

September 2026

IMPLEMENTING REGULATION FOR INDONESIA'S PERSONAL DATA PROTECTION ("PDP") LAW

Overview

On 16 July 2026, the Government of Indonesia issued and promulgated Government Regulation No. 33 of 2026 on the Implementing Regulation of Law No. 27 of 2022 on PDP ("**GR 33/2026**"). GR 33/2026 contains 225 articles and will enter into force six months after promulgation, on 16 January 2027.

GR 33/2026 provides the principal implementing framework for Law No. 27 of 2022 on PDP ("**PDP Law**"), setting out more detailed rules on various matters, including lawful bases for processing, data subject rights, data protection impact assessments, personal data protection officers, cross-border data transfers, regulatory supervision, administrative sanctions, and dispute resolution.

Existing regulations regarding PDP remain in effect to the extent that they do not conflict with GR 33/2026. In addition, pending the issuance of the relevant PDP authority ("**PDP Authority**") regulation on personal data processing, personal data controllers ("**Controllers**") and personal data processors ("**Processors**") may continue to process personal data, provided that such processing does not conflict with GR 33/2026.

Key Provisions

- **Lawful Bases for Processing and Legitimate Interests:** GR 33/2026 retains six lawful bases for personal data processing. A Controller relying on legitimate interests must assess the necessity and purpose of the processing, balance its interests against the rights of the data subject, assess whether the processing may cause legal or detrimental effects, adopt mitigation measures where needed, and document the assessment. GR

33/2026 identifies security monitoring, health, safety, and crime prevention as examples of activities that may fall within legitimate interests, subject to the required assessment.

- **Consent Requirements:** Where processing relies on consent, consent must be obtained freely with awareness, specifically, and unambiguously. Relevant information must be available before consent is given, and the Controller must provide an electronic or non-electronic mechanism for obtaining consent. If a data subject declines consent, the Controller must generally continue to provide and must not reduce the quality of the relevant goods, services, or assistance, unless the processing is necessary to provide them. Where consent-based processing is used to offer goods or services, additional information requirements apply. GR 33/2026 also regulates specific requirements for processing the personal data of children and persons with disabilities, including parental and/or guardian consent requirements for children and consent requirements and accessibility measures for persons with disabilities.

- **Transparency and Privacy Notices:** Controllers must provide required information about processing across all lawful bases. This includes the legality and purpose of processing, the type and relevance of the personal data, retention, details of information collected, the processing period, and data subject rights.

Where personal data is obtained indirectly, the required information must be provided no later than 30 business days after the data is collected or obtained. GR 33/2026 also prohibits exoneration clauses that reduce,

restrict, or release a Controller's obligations or liability in personal data protection notices.

- **Records of Processing and Retention:** Controllers must record all personal data processing activities. The record must include, among other things, Controller and Processor contact details, sources of collection, lawful bases, purposes, data categories, parties with access to data, fulfillment of data subject rights, data flows, retention periods, security measures, and transfer details. Controllers must ensure that appointed Processors maintain the records required of them, and relevant records must be made available where required for audit and supervision.

Controllers must also establish a documented retention policy covering, among other things, applicable retention periods, destruction methods, responsible persons, and relevant legal bases.

- **Exercise of Data Subject Rights:** GR 33/2026 provides more detailed procedures and time limits for data subject rights recognised under the PDP Law. A Controller must generally provide access to personal data and update or correct inaccurate data no later than 3 x 24 hours after receiving the relevant request. The same statutory time limit applies to specified obligations following withdrawal of consent and requests to suspend or restrict processing.

GR 33/2026 also provides procedures relating to compensation claims, including the information and evidence to be submitted and the Controller's mechanism for handling such claims.

- **Data Protection Impact Assessment:** Controllers must conduct a data protection impact assessment ("DPIA") before commencing processing that has a potentially high risk to data subjects. The DPIA must address matters including the

necessity and proportionality, risks to data subjects, and mitigation measures. It must be documented and reassessed where processing risk changes. The elucidation of GR 33/2026 identifies artificial intelligence, machine learning, smart technology, and the internet of things as examples of "new technologies" relevant to the high-risk processing category.

Where a personal data protection officer has been appointed, the Controller must also seek and document the officer's advice in connection with the DPIA.

- **Personal Data Security and Oversight:** GR 33/2026 further specifies technical and operational measures for protecting personal data, including pseudonymization and encryption, maintaining the security and resilience of systems and services, restoring access and availability following incidents, and regularly testing and evaluating security measures.

Controllers must take account of relevant technology, implementation costs, the nature, scope, context and purposes of processing, and the associated risks. They must also supervise parties involved in processing under their control and ensure, by default, that processing is limited to personal data necessary for the relevant purpose.

