TRILEXICA
AT LAW

CLIENT ALERT · 31 August 2026

Indonesia's New Personal Data Protection Regulation

What Government Regulation No. 33 of 2026 Means for Your Business

A Six-Month Runway to Comply with the PDP Law's Implementing Regulation

DATA PROTECTION & PRIVACY PRACTICE GROUP

CLIENT ALERT

Indonesia's New Personal Data Protection Regulation: What Government Regulation No. 33 of 2026 Means for Your Business

A Six-Month Runway to Comply with the PDP Law's Implementing Regulation

By **Trilexica Data Protection & Privacy Practice Group**

IN BRIEF

a. Government Regulation No. 33 of 2026 on the Implementing Regulation of Law No. 27 of 2022 on Personal Data Protection ("**GR 33/2026**") was enacted and promulgated on **16 July 2026** and will enter into force on six months later, **16 January 2027** (GR 33/2026, Art. 225), giving businesses a defined compliance runway.

b. A new "Transitional Provisions" chapter allows controllers and processors to continue processing personal data pending the issuance of implementing regulations by the data protection authority (the "**DPA**"), so long as such processing does not conflict with GR 33/2026.

c. Administrative fines remain capped at up to 2% of annual revenue, but GR 33/2026 now specifies the calculation factors, rather than deferring the entire methodology to future DPA regulation.

d. Businesses that process personal data in Indonesia, or that process the personal data of Indonesian data subjects from abroad, should complete their compliance gap assessment before **16 January 2027**, particularly around legal bases for processing, mandatory appointment of a data protection officer (now termed **"PPDP"**), breach notification, and cross-border data transfer.

The bottom line: *businesses should treat 16 January 2027 as a hard compliance deadline and begin gap assessments now.*

On 16 July 2026, the government has enacted and promulgated GR 33/2026, nearly four years after Indonesia's Law No. 27 of 2022 on Personal Data Protection (the **"PDP Law"**) came into force. GR 33/2026 was published in the State Gazette (*Lembaran Negara*) of the Republic of Indonesia Year 2026 Number 88, and is countersigned by the Minister of State Secretariat. It is the primary implementing regulation mandated under the PDP Law and provides long-awaited operational detail on, among other things, the

legal bases for processing personal data, data subject rights, the appointment of PPDP, personal data breach notification procedures, cross-border data transfer mechanisms, supervision of controller compliance, and administrative sanctions.

This Client Alert highlights the key features of GR 33/2026 and, where relevant, compares them with the publicly circulated draft dated 31 August 2023 (the "**August 2023 Draft**"). Further analysis of GR 33/2026 and the relevant developments from the August 2023 Draft is set out below.

1. Background

The PDP Law was enacted on 17 October 2022 as Indonesia's first comprehensive, cross-sectoral personal data protection framework. The PDP Law set out core principles, obligations, and sanctions but left a significant number of operational matters to be regulated further through implementing regulations, principally a Government Regulation (*Peraturan Pemerintah*).

The PDP Law expressly mandated further regulation by Government Regulation under, among others, Articles 10(2), 12(2), 13(3), 16(3), 34(3), 48(5), 54(3), 56(5), 57(5), and 61 — the same recital basis carried into GR 33/2026 itself. The PDP Law also provided a two-year transition period for compliance, which lapsed in October 2024; businesses have therefore technically been required to comply with the PDP Law's substantive obligations since that date, even without full implementing regulations in place.

GR 33/2026 follows a lengthy drafting process, starting with the publicly circulated the **August 2023 Draft** and continuing through a later harmonized draft prepared in March 2025. The March 2025 draft reflected further input from, among others, the Coordinating Ministry, the Ministry of Communication and Digital Affairs, the Ministry of Health, the National Cyber and Crypto Agency, the National Archives, the Ministry of Law, and the Ministry of State Secretariat, with a number of issues still under inter-ministerial discussion at that stage. As the March 2025 draft remained subject to the ongoing drafting and harmonization process, this Client Alert uses the August 2023 Draft as its comparison baseline. GR 33/2026 was ultimately issued nearly three years after the August 2023 Draft and almost four years after the PDP Law itself.

