PP 33/2026: SIX IMPLEMENTATION PRIORITIES BEFORE 16 JANUARY 2027

RSM INDONESIA CLIENT ALERT – 18 SEPTEMBER 2026

Indonesia promulgated Government Regulation No. 33 of 2026 concerning the Implementing Regulation of Law No. 27 of 2022 on Personal Data Protection (PP 33/2026) on 16 July 2026. Under Article 225, the regulation will take effect six months later, on 16 January 2027.

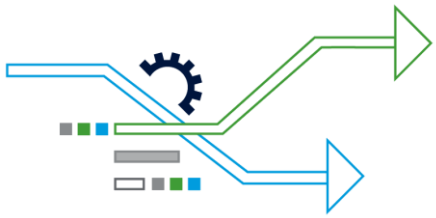
This is not the beginning of PDP compliance. The UU PDP is already in force and its two-year adjustment period has ended. PP 33/2026 now provides more detailed operational requirements and strengthens expectations that organizations can demonstrate—not merely state—their compliance.

Across its 225 articles, the regulation provides greater detail on lawful processing, Data Subject rights, high-risk processing and Data Protection Impact Assessment (DPIA), breach management, Processor and international transfer arrangements, PPDP governance, accountability, supervision, and administrative sanctions.

Indonesia issued Government Regulation No. 33 of 2026 (PP 33/2026), implementing Law No. 27 of 2022 on Personal Data Protection (UU PDP), on 16 July 2026. Under Article 225, PP 33/2026 takes effect six months after its promulgation, on 16 January 2027.

WHAT THE REGULATION REQUIRES IN PRACTICE

Many of the core duties originate in the UU PDP. PP 33/2026 translates those duties into more detailed operational and evidentiary requirements and specifies mechanisms that organizations may not yet have embedded in their processes and systems, including internal and external personal data protection audits for Controllers (Article 138). The practical question is no longer whether a policy exists, but whether the organization can demonstrate that its controls operate in practice. The six implementation priorities below identify the areas that require review.



SIX IMPLEMENTATION PRIORITIES

1) Processing inventory, lawful bases, notices, and consent

PP 33/2026 sets out the lawful bases for processing (Article 30). Where processing relies on consent, that consent must be explicit, freely given, informed, specific, and unambiguous, with a mechanism to obtain and withdraw it and evidence that it was given (Article 30(3)(a) and Articles 32–37). The obligation to keep personal data accurate remains a core principle (Article 9), supported by operational obligations on data quality (Article 69). Separately, Controllers must maintain a record of all processing activities (Article 74), which underpins the processing inventory.

Organizations should ensure these elements are reflected consistently across their processing inventory, privacy notices, internal procedures, systems, and contracts.

2) Data Subject rights and operational response mechanisms

The regulation sets out rights that systems and processes must be able to support. The right to object applies to a decision based solely on automated processing, including profiling, that produces a legal effect or a significant impact on the Data Subject (Articles 93–96). It does not extend to all automated processing.

The right to data portability and interoperability applies only where the processing is based on explicit consent or performance of a contract and is carried out by automated means (Article 111(3)). Organizations should confirm that their procedures for handling Data Subject requests, objections, and data export operate in practice.

3) High-risk processing, DPIA, and AI-related processing

A DPIA is required where processing poses a high risk to Data Subjects. Article 120(2) sets out the categories of high-risk processing that require a DPIA. The Elucidation to Article 120(2)(f) expressly identifies artificial intelligence, machine learning, smart technology, and the Internet of Things as examples of new technology. Where these technologies are used to process personal data, the processing falls within the new-technology category and requires a DPIA. Under Article 120(2), the categories of high-risk processing that require a DPIA are:

a. automated decision-making with a legal or significant effect;

b. processing of specific (sensitive) personal data;

c. large-scale processing;

d. systematic evaluation, scoring, or monitoring of Data Subjects;

e. matching or combining of data sets;

f. use of new technology, including artificial intelligence and machine learning; and

g. processing that restricts the exercise of Data Subject rights.

Two further indicators are worth screening even though they are not statutory triggers under Article 120:

a. processing that involves third parties or complex data-sharing; and

b. processing that involves international transfers.

Organizations should determine which initiatives require a DPIA, rather than treating all third-party or cross-border processing as automatically in scope. The assessment should address the processing, its necessity and proportionality, the risks to Data Subjects, and the measures to mitigate those risks.

4) Processors, subprocessors, and international transfers

The engagement of a Processor must be based on a written agreement that sets out the required minimum terms (Article 14). Where a Processor engages a further Processor (subprocessors), the Controller's prior written approval is required, and an equivalent level of protection must be maintained (Article 15). Organizations should review arrangements with cloud providers, SaaS platforms, outsourcing providers, and group entities against both requirements.

For international transfers, organizations should identify where personal data is stored, accessed, or transferred outside Indonesia, and apply the transfer basis in the order set out in Article 165. The destination must first provide an equivalent or higher level of protection. If that condition is not met, the transfer must be based on adequate and binding safeguards. Only where neither condition is met may the transfer rely on the Data Subject's consent.

