data protection that is equivalent to or higher than that regulated in Indonesia's data protection laws and regulations.
- The names of the parties that are bound by the corporate regulations.
- A determination that the recipient country and territory should be based on such binding regulations.
- The distribution of roles, rights and obligations of the parties involved.

Data Transfer Agreements

17. Are data transfer agreements contemplated or in use? Has the supervisory authority approved any standard forms or precedents for cross-border transfers?

If it is not possible for a data controller to transfer data to a foreign jurisdiction on an adequate-protection basis, they may be able to rely on an appropriate-safeguards basis (see *Question 16*). In this case, implementation would be achieved by using standard data protection clauses which would be incorporated into a Data Transfer Agreement. According to the *Draft GR PDP*, these standard clauses will be determined by the Ministry of Communication and Digital Affairs (MOCD) and should contain, at a minimum:

- The basis for processing.
- A personal data protection clause.
- The relevant notification obligations in the event of any failure to protect the personal data.
- The obligation to carry out feasibility test on other parties receiving personal data transfer.

A Data Transfer Agreement that incorporates the standard data protection clauses would therefore be sufficient to legitimise a cross-border data transfer (provided it is not possible for the data controller to rely on an adequate-protection basis instead). However, the MOCD has not issued any further guidance on the matter and there is presently no indication as to whether the Indonesian government is intending to publish the standard clauses anytime in the near future.

In addition to the standard clauses, the Draft GR PDP allows for other forms of implementation, such as binding corporate rules.

For more information on the MOCD's notification, registration, or authorisation requirements before transferring personal data cross-border, see *Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Indonesia: Question 2 and Question 3.*

Enforcement and Sanctions

18. What are the enforcement powers of the supervisory authority?

The Ministry of Communication and Digital Affairs (MOCD) is responsible for regulating, supervising, and enforcing Indonesia's personal data protection policies and the PDP Law. See *Regulator Details.*

The PDP Law authorises the MOCD to:

- Formalise and adopt policies in the field of personal data protection.
- Supervise data controllers' compliance with the PDP Law.
- Impose administrative sanctions for any breaches of personal data protection committed by the data controller or the data processor.
- Assist law enforcement officers in handling alleged criminal offences regarding personal data under the PDP Law.
- Co-operate with foreign data protection authorities in resolving any alleged cross-border criminal offenses with regards to personal data protection.
- Review cross-border data transfers to assess their compliance with the necessary requirements.
- Give orders to act on the results of supervision of the data controller or the data processor.
- Publish the results of the supervision of personal data protection under laws and regulations.
- Receive complaints and reports on alleged personal data protection breaches.
- Examine and trace complaints, reports, and results of supervision of alleged personal data protection breaches.
- Summon any person or public entity involved in the alleged breaches of personal data protection to appear and order their attendance.

- Seek statement, data, information, and documents from any person or public institution involved in the alleged breaches of personal data protection.
- Summon experts to appear and order their attendance for examination and tracing of the alleged breaches of personal data protection.
- Examine and trace electronic systems, facilities, or workspaces used by data controllers or data processors, including for the purpose of gaining access to data.
- Seek legal assistance from the Indonesia prosecutor to settle disputes in relation to personal data protection matters.

(Article 60, *PDP Law*.)

Furthermore, under the *Draft GR PDP*, the MOCD has the power to:

- File a public interest lawsuit for the purpose of obtaining compensation to recover losses caused by violations of Indonesia's data protection laws and regulations.
- Conduct examinations, issue decisions, and impose administrative sanctions, following receipt of a PDP Law violation report that provides an examination of the alleged violations.
- Facilitate dispute resolution between parties following the receipt of a settlement request, or to submit verification results to law enforcement officials when it finds elements of a criminal violation.

However, despite the efforts of the Indonesian government to expedite the establishment of MOCD, this authority is yet to be officially formed. In the meantime, under *MOCD Regulation 1/2025 on Organization and Work Procedures* (Indonesian only), matters concerning personal data protection currently remain under the authority of the Directorate General of Digital Space Supervision at MOCD (DG). The DG is tasked with the following:

- Formulating and implementing policies regarding the supervision of the digital space and personal data protection.
- The implementation of monitoring, analysis, evaluation, and reporting in the digital space and in relation to personal data protection.
- Administrative operations.
- Implementing other functions assigned to it by MOCD.