2. Scope and Structure of GR 33/2026

GR 33/2026 comprises 225 articles across 12 chapters, compared with 245 articles across 10 chapters in the August 2023 Draft. Although the final regulation contains fewer articles, its overall structure has been meaningfully reorganized: the August 2023 Draft's dedicated chapter on the powers of the DPA have been redistributed across the relevant substantive chapters, the chapter on rights and obligations has been consolidated from 24 to 23 named parts, and new standalone chapters on "Public Participation" and "Transitional Provisions" have been added. The scope of the regulation has also been reframed from eight principal subject areas in the August 2023 Draft to nine under GR 33/2026, with "Public Participation" and "Supervision of Controller Compliance" now identified as separate subject areas.

Chapter	Title	Key Topics (per GR 33/2026)
I	**General Provisions**	Definitions (including a broadened definition of "Personal Data Protection Breach" or "*Kegagalan Pelindungan Data Pribadi*"); territorial and extraterritorial scope; and the personal or household-use exemption.
II	**Personal Data**	Classification of personal data into specific and general personal data. Unlike the August 2023 Draft, GR 33/2026 no longer contains a separate provision setting out the "elements" of personal data.
III	**Processing of Personal Data**	Categories of processing activities; core personal data protection principles; parties involved in processing, including controllers, processors and joint controllers; and rules on visual monitoring devices (e.g., CCTV).
IV	**Rights and Obligations**	Comprising 23 named parts, covering, among others: general provisions on the exercise of data subject rights; legal bases for processing; limited and specific processing; requests for and provision of information; purpose limitation; accuracy, completeness and consistency; completion, updating and/or correction; recording of processing activities; access and copies; termination of processing, erasure and

Chapter	Title	Key Topics (per GR 33/2026)
		destruction; withdrawal of consent; objections to automated processing; suspension and restriction of processing; claims and compensation; portability and interoperability; Personal Data Breach notification; data protection impact assessments (DPIA); data security; transfer of Personal Data in corporate actions; accountability; processor obligations; PPDP (Data Protection Officer); and exemptions from rights and obligations.
V	**Transfer of Personal Data Outside Indonesia**	Hierarchy of cross-border transfer mechanisms: (i) an equivalent or higher level of personal data protection in the recipient jurisdiction; (ii) adequate and binding safeguards; and (iii) consent where the preceding mechanisms are unavailable.
VI	**International Cooperation**	Bilateral, regional and multilateral cooperation on personal data protection.
VII	**Public Participation**	New chapter. Role of the public in the oversight of personal data protection, through education, training, advocacy, socialization and/or supervision.
VIII	**Supervision of Controller Compliance**	The DPA's supervisory powers, authority to issue written orders to controllers and/or processors, and publication of supervisory outcomes.
IX	**Administrative Sanctions**	Types of administrative sanctions; investigation and enforcement procedures; administrative objections; and the framework for determining administrative fines.
X	**Dispute Resolution**	Resolution through arbitration, courts or other alternative dispute resolution mechanisms; reporting and verification of disputes by the DPA; DPA-facilitated dispute resolution; and mediation through registered mediators or Mediation Institution (*Lembaga Mediasi).*
XI	**Transitional Provisions**	New chapter. Pending issuance of the DPA's implementing regulations, controllers and/or processors may continue processing personal data so long as this does not conflict with GR 33/2026.
XII	**Closing Provisions**	Entry into force six months after promulgation (16 January 2027).

3. Key Provisions

The following summarises the substantive areas most relevant to businesses under the final GR 33/2026.

3.1 Categories of Personal Data

GR 33/2026 retains largely the same categories of personal data as the August 2023 Draft, distinguishing between **specific personal data** (health data and information, biometric data, genetic data, criminal records, children's data, personal financial data, and other categories to be determined by the relevant ministry/agency in coordination with the DPA, taking into account whether the processing of such personal data may have a greater impact on data subjects, including discriminatory treatment, material/immaterial loss, or other impacts contrary to data subjects' rights) and **general personal data** (full name, sex, nationality, religion, marital status, and personal data combined to identify an individual, including through direct reference, mapping reference, triangulation, or other combination methods, which may draw on publicly available data). GR 33/2026 now expressly provides that further rules on the combination of personal data will be regulated under a future DPA regulation (Art. 7(4)).

