UMBRA
STRATEGIC LEGAL SOLUTIONS

NO FIRM LIKE US WE SPEAK YOUR LANGUAGE

NEWSLETTER

11 September 2026

INDONESIA'S NEW PERSONAL DATA PROTECTION IMPLEMENTING REGULATION: POINTS OF REFLECTION

Putu Raditya Nugraha, S.H., Adv. LLM
Senior Partner
+62 812 9410 3923
raditya@umbra.law

Shella Felicia, S.H.
Associate
shella@umbra.law

UMBRA – STRATEGIC LEGAL SOLUTIONS
Telkom Landmark Tower, 49th Floor
The Telkom Hub, Jl. Gatot Subroto Kav. 52
Jakarta 12710 – Indonesia
(+62) 21 5082 0999

An Overview

Following the enactment of Law Number 27 of 2022 on Personal Data Protection (the **PDP Law**), its implementing regulation, Indonesian Government Regulation Number 33 of 2026 (the **GR 33/2026**), has finally been enacted. GR 33/2026 will enter into force on 16 January 2027, six months after its enactment on 16 July 2026.

Although GR 33/2026 was enacted on 16 July 2026, the copy of GR 33/2026 has only recently been circulated unofficially. Such copy serves as the basis for preparing this client alert. As of the date of this newsletter, GR 33/2026 has not yet been published through an official channel, namely at https://www.peraturan.go.id/.

As an implementing regulation of the PDP Law, GR 33/2026 introduces a substantial set of operational requirements, procedural mechanisms, and compliance consequences that were not addressed under the PDP Law. Nevertheless, the implementation of certain aspects under GR 33/2026 further depends on the establishment of the Data Protection Authority (the **DPA**) and the issuance of implementing regulations, standards, and procedures by the DPA. Despite the issuance of GR 33/2026, the DPA has not yet been established as of the date of this newsletter, which remains a significant outstanding issue.

We set out below the highlighted developments and potential compliance gaps under GR 33/2026.

Basis of Personal Data Processing

GR 33/2026 provides greater details than the PDP Law on the requirements applicable to the bases for Personal Data processing. One requirement applied consistently across these bases is that Personal Data processing must adhere to specific purposes that are expressly and clearly communicated to Personal Data Subjects (each, the **Subject**), while taking into consideration the need to balance their interests. From a practical perspective, this reflects a clear shift away from generic bases, such as broad consent, towards bases tied to specific processing purposes.

We highlight below some developments that we view as potential gap in relation to some bases for Personal Data processing to be considered:

(a) **A valid consent**. A Personal Data Controller (the **Controller**) is required to provide a mechanism through which a Subject can provide and withdraw his/her consent for the processing of their Personal Data, whether electronically or non-electronically. GR 33/2026 further specifies examples of a consent mechanism, which includes a consent field, page, or feature. Accordingly, businesses may need to consider consequences of implementation of such consent withdrawal from an operational and compliance perspective.

A Subject's consent must be procured freely, consciously, specifically, and unambiguously. In particular, the elucidation of GR 33/2026 suggests that businesses may no longer rely on a Subject's consent to the Controller's terms and conditions for carrying out Personal Data processing, because such consent may result in ambiguity as to the Personal Data processing to which the Subject has consented.

As an additional point worth noting, GR 33/2026 expressly requires a Controller to provide goods or services to a Subject who does not consent to the processing of his/her Personal Data without reducing the quality of such goods or services, unless the provision of such goods or services requires the processing of Personal Data.

(b) **Satisfaction of obligations under an underlying agreement**. GR 33/2026 specifies certain cases where this basis can be relied upon for Personal Data processing, namely, (i) to perform an agreement to which the relevant Subject is a party, or (ii) to fulfil the relevant Subject's pre-contractual request.

It also sets out certain conditions for relying on this basis, including, among others, that (i) the processing is necessary for a Controller to perform the relevant underlying agreement, and (ii) the Personal Data Protection measures for the relevant Subject have been fulfilled. In regard to point (i), GR 33/2026 does not specify the criteria for determining whether such Personal Data processing is "necessary" for performing the underlying agreement.

In addition, an underlying agreement as a basis for Personal Data processing is required to cover, **at least:**

(i) details and description of the purpose of Personal Data processing;

(ii) connection between the Personal Data processing and the purpose of the agreement;

(iii) Subject's rights and the Controller's obligations;

(iv) type and characteristics of the needs or services to be provided to the Subject;

(v) consequences in the event that the Personal Data processing is not carried out by the Controller;

(vi) impact of the Personal Data processing on the protection of the Subject's rights;

(vii) Controller's representations to (A) carry out the Personal Data processing in accordance with the laws and regulations and (B) fulfil the Subject's rights; and

(viii) parties involved in the processing of Personal Data.

From an implementation perspective, these requirements may create challenges, particularly considering on the nature of the business and the industry in which it operates. A detailed provisions in the underlying agreement may hinder flexibility for businesses in anticipating future development or combining their products or services offering.

(c) **Satisfaction of other valid interests**. This basis can be relied upon by a Controller for Personal Data processing if it has conducted (i) an analysis of the necessity, purpose, and balance between the relevant Subject's rights and the Controller's interests demonstrating a valid interest of the Controller in the processing, and (ii) an assessment of the legal or adverse effects of the processing, as well as implemented measures to mitigate any such effects. Examples of what constitutes valid interests under the elucidation of GR 33/2026 include security supervision, health, safety, and crime prevention. In addition, both the analysis and assessment results must be documented by the Controller.

