

September 2026

NAVIGATING COMPLIANCE UNDER INDONESIA'S PDP LAW IMPLEMENTING REGULATION

Overview

Government Regulation No. 33 of 2026 ("**GR 33/2026**") is the long-awaited implementing regulation for Indonesia's Personal Data Protection Law ("**PDP Law**"). Enacted on 16 July 2026, GR 33/2026 consists of 225 articles designed to convert the high-level legal principles of the PDP Law into concrete obligations.

With a strict 6-month transition period concluding on 16 January 2027, all companies and organizations as controllers or processors this includes companies and organizations operating in Indonesia as well as, in certain circumstances, companies and organizations outside Indonesia whose processing activities have legal consequences in Indonesia or affect Indonesian citizen data subjects outside Indonesia must align their data-handling practices with GR 33/2026. In particular, they must create or update their governance and documentation for the entire data processing lifecycle to meet GR 33/2026's requirements.

Mandatory Governance Documentation

GR 33/2026 transforms general data governance into prescribed operational procedures. Controllers and processors must now prepare, issue, and maintain the following key instruments:

(a) PDP Policy: Data Lifecycle

Controllers must adopt formal internal policies (or a formal privacy policy) governing data processing. These policies should clearly address how data is collected, used, retained, and securely erased or destroyed, as well as the valid legal basis for any data processing.

(b) Record of Processing Activities ("**RoPA**")

Controllers are obliged to maintain a detailed RoPA that must contain the following minimum elements:

- (i) for controllers: at least 13 mandatory elements, including the controller/processor identity, data sources, lawful basis and purpose of processing, retention periods, security measures, and transfer details.
- (ii) for processors: at least 4 mandatory elements, including the processor identity, scope of processing activities, transfer details, and security measures.

(c) Data Processing Agreements ("**DPA**")

Whenever a controller engages a processor, a written contract (DPA) is required under GR 33/2026. This contract must specify the scope and means of processing, data categories, purposes, processing duration, the parties' rights/obligations, and audit or supervisory rights.

Likewise, if two or more controllers jointly determine the means and purposes of processing, they must enter a joint controller agreement covering their respective roles, shared purposes, and a jointly appointed contact point. These joint controllers are jointly and severally liable for compliance.

(d) Personal Data Protection Information (Privacy Notices)

Controllers must provide clear notice to data subjects about any data processing. In particular, privacy notices should cover the controller's identity, legal bases, processing purposes, data categories, retention periods, sources of data, recipients (including any international transfers), security safeguards, lifecycle of the data, and the data subjects' rights.

The regulation extends notice obligations to indirectly obtained data – if a controller receives data from affiliates, vendors, public sources, or via a corporate transaction, it must notify the data subject within 30 business days.

(e) Internal Data Processing Terms and Policies

Controllers and processors must adopt comprehensive internal policies governing personal data handling. This includes rules and procedures for data access, verifying requestors' identities, logging processing activities, and documenting any decisions. In sum, companies must maintain written records (policies, logs, audit trails, reports) for all key processes – from access control to incident management.

(f) Data Protection Impact Assessment (“**DPIA**”) Documents

A DPIA is mandatory whenever a processing activity falls into high-risk processing categories. GR 33/2026 provides seven broad DPIA triggers, though no fixed thresholds are given; instead, factors like volume of data, sensitivity, duration and number of data subjects guide the analysis.

When required, the DPIA must be completed before processing begins and must include a detailed description of the processing, its necessity and proportionality, an assessment of risks to data subjects, and the proposed mitigation measures. Accordingly, controllers should establish a standard DPIA template to ensure each high-risk project is properly reviewed and recorded (including any follow-up actions).

(g) Data Transfer Outside Indonesia

Before any cross-border transfer, a controller must map the transfer (purpose, data, recipient) and inform the data subject of the transfer's purpose, protection instruments and any risks. Transfers may only proceed on one of three bases: adequacy, safeguards, or consent.

All cross-border transfers must also appear in the RoPA and in the privacy notice to the data subject.

(h) DPO Appointment

A DPO must be appointed if any of the statutory triggers is met, which includes processing for public service purposes; core activities involving large-scale, systematic monitoring of personal data; or large-scale processing of sensitive or criminal data.

