

Indonesia: Government Regulation No. 33 of 2026, the Implementing Regulation for the Personal Data Protection Law

In brief

Government Regulation No. 33 of 2026 ("**GR 33/2026**"), the implementing regulation for Law No. 27 of 2022 on Personal Data Protection ("**PDP Law**"), was recently made accessible to the public. Having a promulgation date of 16 July 2026, it is expected to take effect on 16 January 2027. GR 33/2026 provides substantially more detail on how personal data should be collected, used, protected and shared, although several procedures will remain subject to further interpretation, evolving practice, and regulations to be issued by the future Personal Data Protection Authority ("**PDP Authority**").

Key takeaways

1. A more operational framework

GR 33/2026 appears to be intended to translate broad statutory duties into more specific operational requirements. It covers the principal areas for which the PDP Law required implementing rules, while also introducing requirements not stated expressly in the PDP Law. These include detailed rules for joint controllers and processors, internal processing policies, privacy notices, records of processing, retention, security controls, audits, complaints, supervision and dispute resolution.

The regulation also clarifies several working concepts, including personal data protection failure, retention periods and the data protection officer function. A child is defined as a person under 18 years old who is not married. GR 33/2026 also elaborates on the personal or household activity exemption by referring to processing for personal or household needs, processing that is not professional or commercial, and processing not intended for the public.

2. Data subject requests and transparency

Controllers should provide an electronic and/or non-electronic channel that is easy for data subjects to access. Where processing is electronic, requests should be submitted electronically. Requests must be verified through a proportionate mechanism, and responses should generally use the same communication medium or another medium that is easily accessible. If a controller does not perform its obligations, a data subject may report the matter to the PDP Authority.

The information requirements previously associated primarily with consent appear to apply under all legal bases. Privacy information/notification should be available before processing begins, remain accessible throughout the processing, and be updated before a relevant change takes effect. Where personal data is obtained indirectly, the information should be provided no later than 30 days after collection or receipt.

3. Consent, marketing and special categories of individuals

A refusal to consent should not, by itself, reduce the availability or quality of goods, services or access, unless the relevant processing is genuinely required to provide them. Where consent supports marketing, the controller should

identify third-party recipients, explain the form of marketing, and provide mechanisms to withdraw consent and report marketing that continues after withdrawal. Consent must not be obtained through deceptive or misleading practices.

For children, controllers are expected to take steps to identify the child, verify parental or guardian consent taking account of available technology, support rights requests, and maintain a transition procedure when the individual is no longer treated as a child. Processing involving persons with disabilities should use accessible communications and a specific mechanism for exercising data subject rights.

4. Processing records, retention and internal governance

Controllers should establish internal personal data processing rules in line with future PDP Authority guidance. Records of processing are expected to cover, among other matters, contact details of personal data controller(s) and the Data Protection Officer ("DPO"), data sources and destinations, legal bases, purposes, data and data subject categories, third-party access, rights handling, data-flow mapping, retention, safeguards and transfer details. Records should be maintained in written electronic and/or non-electronic form, updated when information changes, and made available for audit, supervision or requests from the PDP Authority. A documented retention policy should address retention definitions and periods, affected data subjects and data types, archives, de-identification for statistics or scientific research, electronic and physical destruction methods, processor requirements, responsible personnel, documentation, notices and any statutory basis for retention.

5. High-risk processing and impact assessments

A data protection impact assessment should be completed before high-risk processing begins. Relevant triggers include solely automated decisions with legal or similarly significant effects, specific personal data, large-scale processing, systematic evaluation, scoring or monitoring, dataset matching, new technology, and processing that limits data subject rights. The assessment should describe the operations and purpose, test necessity and proportionality, assess risks to rights and identify safeguards. It should be documented, and revisited when risk changes, and should take account of documented DPO advice. Consultation with the PDP Authority may be available where processing may cause material or non-material loss or where no technical operational measure is available.

6. Corporate actions and overseas transfers

Before personal data is transferred in a merger, separation, acquisition, consolidation or dissolution, the relevant controller should assess outstanding rights and compliance obligations. Both the old and new controllers have notification responsibilities, including information on the transfer, processing activities, the new controller, objection or cessation mechanisms, and when the new processing begins. Overseas transfers follow a hierarchy: an equivalent or higher level of protection; adequate and binding safeguards; or, if neither is available, data subject consent. Binding safeguards may include legally enforceable instruments, standard contractual clauses, binding corporate rules or another mechanism recognized by the PDP Authority. The PDP Authority is expected to identify adequate destinations, issue standard clauses and approve binding corporate rules. Organizations may therefore wish to maintain a documented interim transfer assessment and evidence of the safeguards used.

7. DPO

A DPO is required for public-service processing, regular and systematic large-scale monitoring, and large-scale processing of specific personal data. The appointment should reflect professional knowledge and capability. The DPO may be internal or external, must have access to senior management and processing activities, and should operate objectively, independently and without conflicting duties. Adequate resources, access and documentation of the DPO's work are also expected.

8. Sanctions

Multiple sanctions may be imposed together and without prior warning. A fine may reach 2% of annual income or revenue, but may be reduced to Rp0 after certain consideration, the details of which are still unclear in GR 33/2026.

Action to consider

With the 16 January 2027 effectiveness date approaching, in-house legal and compliance teams may wish to prioritize the following workstreams:

- a. **Governance and accountability.** Establish a cross-functional implementation plan, identify accountable owners, review the DPO trigger analysis and reporting line, and confirm that the DPO has appropriate independence, resources and access.
- b. **Data inventory and documentation.** Expand records of processing to cover the prescribed fields, map data flows and third-party access, and prepare a retention policy addressing deletion, destruction and de-identification.
- c. **Notices, consent and individual rights.** Review privacy notices across all legal bases, indirect collection notices, consent and withdrawal journeys, marketing disclosures, accessible channels, verification steps and escalation procedures.
- d. **Contracts and third parties.** Update controller-processor agreements for the minimum required terms, review subprocessor approval and equivalent protection, and formalize joint-controller arrangements and responsibility allocation.
- e. **Children and accessibility.** Confirm age-identification and parental or guardian verification measures, transition arrangements when a child reaches the applicable threshold, and accessible mechanisms for persons with disabilities.
- f. **High-risk and automated processing.** Identify processing that may require an impact assessment, and establish pre-launch review gates, for significant automated decisions.
- g. **Security and incident response.** Assess pseudonymization, encryption, resilience, restoration and testing controls; update breach procedures to capture the notification trigger, required records, processor escalation and contact details.
- h. **Transfers and corporate transactions.** Inventory overseas transfers, document the applicable transfer hierarchy and safeguards, and add privacy due diligence, assessment and notification steps to transaction playbooks.
- i. **PDP Authority monitoring.** Track the presidential regulation establishing the PDP Authority.

GR 33/2026 marks a significant step in the development of Indonesia's data protection regime and is likely to require coordinated action across legal, compliance, security, product, procurement, human resources and operational teams. Although some provisions remain open to interpretation, organizations should consider beginning implementation now by taking a proportionate, well-documented approach that can be adapted as further guidance from the PDP Authority and potential market practice emerge.

Contact us



Daru Lukiantono
Senior Partner
daru.lukiantono@hhplawfirm.com



Daniel Pardede
Senior Partner
daniel.pardede@hhplawfirm.com



Harry Kuswara
Associate Partner
harry.kuswara@hhplawfirm.com