5) Personal data breach readiness

PP 33/2026 sets out operational obligations for managing a personal data breach (Articles 114–118). These obligations are likely to be tested when an incident occurs:

a. written notification to the affected Data Subjects and 'the Lembaga' (the supervisory authority) within 3 × 24-hour (Article 114);

b. public notification where the breach disrupts public services or has a seriously affects the public interest (Article 115);

c. documentation of the incident and the remediation taken (Article 116);

d. internal policies, procedures, role allocation, escalation, and post-incident review (Article 117); and

e. a Processor's obligation to report a breach to the Controller at the first opportunity (Article 118).

Organizations should confirm that their breach-response procedure operates from end to end, including the 3 × 24-hour notification requirement and the assessment of whether public notification is required.

6) Governance of the data protection officer, accountability, and audits

The regulation sets out when a *Pejabat atau Petugas yang Melaksanakan Fungsi Pelindungan Data Pribadi* (PPDP, the data protection officer, or DPO) must be appointed: where processing is carried out for public services; where the organization's core activities require regular and systematic large-scale monitoring of Data Subjects; or where its core activities involve large-scale processing of specific personal data or personal data relating to criminal offences (Article 142). The appointment must reflect professionalism, knowledge of the relevant law, and competence (Article 143). The PPDP's tasks, position, access to the highest level of management, independence, resources, and avoidance of conflict of interest are set out in Articles 144–146.

Controllers must demonstrate accountability by documenting their processing activities, retaining evidence of compliance, responding to information requests from the Lembaga, and conducting internal and external personal data protection audits (Article 138). Processors carry corresponding accountability and audit obligations (Articles 139–141).

ENFORCEMENT AND SANCTIONS

For specified violations, 'the Lembaga' may issue a written warning, temporarily suspend processing, order the deletion or destruction of personal data, and/or impose an administrative fine. More than one sanction may be imposed at the same time, and a sanction need not be preceded by a written warning (Article 184).

An administrative fine may be up to 2% of the Controller's or Processor's annual revenue or annual receipts. The amount is determined by reference to factors including the impact and duration of the violation, the categories of personal data and the number of Data Subjects affected, the level of cooperation during examination, business scale, ability to pay, and compliance history (Article 185). 'The Lembaga' may also publish the results of its supervision (Article 183), which may carry reputational as well as financial consequences.

WHAT ORGANIZATIONS SHOULD DO NOW

The following actions establish where the organization stands before 16 January 2027:

1. confirm executive ownership and assess whether a PPDP appointment is required;
2. update the processing inventory and the record of cross-border data flows;
3. identify high-risk processing and any outstanding DPIAs;
4. test the Data Subject request and breach-response procedures from end to end;
5. review agreements with Processors and subprocessors;
6. identify the applicable international-transfer basis; and
7. assemble compliance evidence and establish the approach to internal and external audits.

The period to 16 January 2027 is limited. Organizations should therefore complete a baseline assessment promptly and sequence remediation according to regulatory exposure and implementation complexity. The assessment should distinguish what has already been addressed, what requires remediation, and what remains dependent on further regulations to be issued by 'the Lembaga'.

WHAT THIS MEANS IN PRACTICE — RSM VIEW

PP 33/2026 sets out the operational requirements that organizations must be able to evidence. Several matters remain subject to further regulation by 'the Lembaga'. Pending those regulations, processing may continue provided it does not conflict with the regulation (Article 223); this is not a basis for deferring implementation.

Organizations with established General Data Protection Regulation (GDPR)-aligned privacy programs may have a useful starting point, particularly for DPIA, Data Subject rights, Processor management, DPO governance, and international transfers. However, GDPR alignment does not establish Indonesian compliance. International-transfer mechanisms also remain subject to further action by 'the Lembaga': destination equivalence under Articles 167–168 and standard contractual clauses under Article 170. Organizations should therefore not assume that approved destinations or standard clauses are currently available for use.

Controllers are required to conduct internal and external personal data protection audits under Article 138, while Processors must conduct audits under Article 141. Neither provision prescribes the frequency of those audits. Organizations should therefore consider a risk-based reassessment cycle rather than treating the first audit as a one-off exercise. This is particularly relevant to DPIAs, which must be completed before the relevant processing begins and reviewed when the processing risk changes (Article 121(1) and (5)).

A formal mapping therefore remains necessary to distinguish Indonesia-specific requirements, controls that can be leveraged from existing privacy programs, and areas dependent on further regulation by 'the Lembaga'.

HOW RSM CAN HELP

RSM can help organizations establish a clear PP 33/2026 readiness baseline, identify priority gaps, and develop a sequenced implementation roadmap. Depending on the organization's needs, this may extend to targeted remediation, DPIA and privacy risk assessment, Processor governance and international-transfer arrangements, breach-response readiness, support for the PPDP operating model, and personal data protection audits.

Disclaimer: This Client Alert is provided for general information only and does not constitute legal advice. It reflects the provisions of PP 33/2026 as at the date of publication and does not account for any subsequent regulations or guidance issued by 'the Lembaga' or other competent authorities.

For further information please contact:

RSM Indonesia
Plaza ASIA Level 10
Jl. Jend. Sudirman Kav.59
Jakarta 12190
T: +62 21 5140 1340
E: inquiry@rsm.id
rsm.id