

Implementation of Personal Data Protection Law: Key Provisions under GR No. 33 of 2026

The Indonesian government has finally issued Government Regulation No. 33 of 2026 on the Implementation of Personal Data Protection (“**GR No. 33/2026**”), which acts as the implementing regulation of Law No. 27 of 2022 on Personal Data Protection as last amended through Law No. 1 of 2026 on Criminal Adjustment (“**PDP Law**”). This issuance has been long awaited and marks a further development in the regulatory framework governing personal data protection in Indonesia by providing more detailed provisions on matters previously regulated at a general level under the PDP Law.

Once effective on 16 January 2027, GR No. 33/2026 will serve as an important reference for data controllers, data processors, and other stakeholders in understanding and implementing their respective obligations and rights under the personal data protection framework.

In light of the issuance and forthcoming effectiveness of GR No. 33/2026, businesses and other organizations that process personal data (“**Controller**”) should assess the implications of the new provisions for their existing data protection framework, policies, procedures, contractual arrangements, and operational practices. Where necessary, relevant adjustments should be considered to ensure compliance with the applicable requirements following the effectiveness of GR No. 33/2026.

Here are several key provisions under GR No. 33/2026 that may be particularly relevant to businesses, along with an overview of their potential legal and compliance implications.

1. Basis of Personal Data Processing

While the PDP Law has established the general bases for data processing, GR No. 33/2026 provides more detailed requirements and parameters governing their application. The key developments under GR No. 33/2026 are as follows:

a. Valid Consent.

Under GR No. 22/2026, the Controller is required to provide the individual whose personal data is being processed (the “**Data Subject**”) with relevant information prior to obtaining consent, ensure that the consent mechanism is appropriately linked to such information, and maintain evidence demonstrating that consent has been validly obtained. In addition, the Controller must also ensure that data subjects are able to withdraw their consent at any time. The Controller must also provide clear information regarding any third party that will receive the personal data, the nature and form of the offer, and the mechanism for reporting any continued solicitation following the withdrawal of consent.

Should the Data Subject refuse to provide any consent, the Controller is required to continue providing goods, services, or facilities without reducing the quality of such goods, services, or facilities, unless the provision thereof requires the processing of the relevant Personal Data.

b. Data Processing for Certain Categories of Data Subjects

GR No. 33/2026 further elaborates the safeguards applicable to the processing of Personal Data of children and people with disabilities. In relation to children, the Controller is required to obtain and verify the consent of the child's parent and/or guardian, taking into account the available technology. The Controller must also establish a transition mechanism for the processing of a child's Personal Data once the child reaches the applicable age or otherwise no longer qualifies as a child.

For people with disabilities, in particular, the Controller must provide specific accessibility mechanisms to enable people with disabilities to provide consent and submit requests for the exercise of their rights as Data Subjects.

c. Performance of an Underlying Agreement

GR No. 33/2026 further regulates the use of contractual necessity as a basis for processing Personal Data. This basis may be relied upon where the Data Subject is a party to an agreement or where processing is necessary to fulfill the Data Subject's request prior to entering into an agreement. Processing must be limited to what is necessary to fulfill the purposes set out in the agreement and must be supported by appropriate data protection measures.

d. Protection of Vital Interests

GR No. 33/2026 provides that the protection of vital interests may be relied upon as a basis for Personal Data processing where (i) a threat exists to the life, physical integrity, and/or property or assets of the Data Subject or another person; and (ii) obtaining the Data Subject's consent is not reasonably practicable in the circumstances. Following such processing, the Controller is required to notify the Data Subject of the processing.

e. Other Legitimate Interests

GR No. 33/2026 provides that reliance on legitimate interests as a basis for Personal Data processing requires the Controller to conduct a necessity and purpose assessment and balance the Data Subject's rights against the Controller's legitimate interests. The assessment must establish the legitimacy and necessity of the processing and identify any legal or adverse effects on the Data Subject, with appropriate mitigation measures implemented where such effects arise. Accordingly, the Controller must be able to

demonstrate that the processing is justified by a legitimate interest and does not result in unmitigated adverse consequences for the Data Subject.

2. Timeframe and Procedure for Access Request

GR No. 33/2026 further specifies the procedures and timeframe for Controllers to fulfill Data Subjects' access rights. Following verification, the Controller must provide access to the relevant Personal Data and processing records within 72 hours deadline from receiving the request. Access may be restricted where it could compromise the security or physical or mental health of the Data Subject or another person, disclose another person's Personal Data, or conflict with national defense and security interests.

3. Compensation for Personal Data Processing Violations

GR No. 33/2026 further specifies the procedure for Data Subjects to seek compensation for violations in the processing of their Personal Data. The Controller must establish a mechanism and policy for handling compensation claims, assess each claim, and provide a response to the Data Subject. A claim must include, at minimum, the Data Subject's identity, supporting evidence, and the legal relationship between the Data Subject and the Controller in connection with the processing. Where a claim is rejected or no agreement on compensation can be reached, the Data Subject may pursue legal action in accordance with applicable laws and regulations.

4. Cross-Border Transfer of Personal Data

GR No. 33/2026 introduces more detailed requirements for of Personal Data outside Indonesia's territory. Prior to conducting a cross-border transfer, the Controller must document and map the relevant data transfer flow and its implications, assess the legal instrument relied upon for the transfer and its effectiveness, and conduct periodic reviews. The Controller must also inform the Data Subject of the intended transfer prior to its implementation.