A DPO is responsible for advising on compliance, monitoring implementation of the PDP Law and internal policies, overseeing DPIAs, and acting as the contact point for data subjects and authorities. The DPO shall be involved in all processing activities, including access to senior management, and adequate resources and authority. The appointment (with job description and duties), and all advice or decisions by the DPO, must be documented in the company's records.

(i) PDP Failure Protocols (Incident Response)

A controller that confirms a personal data failure must notify affected individuals and the authority within 72 hours that starts only once the controller has conducted a reasoned assessment and determined (based on evidence) that a breach has indeed occurred. In practice, companies should have a tested incident-response plan to detect, investigate and document breaches swiftly. For each incident, they must record affected data, circumstances, impact assessment, remedial steps taken, and notification details. The protocols should also be updated regularly.

(j) Corporate Transaction Documentation and Agreements

Controllers must notify affected data subjects both before and after any transfer of data in a corporate deal (mergers, acquisitions, spin-offs, consolidations, or dissolutions), outlining the identity of the new controller, intended processing, and mechanisms to object. The parties must sign a data sharing agreement covering the handover. In addition, all corporate transaction documents (NDAs, sale agreements, etc.) should include detailed PDP clauses and ensure the statutory notice requirements are met.

Non-Compliance Risks

Non-compliance with GR 33/2026 exposes controllers and processors to immediate multi-tiered liabilities across administrative, criminal, civil, and contractual domains.

(a) Administrative Sanctions

GR 33/2026 confirms statutory administrative fines of up to 2% of annual gross revenue – the regulation explicitly defines "revenue" as gross economic inflows, not net profit – for non-compliance across key duties (including failure of legal basis, non-fulfillment of data subject rights, improper cross-border transfers, missing DPIA/RoPA, and unnotified data breaches).

(b) Criminal Liability

GR 33/2026 adds to the risk of criminal liability, which creates a direct bridge between administrative enforcement and criminal prosecution. If an administrative investigation uncovers elements of a crime (e.g., unlawful data trading, falsification, or intentional data alteration), authorities may report a criminal case to the police.

(c) Immediate Risks

While administrative fines and criminal reports will formally require the institutional setup of the Data Protection Authority, the following risks shall take effect immediately:

- (i) **Reputational and Contractual Risk:** A data breach or non-compliance can lead to loss of customer trust, brand damage, and contract terminations.
- (ii) **Civil Liability Risk:** Data subjects may seek compensation for harm caused by unlawful processing. Individuals can potentially sue controllers for damages.

Compliance Action Plan

To achieve full compliance by the 16 January 2027 deadline, companies should take a holistic approach. The key immediate steps include:

1. **Data Mapping and Audit:** Inventory all personal data flows and processing activities. Document what data is collected, where it is stored, who has access, where it is transferred, and under which lawful basis. Update or create a comprehensive RoPA and retention schedule reflecting every processing activity. Ensure that each processing has a valid legal basis and that permissions (e.g. consent forms) are documented.
2. **Policy and Process Updates:** Compare existing privacy policies and procedures against GR 33/2026's requirements. Draft or revise all required documents: privacy notices, internal data protection policies, security standards, breach response plans, DPIA templates, and DPA/joint-controller agreements. Remove any contractual clauses that conflict with the law (e.g. exoneration clauses) and ensure that all processing contracts contain the mandated clauses.
3. **DPO and Governance:** Determine whether a DPO must be appointed. If so, officially designate the DPO with clear independence, access to top management, and sufficient resources. Document the appointment and maintain a job description. Ensure the DPO is involved in all high-risk projects and consulted on DPIAs.
4. **Breach Response and Training:** Establish an incident-response team and train staff on breach detection. Prepare a detailed breach response plan so that, when a breach is discovered, the team can promptly verify it and issue notifications within 72 hours of confirmation.
5. **Awareness and Documentation:** Train employees about the new PDP obligations. Maintain records of all compliance efforts (risk assessments, audit findings, training logs, policy issuance, DPIAs, DPO advice, etc.) to demonstrate accountability to regulators.

By taking these steps now and thoroughly documenting each action, companies will not only meet GR 33/2026's mandates but will also ingratiate the "accountability" principle at the core of Indonesia's new data protection regime.

For further information, please contact:

Henny Marlyna at henny.marlyna@nusaadvocates.com

Andika Mendrofa at andika.mendrofa@nusaadvocates.com