ADP Counsellors at Law

THE BEST LEGAL SERVICE TO NAVIGATE YOUR BUSINESS

Insight

Government Regulation No. 33 of 2026: From Substantive Compliance to Demonstrable Compliance

Tanya Widjaja Kusumah, Khrisna Bagus Nugroho, and Quinto Halomoan Simbolon

ADP Counsellors at Law

Plaza Simatupang 6th Floor Kav. IS No. 01, Jl. T.B. Simatupang, RT.2/RW.17, Pd. Pinang, Kec. Kby. Lama, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12310 | info@adplaws.com

Introduction

Law No. 27 of 2022 concerning Personal Data Protection ("PDP Law") establishes the principal legal framework governing the processing of Personal Data in Indonesia, including the rights of Data Subjects and the obligations of Personal Data Controllers and Personal Data Processors. The PDP Law also delegates several matters for further regulation, including implementing certain Data Subject rights, Personal Data Protection Impact Assessments, cross-border transfers, administrative sanctions, and supervisory authority.

Government Regulation No. 33 of 2026 concerning the Implementing Regulation of Law No. 27 of 2022 concerning Personal Data Protection ("PP 33/2026") was enacted and promulgated on 16 July 2026. The Regulation consists of 225 Articles and provides more detailed rules concerning Personal Data processing, Data Subject rights, cross-border transfers, supervision, administrative sanctions, and dispute resolution. Pursuant to Article 225, PP 33/2026 will come into force six months after its promulgation, namely on 16 January 2027.

However, the significance of PP 33/2026 extends beyond completing the implementing framework contemplated by the PDP Law. The Regulation provides more detailed requirements concerning the lawful basis for processing, risk assessment, processing records, and accountability. Taken together, these provisions may be characterized as a shift from substantive compliance toward demonstrable compliance.

The first layer concerns what organizations must do to ensure lawful and responsible processing. The second concerns how they demonstrate that those obligations have been fulfilled. This distinction is particularly relevant because PP 33/2026 requires not only compliance with Personal Data protection obligations, but also supporting records and documentary evidence.

Substantive Compliance under PP 33/2026

PP 33/2026 requires Controllers to establish a lawful basis before processing Personal Data. Article 30 recognizes several bases, including valid consent, contractual necessity, legal obligation, vital interests, public interest or lawful authority, and other legitimate interests subject to the Regulation. Where consent is relied upon, it must be given freely, consciously, specifically, and unambiguously.

The practical significance is that **consent is no longer the default answer to every processing activity; Controllers must first establish the lawful basis applicable to the specific processing.** Where processing relies on legitimate interests, for example, the Controller must consider the purpose and necessity of the processing, balance its interests against the rights of the Data Subject, and assess relevant risks and mitigation measures.

PP 33/2026 also introduces preventive requirements for high-risk processing. Article 120 requires a Personal Data Protection Impact Assessment ("DPIA") for certain processing activities involving high risks, including specific Personal Data, large-scale processing, systematic evaluation or monitoring, profiling or scoring, new technologies, and certain automated decision-making. The DPIA is intended to identify risks to Data Subjects and the measures necessary to mitigate them.

This requirement is particularly relevant to organizations adopting new technologies. The Explanation to Article 120 identifies artificial intelligence, machine learning, smart technology, and the Internet of Things as examples of new technologies. Meanwhile, the Regulation addresses decisions based solely on automated processing, including profiling, where they produce legal consequences or significant effects. For organizations using AI-based recruitment, credit scoring, or similar systems, the relevant risk and DPIA assessment should therefore be considered before deployment.

PP 33/2026 further provides a mechanism for Data Subjects to object to qualifying automated decisions. The Controller must provide a mechanism for responding to such objections and information concerning the technology used and its consequences. Where a verified objection is accepted, the Controller must provide an alternative involving human intervention and/or a process that is not based on the automated result.

These provisions demonstrate the first layer of the Regulation: organizations must assess the legality and risks of processing before the activity is undertaken and must provide safeguards where processing may materially affect Data Subjects.