5. Joint Controller Agreement

GR No. 33/2026 further elaborates on the requirements for agreements governing the processing of Personal Data between Controllers. This agreement provides greater clarity on the allocation of roles, responsibilities, and accountability among the parties involved in processing Personal Data, while ensuring that the respective processing purposes, legal bases, and arrangements applicable to each Controller are clearly identified and documented.

6. Transfer of Personal Data in Corporate Transactions

While the PDP Law already requires controllers involved in a merger, demerger, acquisition, consolidation, or dissolution of a legal entity to notify Data Subjects of the transfer of Personal Data, GR No. 33/2026 provides a more detailed framework governing such transfers.

Prior to the transfer, the existing Controller must assess the outstanding rights of Data Subjects and the remaining data protection obligations arising during and following the corporate transaction, update the relevant Data Protection Impact Assessment (“**DPIA**”), and establish the operational measures required for the transfer. In addition, both the existing and new Controllers must provide specified notices to Data Subjects before and after the transaction.

GR No. 33/2026 also treats the existing and new controllers as joint controllers until the relevant corporate transaction is legally completed and requires them to enter into a data protection agreement.

7. Accountability and Demonstrable Compliance

GR No. 33/2026 further emphasizes the accountability principle under the PDP Law by requiring Controllers not only to be responsible for their Personal Data processing activities but also to demonstrate compliance with applicable data protection requirements. In implementing such accountability and compliance, Controllers must at a minimum (i) implement appropriate technical and organizational measures to meet accountability requirements; (ii) document all Personal Data processing activities; (iii) respond to information requests from the relevant authority; (iv) maintain documentary evidence demonstrating compliance; and (v) conduct internal and external Personal Data protection audits.

8. Personal Data Protection Officer

The PDP Law already requires certain Controllers to appoint an Official or Personnel Responsible for Performing Personal Data Protection Functions (“**DPO**”). GR No. 33/2026 further emphasizes this requirement by specifying the circumstances that trigger the obligation such appointment, such as certain large-scale processing activities.

The DPO is responsible for, among other matters, monitoring compliance with Personal Data protection requirements, providing advice and recommendations to the Controller or processor, overseeing and supporting the implementation of data protection measures, assisting with risk assessments and DPIA, and acting as a point of contact in relation to Personal Data protection matters. The DPO is also expected to have an appropriate position and access to the information and resources necessary to perform these functions

effectively. In practice, Controllers and processors should assess whether their processing activities fall within the appointment criteria, formally designate the DPO where required, clearly define the role and reporting line of the PPDP, and ensure that the individual is provided with sufficient authority, resources, and access to perform the required compliance and risk-management functions.

9. Personal Data Protection Impact Assessment

While the PDP Law already requires Controllers to conduct a DPIA for processing activities that may pose a high risk to Data Subjects, GR No. 33/2026 provides greater clarity on the assessment process and its required substance. In particular, processing activities that may pose a high risk to Data Subjects include: (i) automated decision-making that has legal effects or significant impacts on Data Subjects; (ii) processing of specific categories of Personal Data; (iii) large-scale processing of Personal Data; (iv) processing for systematic evaluation, scoring, or monitoring of Data Subjects; (v) processing involving the matching or combining of datasets; (vi) the use of new technologies in Personal Data processing; and/or (vii) processing that restricts the exercise of Data Subjects' rights.

In such cases, the Controllers are required to identify the risks associated with the proposed processing, assess the likelihood and severity of their potential impact on Data Subjects, and determine appropriate measures to prevent, reduce, or otherwise mitigate such risks. The assessment should be conducted prior to the commencement of the relevant high-risk processing and documented as evidence of the Controller's risk-based approach to compliance. Controllers should also review and, where necessary, update the DPIA where material changes to the processing activities, technology, or risk profile may affect the assessment. In practice, this requires Controllers to establish a documented DPIA process, define clear risk-assessment criteria, record the safeguards and mitigation measures adopted, and maintain the assessment as part of their broader Personal Data protection compliance framework.

The issuance of GR No. 33/2026 represents a development in the implementation of the PDP Law, as it further establishes the regulatory framework for personal data protection and provides greater clarity on the practical application of its obligations. Businesses should therefore assess their existing personal data protection framework against these requirements, with particular attention to updating internal policies, contractual arrangements, processing records, and operational procedures, where necessary, and maintaining sufficient evidence of compliance.

Further information

For any inquiries, please contact:



Michael Cecio Bangun

Partner

michael.c.bangun@imcolaw.com



Rania Nasir

Associate

rania.nasir@imcolaw.com



Office 8 Building, 35th Floor, Zone G
Sudirman Central Business District Lot. 28
Jl. Jend. Sudirman Kav. 52-53,
Jakarta 12190, Indonesia

Tel : +62 21 2933 3800
Fax : +62 21 2933 3801
Email: info@imcolaw.com

Disclaimer: The information provided in this article does not, and is not intended to, constitute legal advice. Otherwise, all information and materials available in this article are for general legal update or informational purposes only. We are not responsible for any implications arising from this article. All summaries of the laws, regulations, and practices are subject to change.