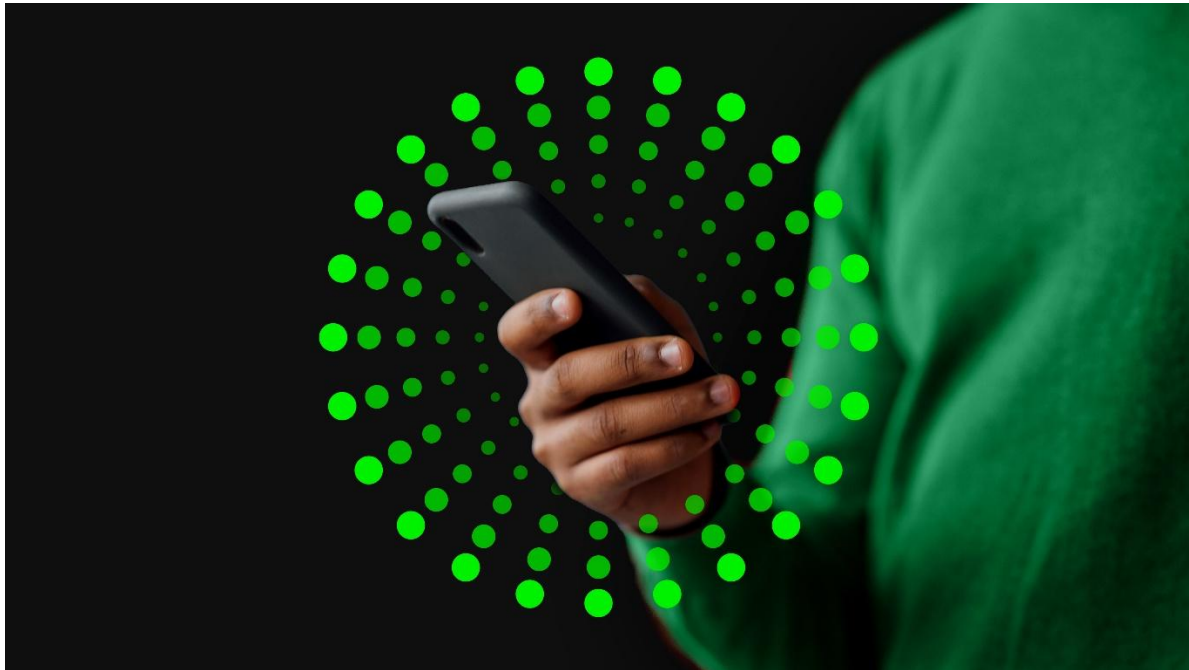




Client Alert October 2026

Indonesia's implementing regulation for personal data protection

Government Regulation Number 33 of 2026 on the Implementation of Law Number 27 of 2022 on Personal Data Protection

Background

Indonesia's personal data protection framework is governed by Law Number 27 of 2022 on Personal Data Protection (PDP Law), which establishes the general rights, obligations, and principles applicable to the processing and protection of personal data. To provide further guidance on the implementation of the PDP Law, the government has enacted Regulation Number 33 of 2026 on the Implementation of Law Number 27 of 2022 (GR PDP). GR PDP was promulgated on 16 July 2026 and will enter into force six months after its promulgation, on 16 January 2027.

Overview

With the enactment of GR PDP, the obligations and implementation mechanisms previously contemplated in the Draft GR PDP (PDP Bill) are now formally established. These include provisions concerning the processing of personal data, rights of data subjects, obligations of data controllers and data processors, cross-border transfers, personal data protection impact assessments, personal data protection failures, supervision, and administrative sanctions.

Compared with the previously circulated PDP Bill, GR PDP introduces several additional provisions, including two new chapters: Chapter VII on Public Participation and Chapter XI on Transitional Provisions. GR PDP also expands certain provisions that may have practical implications for businesses, including obligations to notify data subjects of certain corporate actions and requirement concerning personal data protection agreements between relevant data controllers. It also strengthens the supervisory and

enforcement powers of the governmental body responsible for administering personal data protection (hereinafter referred as Institution (*Lembaga*)¹.

Given the enactment of GR PDP, businesses should ensure that their existing personal data protection frameworks are compliant with the requirements under GR PDP, including any newly introduced or further elaborated requirement, and make any necessary adjustments ahead of its effective date. In particular, businesses involved in corporate transactions, cross-border data transfers, or the processing of personal data through third-party service providers may wish to assess the potential implications of the new requirements for their existing structures and arrangements.