Demonstrable Compliance under PP 33/2026

The second layer concerns the ability to demonstrate that those substantive obligations have been fulfilled. Article 74 requires Controllers to record Personal Data processing activities, including the lawful basis, purpose, categories of data and Data Subjects, data flows, retention periods, security measures, and transfers. Article 138 further requires Controllers to demonstrate accountability in fulfilling Personal Data protection principles, including through documentation, responses to information requests, evidence of compliance, and internal and external audits. Similar obligations apply to Processors.

Accordingly, compliance is no longer limited to whether an organization has adopted a privacy policy or obtained consent. An organization should also be able to establish a clear compliance trail showing why Personal Data was processed, on what basis, for what purpose, and with what safeguards. This makes documentation part of substantive risk management rather than merely an administrative exercise.

The same approach applies to Personal Data breaches. PP 33/2026 requires notification within 3 x 24 hours after a failure in Personal Data protection has been known with certainty, reasonably, and properly, together with information concerning the affected data, the incident, and measures taken to address it. The Regulation also requires appropriate documentation and procedures for handling such failures.

For businesses, this means that incident response should not be treated solely as a technical cybersecurity function. Organizations should also be able to identify the relevant Personal Data, determine the applicable obligations, document the response taken, and substantiate their compliance when required.

The accountability framework is also extended to corporate transactions. PP 33/2026 regulates the transfer of Personal Data in connection with mergers, separations, acquisitions, consolidations, and dissolutions. Before the transfer, the relevant parties must assess the Data Subject rights and Personal Data protection obligations that remain applicable during and after the transaction, update the relevant DPIA, and establish necessary technical and operational measures.

The Regulation further provides for Joint Controller status between the existing and new Controllers until the corporate transaction is completed under the applicable laws and regulations. It also requires notification and, for specified transactions, an agreement addressing the lawful basis, Personal Data protection principles, Data Subject rights, and the allocation of responsibilities.

For businesses undertaking M&A transactions, the implication is clear: **Personal Data due diligence should not end with identifying what data is held by the target company. The transaction should also establish how that data may lawfully be transferred, who will be responsible for it, and how Data Subject rights will continue to be addressed.**

A similar framework applies to cross-border transfers. Controllers must record and map the transfer cycle, identify and assess the relevant legal instrument, consider risks to Data Subject rights, and implement supplementary safeguards where necessary. Data Subjects must also receive relevant information before the transfer, while the receiving jurisdiction must satisfy the protection requirements prescribed by the Regulation.

These requirements illustrate the broader compliance model under PP 33/2026. Organizations are expected not only to determine that a processing activity is lawful, but also to maintain sufficient records and evidence demonstrating the basis for that determination and the safeguards applied.

The enforcement framework provides the final link between compliance and regulatory accountability. PP 33/2026 provides for written warnings, temporary suspension of processing, deletion or destruction of Personal Data, and administrative fines. The fine may reach 2% of annual revenue or receipts, although the amount is determined by reference to factors prescribed by the Regulation and is not automatically imposed at the maximum rate.

Conclusion

PP 33/2026 provides a more detailed framework for implementing the PDP Law, particularly in relation to lawful processing, high-risk processing, automated decision-making, Personal Data breaches, accountability, corporate transactions, cross-border transfers, and administrative enforcement.

Nevertheless, its significance lies not only in elaborating substantive obligations. The Regulation also places greater emphasis on the ability of Controllers and Processors to **demonstrate** how those obligations have been fulfilled through records, assessments, procedures, and other documentary evidence.

Accordingly, organizations should approach the implementation of PP 33/2026 not merely as an exercise in revising privacy policies or consent mechanisms, but as a broader review of their Personal Data governance framework. The key question will increasingly be not only whether an organization is compliant, but whether it can demonstrate that compliance when required.

Accordingly, PP 33/2026 represents a shift toward a more accountable and demonstrable Personal Data protection compliance regime in Indonesia.

This article is intended for general informational purposes only and does not constitute legal advice. For legal assistance or inquiries specific to your situation, please contact us at info@adplaws.com.

ADP Counsellors at Law

Office
Plaza Simatupang 6th Floor Kav. IS No. 01, Jl. T.B. Simatupang, RT.2/RW.17, Pd. Pinang, Kec. Kby. Lama, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12310

Email
info@adplaws.com

Tel.
+6221 2270 2291