ATD LAW
in association with
MORI HAMADA

Newsletter

September 16, 2026

Indonesia's PDP Implementing Regulation Is Here: Key Takeaways from GR 33/2026

Abi Abadi Tisnadisastra
Partner
abadi.t@morihamada.com

Prayoga Mokoginta
Counsel
prayoga.m@morihamada.com

Aloysius Andrew Jonathan
Associate
andrew.j@morihamada.com

Introduction

Indonesia's Personal Data Protection Law (Law No. 27 of 2022, the "**PDP Law**") was enacted in 2022, with its two-year transitional period expiring in October 2024. Since then, considerable uncertainty has surrounded the implementation of the PDP Law. Many of its key provisions, ranging from the rules on data processing and cross-border data transfers to the establishment of a Data Protection Authority ("**DPA**"), were expressly subject to further elaboration through an implementing regulation that had yet to be issued. This left organizations grappling with uncertainty over how to operationalize their compliance obligations.

In August 2023, the Indonesian Government released a draft of the implementing regulation for public consultation (the "**Draft Regulation**"). We provided an initial overview of, and key insights into, the Draft Regulation in our October 2023 newsletter. Nearly three years after the PDP Law's enactment, the Indonesian Government has now formally issued Government Regulation No. 33 of 2026 on the Implementation of the PDP Law ("**GR 33/2026**"), which was signed on July 16, 2026, and will come into force six months from the date of its promulgation, on **January 16, 2027**. This issuance represents a pivotal milestone and effectively marks the beginning of full enforcement of Indonesia's PDP regulatory framework.

Key Highlights

1. Comprehensive Guidance: Largely Consistent with the Draft Regulation

Our review indicates that GR 33/2026 is substantially consistent with the Draft Regulation released in August 2023 both in its overall approach and in the substance of its rules and requirements. GR 33/2026 adopts the same two-tier regulatory architecture, under which: (i) it provides comprehensive guidance on what organizations (i.e., data controllers and data processors) must do to comply with each of the PDP Law's principles, rules, and requirements; and (ii) it provides for further technical regulations (*peraturan lembaga*) to be issued by the DPA, once established, for more granular operational details.

Specifically, GR 33/2026 covers the full spectrum of data protection compliance, including:

- **Data processing principles and lawful bases**: detailed conditions for each lawful ground (e.g., consent, contractual necessity, legitimate interest, vital interest, legal obligation, and public interest);
- **Rights and obligations**: comprehensive rules on data subject rights (access, rectification, deletion, portability, objection to automated decision-making) and controller/processor obligations (privacy notices, records of processing activities, retention policies, data protection impact assessments);
- **Data breach notification**: mandatory notification to both data subjects and the DPA within 72 hours of becoming aware of a personal data breach. The notification must include a description of the breach, when and how it occurred, the types of data affected, and remedial measures taken;
- **Data Protection Officers ("DPOs")**: mandatory appointment of a DPO for organizations that process personal data for public service purposes, conduct large-scale systematic monitoring, or process sensitive/specific personal data on a large scale;
- **Cross-border data transfers**: a three-tier mechanism: (a) transfers to countries with an equivalent or higher level of data protection (white-list), (b) transfers subject to adequate and binding safeguards (standard contractual clauses, binding corporate rules, or other instruments recognized by the DPA), or (c) transfers based on data subject consent as a last resort;
- **Administrative sanctions**: including written warnings, temporary suspension of data processing activities, deletion/destruction of personal data, and administrative fines of **up to 2% of annual revenue/receipts**; and
- **Dispute resolution**: mechanisms including mediation facilitated by the DPA and arbitration.

2. Key Structural and Substantive Changes

While the overall substance remains largely the same, GR 33/2026 does introduce certain refinements and structural changes compared to the Draft Regulation:

- **Refines the requirement for a contract as a lawful ground**: The Draft Regulation initially requires explicit consent from the data subject before a contract can be relied on as a lawful ground. In the absence of such consent, the agreement would be null and void. GR 33/2026 instead requires only a valid agreement between the controller and data subject. This clearly separates the use of consent with contract as a lawful ground and allows for a more liberal application.
- **Clearer and more streamlined corporate restructuring framework**: The provisions governing data transfers in the context of mergers, separations, acquisitions, consolidations, and dissolution of legal entities have been streamlined. GR 33/2026 now expressly requires the data controller, before transferring personal data, to assess outstanding data subject rights and controller obligations arising both during and after the restructuring process and to update the Data Protection Impact Assessment accordingly. The regulation also clarifies that the old and new data controllers are treated as joint data controllers until the restructuring is legally completed.
- **Removal of the exemption from data breach notification**: The Draft Regulation provides that the data breach notification requirement does not apply where the data breach does not result in unlawful disclosure of personal data. By contrast, GR 33/2026 removes this exemption, requiring notification of any failure of personal data protection.
- **Legitimate interest balancing test**: GR 33/2026 clarifies that legitimate interest may be relied on as a lawful basis only after the data controller has conducted and documented: (a) an analysis of the necessity, purpose, and balance between the data subject's rights and the controller's interests; and (b) an assessment confirming that the processing will neither have legal effects on nor harm the data subject, with mitigation measures in place.

3. Anticipating Further Technical Regulations

Consistent with the Draft Regulation, GR 33/2026 provides for a number of operational and technical matters to be addressed in further technical regulations (Peraturan Lembaga) to be issued by the DPA. These include, among others:

- Detailed rules on automated individual decision-making;
- Technical and operational measures and the determination of security levels;
- DPO appointment, professional competency, and ecosystem requirements;

- Further details on lawful grounds for cross-border data transfers (white-list countries, standard contractual clauses, binding corporate rules);
- Methods and variables for calculating administrative fines; and
- Procedures for data breach notification, requirements for records of processing activities, and procedures for dispute resolution through the DPA.

Organizations should be mindful that full operational clarity on these topics will only emerge once the DPA is established and the relevant technical regulations are promulgated.

Key Takeaways: Preparing for Full Enforcement

With GR 33/2026 set to come into force on January 16, 2027, organizations operating in Indonesia, or processing personal data of Indonesian data subjects, should take proactive steps to prepare for full enforcement:

1. **Conduct a comprehensive gap assessment**: evaluate existing data practices, policies, and systems against the requirements of the PDP Law and GR 33/2026 to identify compliance gaps and prioritize remedial actions.
2. **Review and update internal policies and documentation**: ensure that privacy notices, data handling policies, retention policies, records of processing activities, and data breach response plans are aligned with the detailed requirements now set out in GR 33/2026.
3. **Assess and appoint a DPO (if required)**: determine whether your organization meets the criteria that require the appointment of a DPO, and if so, identify and appoint a qualified individual or team with the requisite professional competency.
4. **Map and evaluate data sharing arrangements**: review all data sharing and disclosure arrangements, including intra-group transfers, arrangements with third-party processors, and cross-border data transfers. Assess the adequacy of existing contractual safeguards (e.g., data processing agreements, standard contractual clauses, binding corporate rules) and update them where necessary.
5. **Ensure data breach readiness**: establish or strengthen your incident response framework to comply with the 72-hour breach notification requirement in respect of both data subjects and the DPA.
6. **Monitor the establishment of the DPA and the issuance of further technical regulations**: stay abreast of developments regarding the establishment of the DPA and the issuance of technical regulations, which will provide further operational guidance on several key compliance areas.