Key provisions

Corporate actions involving personal data

One of the notable developments under GR PDP is the introduction of obligations relating to corporate actions involving personal data (i.e. mergers, consolidations, acquisitions, spin-offs, and dissolutions of legal entities). In general, the relevant data controllers are required to notify data subjects of the transfer of their personal data both before and after the implementation of the corporate actions and, where personal data is transferred to a new data controller, enter into a personal data protection agreement with the new data controller.²

Accordingly, businesses intending to undertake corporate actions should take these obligations into account in the relevant legal due diligence, transaction structuring, contractual arrangements, and post-closing integration processes where a transaction involves personal data held in or processed through the relevant assets, records, systems, or operations.

Cross-border data transfers

In line with the previously circulated PDP Bill, GR PDP provides further guidance on the transfer of personal data outside Indonesia. In particular, GR PDP requires data controllers and/or data processors to:³

- Record and map the personal data transfer cycle, including the implications of the transfer;
- Apply data minimization by ensuring that the personal data transferred is adequate, relevant, and limited to what is necessary for the purpose of the transfer;
- Identify the applicable legal instrument that serves as the basis or reference for the personal data transfer in accordance with applicable laws and regulations;
- Assess the effectiveness of the applicable legal instrument before carrying out the relevant personal data transfer;
- Implement supplementary measures where necessary, which may include contractual, technical, and/or organizational measures;
- Establish procedural steps for the use of supplementary measures, where such measures are required; and
- Conduct periodic reassessments of the relevant transfer arrangements within an appropriate period.

This provision is particularly relevant for multinational groups and businesses that operate through overseas affiliates or regional headquarters or engage international service providers in the course of their operations. The implications may also extend to vendor and outsourcing arrangements where Indonesian personal data is processed outside Indonesia. Businesses should consider whether existing cross-border data transfer arrangements, including contractual safeguards and internal data transfer mechanisms, are aligned with the requirements under GR PDP.

¹ An Institution (*Lembaga*) refers to the body responsible for administering personal data protection as set out in the PDP Law.

² Articles 148–152 of PDP Bill

³ Article 161 of GR PDP

Obligation to appoint a personal data protection officer

GR PDP expressly requires data controllers and data processors to appoint a personal data protection officer⁴ (*Pejabat Pelindungan Data Pribadi* (PPDP)), if certain conditions are met, including where:⁵

- The personal data is processed for public services;
- The core activities involve large-scale regular and systematic monitoring of personal data; and/or
- The core activities involve large-scale processing of specific personal data and/or personal data relating to criminal offenses.

The use of “and/or” above reflects Constitutional Court Decision Number 151/PUU-XXII/2024 (please refer to [Client Alert - August 2025](#)), which amended the corresponding provision under the PDP Law⁶ so that each criterion can apply independently, rather than requiring all criteria to be fulfilled cumulatively.

Enhanced supervision and administrative sanctions

With GR PDP becomes effective starting 16 January 2027, data controllers and data processors are expected to be compliant with the regulation. Compliance will be supervised by the personal data protection Institution (*Lembaga*), which is empowered to monitor compliance and address violations through administrative sanctions. Such administrative sanctions may be in the form of a written warning, temporary suspension of personal data processing, erasure or disposal of personal data, and/or administrative fines.⁷

The imposition of administrative sanctions under GR PDP is to be determined by taking into consideration the following aspects:⁸

- The level or impact of the violation committed by the data controller and/or data processor;
- The continuity of the business activities or public services of the relevant data controller and/or data processor;
- The compliance record of the data controller and/or data processor with applicable personal data protection laws and regulations;
- Clear considerations and grounds supporting the imposition of the relevant sanction; and
- Other considerations that may be determined by the Institution.

These considerations provide a framework for determining the appropriate administrative sanctions by taking into account the specific circumstances of each violation, including its impact, the controller or processor’s compliance history, and other relevant factors. Accordingly, the applicable sanctions may vary depending on the circumstances and characteristics of each case. Businesses should therefore maintain an appropriate compliance record and documentation demonstrating their efforts to comply with personal data protection requirements.

Additional chapters in GR PDP

GR PDP introduces two additional chapters that were not previously included in the PDP Bill:

Chapter VII – Public participation

This chapter provides a framework for public participation in supporting the implementation of personal data protection, including through education, training, advocacy, dissemination, and supervision. Although the provisions on public participation currently provide only a general framework, they establish a basis for greater public awareness and engagement in personal data protection as well as for further

⁴ A data protection officer (*Pejabat atau Petugas yang Melaksanakan Fungsi Pelindungan Data Pribadi*) is an official responsible for ensuring compliance with the principles of personal data protection and for mitigating the risk of personal data protection breaches; Article 1 point 25 of GR PDP.

⁵ Article 142 paragraph (1) of GR PDP.

