

PASAKA
RIEVAN

SMITH

Counsellors at Law

NewsLetter

7 Minute Read



September 2026

Government Regulation No. 33 of 2026:

Indonesia's PDP Framework Moves from Principle to Practice



READ MORE

pasakariEVANsmith.com

What Businesses Need to Have in Place Before 16 January 2027

Key Takeaways

- **Deadline:** PP 33/2026 was promulgated on 16 July 2026 and takes effect on 16 January 2027.
- **What changes:** The PDP Law's broad principles become operational requirements, including records of processing, DPIAs, cross-border transfer assessments, PPDP appointment and 72-hour breach notification.
- **Exposure:** Administrative fines of up to 2% of annual revenue or receipts, alongside suspension of processing and deletion of data.
- **Most affected:** Businesses using AI or data-intensive systems, companies relying on overseas group systems or cloud providers, and parties to M&A transactions.

Indonesia's personal data protection ("**PDP**") regime has entered its operational phase with the issuance, on 16 July 2026, of Government Regulation No. 33 of 2026 on the Implementation of the Personal Data Protection Law ("**PP 33/2026**").

Since the enactment of Law No. 27 of 2022 on Personal Data Protection ("**PDP Law**"), businesses have been subject to broad obligations concerning the collection, use, storage, transfer and other processing of personal data, but with little guidance on what compliance looks like in practice. PP 33/2026 fills much of that gap by setting out how these obligations are to be implemented.

The regulation will take effect on 16 January 2027, less than four months away. The question for businesses is no longer whether they have a privacy policy, but whether they can demonstrate to the regulator, customers and transaction counterparties that their day-to-day practices comply.

WHAT HAS CHANGED AND WHAT DOES IT MEAN FOR BUSINESSES?

1. Processing Activities Must Be Documented, Not Just Disclosed

PP 33/2026 sets out in greater detail the respective roles and obligations of personal data controllers (“**Controllers**”) and processors (“**Processors**”), including the obligation to keep records of processing activities. A privacy policy alone is no longer enough: businesses should be able to show what personal data they hold, why they hold it, who can access it, where it is stored and how long it is kept.

2. High-Risk Processing and Automated Decision-Making Require a DPIA Before Launch

PP 33/2026 requires a Data Protection Impact Assessment (“**DPIA**”) before high-risk processing is carried out. Triggers include large-scale processing, systematic monitoring, profiling or scoring, automated decision-making with legal or similarly significant effects on individuals, and the use of new technologies. This is relevant for businesses using AI or other data-intensive.

3. Cross-Border Data Transfers Become a More Structured, Documented Exercise

Personal data may be transferred outside Indonesia only where the recipient country provides an equivalent or higher level of protection, where adequate and binding safeguards are in place or, failing both, with the data subject’s consent. PP 33/2026 adds procedure to this framework, including a pre-transfer assessment (often referred to as a Transfer Impact Assessment (“**TIA**”)) and disclosure to data subjects before the transfer takes place.

4. Personal Data Becomes a Deal Issue in Corporate Transactions

PP 33/2026 addresses transfers of personal data in corporate actions that result in a change of Controller, such as mergers, spin-offs, acquisitions and dissolutions, including related assessment and notification obligations.

5. PPDP Appointment and Data Subject Rights Must Be Operational

PP 33/2026 clarifies when a Personal Data Protection Officer (“PPDP”) must be appointed, notably where core activities involve large-scale, regular and systematic monitoring of individuals or large-scale processing of specific personal data. It also details how data subjects may exercise their rights, including rights of access, correction, deletion and objection, and claims for compensation.

6. Data Breaches Must Be Notified Within 72 Hours

In the event of a personal data breach, the Controller must notify the affected data subjects and the PDP supervisory authority (“Authority”) in writing within 3 x 24 hours. Where a breach disrupts public services or seriously affects the public interest, the public must also be informed.

7. The Enforcement Framework Becomes More Concrete

Administrative sanctions include written warnings, temporary suspension of processing, deletion or destruction of personal data and administrative fines of up to 2% of annual revenue or receipts. PP 33/2026 sets out the factors used to determine the amount of a fine, including the severity and duration of the violation, the number of data subjects affected and the level of cooperation with the Authority. [Sanction decisions may also be published by the Authority.