3.2 Legal Bases for Processing

GR 33/2026 retains the six legal bases set out in the PDP Law and previously reflected in the August 2023 Draft. Controllers must have a legal basis for processing personal data, and such legal basis must exist before the controller carries out the relevant personal data processing activities (Art. 30(1) – (2)). The legal bases are: (i) explicit valid consent; (ii) performance of a contract; (iii) compliance with a legal obligation; (iv) protection of the data subject's vital interests, which the Elucidation clarifies covers circumstances relating to the data subject's survival, such as where processing is necessary for serious medical treatment; (v) performance of tasks in the public interest, public service, or exercise of authority under applicable laws and regulations; and/or (vi) fulfilment of other legitimate interests, taking into account the purpose, needs, and balance between the controller's interests and the data subject's rights (Art. 30(3)).

3.3 Data Subject Rights and Consent Mechanics

Chapter IV of GR 33/2026 sets out detailed provisions on data subject rights and controller obligations, including dedicated parts on **withdrawal of consent** (Arts. 90 – 92), **objection to processing based on automated decision-making** (Arts. 93 – 96), **suspension and restriction of processing** (Arts. 97 – 104), **claims and compensation** (Arts. 105 – 110), and **data portability and interoperability** (Arts. 111 – 113). Data subjects (or their authorized representatives, parents/guardians for children, or guardians for persons with disabilities) exercise their rights through a recorded request submitted electronically or non-electronically, with controllers required to provide an accessible request channel and to verify requests proportionately. (Arts. 20 – 25, 38 – 39).

For consent-based processing, GR 33/2026 clarifies that explicit consent must be obtained **freely, knowingly, specifically, and unambiguously** (Art. 32(2))**.** The Elucidation further explains that consent may be considered ambiguous where consent to personal data processing is bundled with acceptance of general terms and conditions, such that merely reading the terms and conditions is deemed to constitute consent (Elucidation of Art. 32(2))**.**

3.4 Data Protection Officer (now "PPDP")

GR 33/2026 renames the data protection officer role as the **"*Pejabat atau Petugas yang Melaksanakan Fungsi Pelindungan Data Pribadi*"**, or **PPDP** (the August 2023 Draft had used "*Pejabat Petugas Pelindung Data Pribadi*"). A controller or processor must appoint a PPDP where the statutory threshold applies, namely: (a) processing is for public service purposes; (b) its core activities, by their nature, scope, and/or purpose, require regular and systematic monitoring of personal data on a large scale; and/or (c) its core activities consist of large-scale processing of specific personal data and/or data relating to criminal offenses (Art. 142). The PPDP is appointed on the basis of professionalism, legal knowledge, personal data protection practice, and capability to perform the role, may be one person or several, and may be sourced from inside and/or outside the controller's or processor's organization (Arts. 143 – 144). Further detail on the obligation to appoint a PPDP, PPDP professionalism and competence, and PPDP appointment mechanics is left to future DPA regulation (Arts. 142 – 144).

3.5 Personal Data Breach Notification

GR 33/2026 adopts the broader definition of a **"*Kegagalan Pelindungan Data Pribadi*"** (personal data breach) in its general definitions, reflecting the definition previously set out in the Elucidation of Article 46(1) of the PDP Law. Under the GR 33/2026, a personal data breach means a failure to protect the confidentiality, integrity, and availability of personal data, including any security breach, whether intentional or unintentional, that leads to the destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data that is transmitted, stored, or otherwise processed (Art. 1(18)).

A controller must notify both the affected data subject and the DPA in writing within **3 x 24 hours**, counted from when the breach is known with certainty, propriety and reasonableness (Art. 114(1) – (2)). **GR 33/2026 does not expressly provide a materiality or risk threshold for omitting notification**. The notification must at least include the personal data disclosed, when and how the personal data was disclosed, the controller's handling and recovery measures, and information on the PPDP or contact person appointed by the controller (Art. 114(3) – (4))**.**

A further public notification obligation applies where the breach disrupts public services and/or has a serious impact on the public interest (Art. 115). Controllers must also maintain internal breach-

handling documentation and internal breach prevention and response policies/procedures (Arts. 116 – 117), and a processor must report a breach to its controller "at the first opportunity" (Art. 118).

3.6 Visual Monitoring Devices (CCTV)

GR 33/2026 refines the August 2023 Draft's provisions on visual processing or visual data processing devices. The August 2023 Draft prohibited controllers and/or processors from placing such devices in areas where individuals have an expectation of privacy and required them to prevent or minimise recordings of persons or property outside the monitoring purpose. GR 33/2026 instead provides that installation of visual monitoring devices in public places and/or public service facilities must be for specified purposes, namely security, disaster prevention, and/or traffic operations or the collection, analysis, and regulation of traffic information (Art. 17(1)).