19. What are the sanctions and remedies for non-compliance with data protection laws?

Administrative Sanctions

Failure to comply with *PDP Law* may result in the following administrative sanctions:

- Written warnings.
- Temporary suspension of processing activities.
- Erasure or destruction of personal data.
- Administrative fines.

(Article 57(2)(a) to (d), PDP Law.)

Administrative fines may be for up to 2% of the entity's annual income or annual revenue that can be attributed to the amounts received by the entity due to the violation, though there is some confusion about how annual income is meant to be calculated when it comes to global organizations (Article 57(3), PDP Law).

Criminal Sanctions

In addition to administrative sanctions, the PDP Law sets out specific criminal offences. These offences, which are punishable with imprisonment, fines, or both, include:

- Deliberately acquiring or collecting another person's personal data for their own or another party's benefit in an unlawful manner, or which may cause the data subject damage. This is punishable by imprisonment of up to five years, fines of up to IDR5 billion, or both. (Article 67(1), PDP Law.)
- Deliberately and unlawfully disclosing another person's personal data. This is punishable by imprisonment of up to four years, fines of up to IDR4 billion, or both. (Article 67(2), PDP Law.)
- Deliberately and unlawfully using another person's personal data. This is punishable by imprisonment of up to five years, fines of up to IDR5 billion, or both. (Article 67(3), PDP Law.)
- Deliberately falsifying personal data for the benefit of themselves or another party, or which may cause damage or loss to other person. This is punishable by imprisonment of up to six years, fines of up to IDR6 billion, or both. (Article 68, PDP Law.)

If any of the above crimes are committed by a corporation, criminal penalties may be imposed on the management, control holder, person giving the orders, beneficial owner, or the corporation itself. Fines are the only criminal penalties that may be

imposed on a corporation, with the maximum fine being up to ten times the fine values set out above. (Article 70(1) to (3), PDP Law.)

In addition to being subject to a fine, corporations may be subjected to the following additional penalties:

- Seizure of assets obtained or generated from the crime.
- The freezing of all or part of the corporation's business.
- Permanent prohibition on carrying out certain actions.
- Closure of all or part of the corporation's business premises and activities.
- An order to carry out an obligation that has been neglected.
- Payment of compensation.
- Revocation of the corporation's licence.
- Dissolution of the corporation.

(Article 70(4), PDP Law).

Regulator Details

Ministry of Communication and Digital Affairs

www.komdigi.go.id

Main areas of responsibility. Supervising data protection activity under the *Law No. 27 of 2022 on Personal Data Protection* (in Indonesian).

Under the PDP Law, the Ministry of Communication and Digital Affairs (MOCD) will be responsible for regulating, supervising, and enforcing Indonesia's personal data protection policies, but until it is established primary enforcement rests with the Directorate General of Digital Space Supervision at the MOCD (DG).

Contributor Profiles

Agus Ahadi Deradjat

ABNR Counsellors at Law
aderadjat@abnrlaw.com
www.abnrlaw.com/

Professional qualifications. Indonesia, lawyer

Areas of practice. Corporate; mergers and acquisitions; foreign direct investment; technology, media and telecoms.

Professional associations/memberships. Professional membership with Peradi and AKHI.

Mahiswara Timur, Senior Associate

ABNR Counsellors at Law
mtimur@abnrlaw.com
www.abnrlaw.com/

Professional qualifications. Indonesia, lawyer; Indonesian Certified Data Protection Officer

Areas of practice. Technology, media and telecoms.

Professional associations/memberships. Professional membership with Indonesian Data Privacy Professionals Association (APPDI).

Cornelia Santoso, Senior Associate

ABNR Counsellors at Law
nsantoso@abnrlaw.com
www.abnrlaw.com/

Professional qualifications. Indonesia, lawyer

Areas of practice. Competition; mergers and acquisitions; foreign direct investment; technology, media and telecoms.

Dhan Partap Kaur (Sonia), Associate

ABNR Counsellors at Law
dkaur@abnrlaw.com
www.abnrlaw.com/

Professional qualifications. Indonesia, lawyer

Areas of practice. Corporate; technology, media and telecoms.

Professional associations/memberships. Professional membership with Indonesian Data Privacy Professionals Association (APPDI).

Edmund Khovey, Associate

ABNR Counsellors at Law
ekhovey@abnrlaw.com
www.abnrlaw.com/

Professional qualifications. Indonesia, lawyer

Areas of practice. Dispute resolution; employment; shipping; technology, media and telecoms.

END OF DOCUMENT