⁶ Article 53 paragraph (1) of PDP Law.

⁷ Article 184 paragraph (2) of GR PDP.

⁸ Article 184 paragraph (6) of GR PDP.

implementing measures and initiatives, including regulations issued by the Institution (*Peraturan Lembaga*).⁹

Chapter XI – Transitional provisions

The chapter provides transitional arrangements pending the issuance of further regulations by the Institution concerning personal data processing. In particular, until the relevant regulation is issued by the Institution, data controllers and/or data processors may continue processing personal data, provided that such processing does not conflict with GR PDP¹⁰. Businesses should use this transitional period to assess and update their personal data processing arrangements, while also monitoring the issuance of further implementing regulations.

These provisions provide additional clarity on public participation and the transitional position of businesses as PDP framework is further implemented.

Detailed operational requirements

GR PDP sets out certain requirements in greater detail than those contemplated in the PDP Bill. These include requirements relating to legal bases for processing, consent, internal processing policies, appointment and functions of personnel responsible for personal data protection, personal data protection impact assessments, personal data protection failures, and arrangements between data controllers and data processors. Accordingly, businesses should review their existing personal data protection frameworks to assess whether their policies, procedures, and practices remain aligned with the requirements under GR PDP and to identify any areas that may require adjustment.

Further implementation through regulations issued by the Institution

GR PDP provides that certain aspects of the personal data protection framework will be further regulated through regulations issued by the Institution. The government has planned to establish the Institution, which is expected to exercise supervisory and enforcement powers, including the authority to impose administrative sanctions. As of the date of issuance of GR PDP, however, the Institution has not yet been established.

Nevertheless, GR PDP requires the Institution, once established, to issue further regulations providing additional detail on certain technical and operational matters relating to personal data processing and the fulfillment of obligations under GR PDP. The matters contemplated to be further regulated through the regulations issued by the Institution include, among others:

- Combination of personal data;
- Use of other legitimate interests as a basis for processing;
- Requests for and provisions of information;
- Verification process;
- Automatic processing;
- Mechanisms for postponing and restricting processing;
- Mechanisms for exercising the right to obtain and use data portability and interoperability;
- Supervision by the data controller;
- Obligation to appoint a PPDP and requirements concerning the professionalism and competence of the PPDP;
- Implementation of consent for the transfer of personal data outside the jurisdiction of Indonesia;
- Public participation;
- Mechanisms relating to alleged violations of personal data protection; and
- Dispute resolution.

⁹ Article 179 of GR PDP.

¹⁰ Article 223 of GR PDP.

The issuance of these implementing regulations will therefore be an important development for businesses. Accordingly, businesses should monitor the issuance of the relevant regulations by the Institution and consider whether their compliance frameworks will need to be further adjusted once the implementing regulations are available.

Key takeaways

- GR PDP was promulgated on 16 July 2026 and will become effective on 16 January 2027, giving businesses six months to review their existing personal data protection arrangements and make any necessary adjustments to comply with the requirements under GR PDP before it takes effect.
- GR PDP formally establishes the obligations applicable to data controllers and data processors, including those relating to personal data processing, governance, impact assessments, personal data protection failures, and controller–processor arrangements. It also expressly addresses personal data requirements in corporate actions, including mergers, acquisitions, consolidations, spin-offs, and dissolutions.
- Certain technical and operational aspects of GR PDP will remain subject to regulations issued by the Institution, and businesses should continue monitoring these developments as further adjustments may be required to existing policies, procedures, contractual arrangements, and governance frameworks.

Stefanus Brian Audyanto
Managing Partner

saudyanto@deloittelegal-id.com

Anthony Pratama Chandra
Partner

anchandra@deloittelegal-id.com

Derryan Rahmat Putra
Junior Partner

dputra@deloittelegal-id.com

Ricardo Nathanael Ginting
Junior Partner

rginting@deloittelegal-id.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

About Deloitte Legal

Deloitte Legal means the legal practices of DTTL member firms, their affiliates or their related entities that provide legal services. The exact nature of these relationships and provision of legal services differs by jurisdiction, to allow compliance with local laws and professional regulations. Each Deloitte Legal practice is legally separate and independent, and cannot obligate any other Deloitte Legal practice. Each Deloitte Legal practice is liable only for its own acts and omissions, and not those of other Deloitte Legal practices. For legal, regulatory and other reasons, not all member firms, their affiliates or their related entities provide legal services or are associated with Deloitte Legal practices.

About Deloitte Legal Indonesia

Deloitte Legal Indonesia is a member of Deloitte Legal network. Deloitte Legal Indonesia provides only legal services, and it is legally separate and independent from other Deloitte entities.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2026 Deloitte Legal Indonesia.