GR 33/2026 also requires information to be displayed in areas where visual monitoring devices are installed and provides that such devices must not be used to identify individuals (Art. 17(1)(b) – (c), 19). These information-display and no-identification requirements do not apply where the devices are used for crime prevention or law enforcement purposes (Art. 17(2)). In addition, GR 33/2026 expressly requires the installation of visual monitoring devices to continue to take privacy aspects into account (Art. 17(4)). Controllers and/or processors must also ensure consistent recording, ensure personal data protection, and use the devices only to monitor the intended area in accordance with the monitoring purpose (Art. 18).

3.7 Cross-Border Transfer of Personal Data

GR 33/2026 retains the three-tier hierarchy of transfer mechanisms from the August 2023 Draft, now set out across four parts of Chapter V: (i) transfer to a jurisdiction with an equivalent or higher level of data protection than Indonesia's; (ii) transfer subject to adequate and binding data protection safeguards; and (iii) transfer based on the data subject's consent (Art. 165).

Controllers may transfer personal data to controllers and/or processors outside Indonesia, provided that the transferring controller and the receiving party comply with the applicable personal data protection requirements under Indonesian law and regulations (Art. 160). Before carrying out a cross-border transfer, controllers must also provide information to data subjects regarding the transfer, including the transfer purpose, the existence of the relevant personal data protection instrument, protection mechanisms to ensure that data subjects may exercise their rights, and transfer risks and mitigation measures (Art. 164).

3.8 Institutional Framework – the Data Protection Authority

The August 2023 Draft contained a dedicated chapter on the authority of the personal data protection institution (*Bab VII – Kewenangan Lembaga Pelindungan Data Pribadi*) covering broad policymaking, supervisory, administrative enforcement, and dispute-facilitation functions. **GR 33/2026 does not carry forward that dedicated DPA authority chapter**. The final regulation's Chapter VIII is instead titled "**Supervision of Controller Compliance**" and focuses on the DPA's authority to supervise controller compliance, issue written follow-up orders to controllers/processors, and publish supervisory findings (Arts. 180 – 183). GR 33/2026 does not address the DPA's own establishment, structure, leadership, or reporting line. **This suggests that the institutional design of Indonesia's data protection authority remains to be addressed outside GR 33/2026**, consistent with the PDP Law, which provides that further provisions on the institution are to be regulated by Presidential Regulation. This is relevant for clients monitoring the establishment and operationalisation of Indonesia's DPA.

3.9 Supervision of Compliance

The DPA has express authority to supervise controller compliance through monitoring, control, inspection, and investigation of suspected personal data protection violations. In carrying out such supervision, the DPA may coordinate with ministries/agencies and/or involve public participation in accordance with applicable laws and regulations (Art. 180). It may issue written orders to controllers/processors, including to fulfil data subject rights, perform controller/processor obligations, stop or restrict processing, or stop or amend agreements with third parties that are suspected to harm data subjects or the public (Art. 181). The DPA may also publish the results of its supervisory activities (Art. 183).

3.10 Administrative Sanctions

GR 33/2026 retains the four categories of administrative sanction under the PDP Law: (i) written warning, (ii) temporary suspension of personal data processing activities, (iii) deletion or destruction of personal data, and/or (iv) administrative fines (Art. 184(2)). GR 33/2026 further provides that more than one administrative sanction may be imposed concurrently, and that administrative sanctions may be imposed with or without a prior written warning (Art. 184(7) – (8)).

Administrative fines remain capped at **up to 2% of annual revenue or annual receipts**. The August 2023 Draft already included the 2% cap and violation variables, and GR 33/2026 retains and refines this framework. The violation variables include the negative impact caused, the duration of the violation, the type of personal data affected, the number of affected data subjects, how the violation was discovered, the controller's and/or processor's openness and cooperation during investigation, business scale, ability to pay, compliance, and other relevant variables determined by the DPA (Art. 185(1) – (2)).

GR 33/2026 also expressly provides that, with certain considerations, administrative fines may be set at as low as **Rp0 or 0% (Art. 185(3))**. Administrative fines are calculated in accordance with applicable laws and regulations on non-tax state revenue, and fines stipulated in a final and binding DPA decision are payable to the state treasury as non-tax state revenue (Arts. 185(4), 186(1)).