- **Visual Monitoring Devices:** GR 33/2026 further regulates visual monitoring devices such as CCTV. Where such devices are installed in public places and/or public service facilities, their installation must satisfy the applicable purposes and conditions, information must generally be displayed in monitored areas, and the devices must not be used to identify individuals except as permitted for crime prevention or law enforcement purposes. Relevant privacy considerations include matters such as the location and angle of the monitoring device.

- **Personal Data Protection Failure:** Where a personal data protection failure occurs, a Controller must notify the affected data subject and the PDP Authority in writing no later than 3 x 24 hours from when the failure becomes known with certainty or is reasonably and justifiably known. The notice must contain information on the affected personal data, when and how it was disclosed, response and recovery measures, and the relevant PPDP or designated contact person.

Controllers must document failures and establish internal prevention and response policies and procedures. Where a failure occurs in processing performed by a Processor, the Processor must report it to the Controller at the earliest opportunity.

- **Personal Data Protection Officer:** Controllers and Processors must appoint a person or personnel performing the personal data protection function (“**PPDP**”, commonly referred to as a Data Protection Officer or DPO). A PPDP must be appointed where: (i) processing is for public service purposes; (ii) its core activities require regular and systematic large-scale monitoring; and/or (iii) its core activities involve large-scale processing of specific personal data and/or criminal-record data.

A PPDP may be internal or external and may comprise one or more persons, subject to the organisation’s structure, size, and needs. The PPDP must operate objectively, without intervention, and independently, and must have access to the highest level of management.

- **Personal Data in Corporate Actions:** GR 33/2026 provides more detailed requirements for transfers of personal data in mergers, demergers, acquisitions, consolidations, and dissolutions. The former and new Controllers must notify data subjects before and after the relevant corporate action takes effect.

Where a merger, demerger, acquisition, or consolidation involves a transfer of personal data, the transferring and receiving Controllers must enter into a personal data protection agreement. Their relationship is treated as joint control until the relevant corporate action is deemed complete under applicable laws and regulations.

- **Cross-Border Personal Data Transfers:** The PDP Law and GR 33/2026 establish a hierarchy for transfers of personal data outside Indonesia. A Controller must first ensure that the recipient country has an equivalent or higher level of personal data protection. If that condition cannot be satisfied, the Controller must ensure adequate and binding safeguards. Where the preceding requirements cannot be met, the transfer may rely on data subject consent, subject to additional requirements under GR 33/2026.

The PDP Authority will assess whether a country has an equivalent or higher level of protection and determine a list of countries and/or international organisations that provide an equivalent or higher level of protection. Relevant considerations include the existence of personal data protection laws, a supervisory authority, and relevant international commitments.

Controllers must also generally provide relevant information regarding the transfer to data subjects before the transfer takes place.

- **Supervision and Administrative Sanctions:** GR 33/2026 regulates the supervision and administrative enforcement framework under the PDP Law. PDP Authority has the authority to supervise the Controllers’ and Processors’ compliance through monitoring, control, examination, and tracing into suspected violations of personal data protection. PDP Authority is also authorized to publish the results of its supervisory activities.

Administrative fines are capped at 2% of annual income or annual receipts, with the amount determined by reference to various variables such as the impact and duration of the violation, affected personal data and data subjects, cooperation during examination, business scale, ability to pay, and compliance history.

More than one administrative sanction may be imposed concurrently, and a sanction need not always be preceded by a written warning. GR 33/2026 also regulates complaints and reports, examination of alleged violations, sanction decisions, implementation, and administrative objections.

- **Dispute Resolution:** The PDP Law permits personal data protection disputes to be resolved through arbitration, the courts, and other alternative dispute resolution mechanisms. GR 33/2026 further establishes a structured dispute-facilitation mechanism through the PDP Authority, including through mediation.

Closing

GR 33/2026 marks a significant development in operationalizing Indonesia's personal data protection framework and will take effect on 16 January 2027. Organisations should use the period before effectiveness to map processing activities, review lawful bases and notices, establish or update records of processing and retention schedules, test data-subject-request and incident-response workflows, assess high-risk processing, and address other compliance requirements.

GR 33/2026 is, however, not the final layer of Indonesia's personal data protection regulatory framework. Numerous provisions contemplate further regulations by the PDP Authority including in relation to lawful bases for processing, data subject rights, PPDP requirements, cross-border transfers, supervision, administrative sanctions, and dispute resolution. Further regulatory developments should therefore be monitored as Indonesia's personal data protection framework continues to develop.

For more information or inquiries, please contact:

Henny Marlyna – henny.marlyna@nusaadvocates.com

Andika Mendrofa – andika.mendrofa@nusaadvocates.com

Sharon Solomon – sharon.solomon@nusaadvocates.com