FROM PRIVACY POLICIES TO DEMONSTRABLE COMPLIANCE

The practical shift under PP 33/2026 is from having PDP documents to being able to demonstrate compliance. Regulators, business partners and transaction counterparties will increasingly expect evidence: records of processing, completed DPIAs, transfer assessments, signed data processing agreements and a working breach response plan.

For businesses that already have a PDP programme in place, 16 January 2027 is an opportunity to test whether it holds up against the new, more detailed requirements. For businesses that have yet to establish one, it is a firm deadline for action.

SIX PRIORITIES BEFORE 16 JANUARY 2027

We recommend that businesses use the remaining transition period to work through the following priorities:

1. Map personal data: what is held, where it is stored, who can access it and where it flows, including outside Indonesia;
2. Review legal bases, privacy notices and consent mechanisms against PP 33/2026;
3. Review vendor and intra-group arrangements, and put data processing agreements in place with Processors;
4. Identify high-risk processing, particularly AI, profiling and monitoring tools, and schedule DPIAs;
5. Document the transfer mechanism relied on for each cross-border data flow; and

Prepare a 72-hour breach response plan and a data subject request procedure, and confirm whether a PPDP must be appointed.

HOW PRS CAN ASSIST

PP 33/2026 cuts across privacy, commercial contracts, technology, employment and corporate transactions. A generic checklist rarely captures how data actually moves through a particular business, especially where group companies and overseas service providers are involved.

PRS assists Indonesian and international clients in translating PP 33/2026 into practical, business-specific measures, including:

- **PDP Compliance Gap Assessment** — reviewing existing PDP policies, practices and governance;
- **Privacy & Data Processing Documentation** — reviewing and updating privacy policies, notices, consent mechanisms, SOPs and internal policies;
- **Controller–Processor Arrangements** — reviewing and drafting Data Processing Agreements and related vendor contracts;
- **DPIA & High-Risk Processing** — identifying activities that may trigger DPIA requirements and advising on appropriate safeguards;
- **Cross-Border Data Transfers** — assessing transfer mechanisms, safeguards and pre-transfer assessments, and preparing supporting intra-group and vendor arrangements;
- **Corporate Transaction Support** — integrating PDP considerations into M&A, restructuring and other transactions involving personal data;
- **PPDP/DPO Governance** — assessing appointment requirements and supporting appropriate governance structures;
- **Data Subject & Regulatory Readiness** — reviewing procedures for data subject requests, objections, compensation claims and regulatory inquiries; and
- **Breach Response Readiness** — preparing incident response plans and 72-hour notification procedures.

To discuss how PP 33/2026 applies to your business, please contact us at [\[inquiry\]@pasakari EvansSmith.com](mailto:[inquiry]@pasakari EvansSmith.com) or your usual PRS contact.

This publication is intended for general information only and does not constitute legal advice. Specific advice should be sought before acting on any matter discussed.

About Us

Pasaka Rievan Smith - Counsellors at Law (“**PRS**”) is comprised of a team of dedicated and trusted lawyers with over 20 years of experience in the legal industry, spanning law firms, multinational corporations, and government institutions. We provide prompt, precise legal counsel and opinions, offering both legal and commercial perspectives to support corporate clients. Confident in our ability to meet the diverse needs of our clients, PRS enables them to focus on achieving their business objectives. With experience in assisting start-ups, growing enterprises, established organizations, and family-owned businesses, we are committed to delivering both personal and professional attention, ensuring the utmost satisfaction for our clients.

This article was prepared by:



OMAR SYARIEF SMITH
Partner
omarsmith@pasakariEVANsmith.com



ATINA PUTRI INDIRA
Associate
indira@pasakariEVANsmith.com



FAHREZA AHMAD SUGIANTO
Associate
sugianto@pasakariEVANsmith.com

This article was prepared by PRS as part of our ongoing effort to provide insights into recent regulatory developments and their practical implications for businesses and investors. The information contained herein is intended for general informational purposes only and should not be construed or relied upon as legal advice. While we strive to ensure the accuracy and relevance of the content at the time of publication, PRS makes no representations or warranties as to its completeness or continuing validity. Readers are encouraged to seek specific legal counsel before making decisions based on this material.

Should you wish to learn more about this topic or require tailored legal advice, please contact us at inquiry@pasakariEVANsmith.com — our qualified lawyers will be pleased to assist you.