3.11 Dispute Resolution

General dispute resolution avenues remain available, including arbitration, the courts, or other alternative dispute resolution institutions (Art. 200). GR 33/2026 also sets out a structured reporting and dispute-facilitation channel through the DPA: a data subject, controller, or processor may lodge a report with the DPA, which issues a registration number and verifies the report; where the verification reveals a suspected criminal element, the matter may be referred to the police; where it reveals an administrative violation, the DPA pursues administrative enforcement; and where neither applies, the DPA facilitates resolution between the parties (Arts. 201 – 205). Dispute facilitation by the DPA prioritises mediation (Art. 206), with further provisions on mediators, mediation institutions, mediation procedures, settlement agreements, and follow-up actions set out in the subsequent provisions (Arts. 207 – 222).

4. Effective Date and Transitional Arrangements

GR 33/2026 was promulgated on 16 July 2026 and, under Article 225, **comes into force six months later, on 16 January 2027**. Article 224 confirms that existing personal-data-related regulations continue to apply to the extent they do not conflict with GR 33/2026. Under the new Article 223 ("Transitional Provisions"), pending the issuance of DPA regulation on personal data processing, controllers and processors may continue processing personal data, provided that such processing does not conflict with GR 33/2026. In practice, businesses should not wait for those DPA regulation before beginning to align their practices with GR 33/2026 itself.

5. Practical Implications and Recommended Actions

With a defined compliance deadline of **16 January 2027**, we recommend that businesses consider, as applicable to their respective personal data processing activities, the following actions:

a. Map personal data processing activities and document the applicable legal basis relied upon for each processing activity.

b. Assess whether the PPDP appointment threshold under Article 142 applies and, if so, begin the appointment process.

c. Review and update privacy notices, consent mechanisms (including consent withdrawal flows), and internal data protection policies to reflect the detailed rights in Chapter IV of GR 33/2026, including objection to automated decision-making, data portability, suspension/restriction of processing, and claims for compensation.

d. Build or refresh a personal data breach response plan capable of meeting the 3 x 24-hour notification requirement to both affected data subjects and the DPA, noting that GR 33/2026 does not expressly provide a materiality or risk threshold for omitting notification.

e. Conduct data protection impact assessments (DPIA) for higher-risk processing activities and document the outcomes.

f. Review cross-border data transfer arrangements (including intra-group transfers and cloud/SaaS vendors) against the three-tier transfer hierarchy in Chapter V of GR 33/2026.

g. Review CCTV/visual monitoring purposes, notices/signage, no-identification rules, retention practices, and access controls against the updated "aspects of privacy" requirement.

h. Review data handling protocols for prospective mergers, demergers, acquisitions, consolidations or dissolutions, given the dedicated provisions on personal data handling in corporate actions.

i. Monitor for forthcoming DPA regulation, including those expected to cover internal personal data processing rules, PPDP appointment and competence, cross-border transfer mechanisms, administrative-sanction procedures, and dispute-resolution/mediation procedures, as well as the separate Presidential Regulation on the DPA's institutional design.

6. What to Watch Next

GR 33/2026 is a major step toward operationalising Indonesia's PDP Law, but it is not the end of the rulemaking process. A significant number of matters remain subject to regulations of the DPA. Priority areas to monitor include:

a. guidelines for internal personal data processing rules;

b. detailed DPIA requirements;

c. PPDP appointment, professionalism and competence requirements;

d. adequacy assessments, adequate and binding safeguards, and consent-based cross-border transfers;

e. breach-notification procedures;

f. administrative-sanction procedures; and

g. dispute resolution through the DPA and mediator competence requirements.

7. How Trilexica Can Help

TRILEXICA's Data Protection & Privacy team can assist businesses in preparing for and implementing GR 33/2026, including by conducting regulatory gap assessments, updating privacy governance frameworks, internal policies and procedures, reviewing data processing and cross-border transfer arrangements, strengthening DPIA, PPDP and breach-response frameworks, and providing practical support in remediating identified compliance gaps. We can also assist clients in developing a prioritised implementation roadmap to achieve compliance ahead of GR 33/2026 becoming effective on 16 January 2027.

OUR DATA PROTECTION & PRIVACY TEAM

Affan Giffari
Co-Managing Partner
E affan.giffari@trilexica.id

Khalisha Dhia
Associate
E khalisha.dhia@trilexica.id

Ratih Pancaringdyah
Associate
E ratih.pancaringdyah@trilexica.id