Personal Data Policies and Records

While the PDP Law does not require specific internal policies or records that must be maintained by businesses to demonstrate compliance with Personal Data Protection requirements, GR 33/2026 now expressly requires Controllers and/or Personal Data Processors (the **Processor**) to establish and maintain several internal policies, records, and procedures in relation to Personal Data processing, including:

(a) policy in relation to Personal Data processing;

(b) policy, procedure, and/or guidelines for the prevention and handling of Personal Data Protection failures;

(c) mechanism and policy for the handling of an indemnity request;

(d) policy on the Personal Data Retention Period;

(e) policy on the performance of duties for the public interest or public services, or the exercise of authorities as one of the bases for the Personal Data processing;

(f) records of all Personal Data processing activities (**ROPA**); and

(g) minutes of deletion and/or destruction of Personal Data.

The policy referred to in point (a) above must be prepared in accordance with the preparation guidelines which will be stipulated by the DPA that have not yet been established. In addition, ROPA as referred to in point (f) must be maintained and made available to the DPA for audit and supervision purposes.

In addition, some of the foregoing policies must contain certain minimum requirements stipulated under GR 33/2026.

Prohibition of Exoneration Clauses

GR 33/2026 imposes a new prohibition on including exoneration clauses in a notification on Personal Data Protection. Such clauses refer to provisions that reduce, limit, and/or release a Controller from its obligations and responsibilities.

Businesses should therefore review their existing privacy notices and ensure that they do not contain any provisions that could be construed as exoneration clauses under GR 33/2026.

Notification for Indirect Procurement of Personal Data from a Subject

GR 33/2026 imposes a new obligation for Controllers that indirectly procure Personal Data from a Subject (i.e., an individual not a legal entity) to notify the relevant Subject owner of the Personal Data of, among others, (i) the legality, purpose, and period of the Personal Data processing, and (ii) the type and relevance, retention period, and details of the Personal Data, no later than 30 business days after the collection or procurement of the Personal Data.

Consideration will need to be taken since this requirement may present practical challenges, for example, (i) where there is an expected adverse implication of such notification due to the nature of the relevant businesses, (ii) where the Controller has limited information to make such notification, and (iii) on how a Controller could determine conclusively the start of the 30 business days notification deadline.

Data Protection Impact Assessment

While the PDP Law requires a data protection impact assessment (the **DPIA**) for Personal Data processing that poses a potential high risk to Subjects, GR 33/2026 provides further clarity by requiring a DPIA to be conducted before such Personal Data processing takes place. GR 33/2026 further specifies the contents of a DPIA, which were not addressed under the PDP Law. The DPIA must cover, at least:

(a) a description on the Personal Data processing activities and their purposes;

(b) an assessment of the necessity and proportionality of the purposes and activities of Personal Data processing;

(c) an assessment of the risks to the rights of the Subjects; and

(d) steps to be taken by the Controller to protect the Subject from risks arising from the Personal Data processing.

The DPIA must take into account and document the advice provided by the Controller's data protection officer (**DPO**) (if any).

Considering the above, from a practical perspective, businesses may need to consider establishing the DPIA process, and, if applicable, the involvement of the DPO, before the relevant Personal Data processing is implemented.

In addition, the PDP Law and GR 33/2026 identify the same categories of Personal Data processing activities as potentially high-risk categories. For large-scale processing, an activity considered potentially high risk, the elucidation of GR 33/2026 requires the Controller to assess whether the processing is carried out on a large scale based on certain stipulated aspects, such as the amount and period of Personal Data processed. The elucidation of GR 33/2026 also recognizes artificial intelligence, machine learning, smart technology, and the Internet of Things as new technologies used in Personal Data processing posing potential high risk.

3x24-Hour Period for Data Breach Notification and Cessation of Personal Data Processing

While the PDP Law imposes a 3x24-hour period for notifying the relevant Subject(s) and the DPA on an occurrence of Personal Data Protection Failure, GR 33/2026 clarifies that the period starts from the time when a Personal Data Protection Failure is known with certainty, reasonably, and properly (*secara pasti, patut, dan wajar*) based on the conclusion drawn from the documentation prepared by the relevant Controller on the incident. From a practical perspective, this clarification provides Controllers with an opportunity to assess and document the incident before determining whether a Personal Data Protection Failure has occurred, following which the 3x24-hour notification period begins. At the same time, GR 33/2026 does not provide objective threshold for determining when a Personal Data Protection Failure is considered to have occurred.

In addition, as required under the PDP Law, GR 33/2026 consistently provides a 3x24-hour period for ceasing Personal Data processing where a Subject withdraws their consent. The period starts upon receipt of the consent withdrawal request by the Controller. GR 33/2026 requires the Controller to complete the verification of the withdrawal request before ceasing the relevant Personal Data processing. This can be interpreted to mean that the verification must also be completed within the 3x24-hour period.

Consequently, there may be operation, technical, and regulatory compliance challenges in complying with these requirements in the event of a consent withdrawal and/or Personal Data Protection Failure. For instance, the applicable period contemplated above could differ from the period stipulated under sectoral regulations, such as those issued by the Indonesian Financial Services Authority, and any period contractually binding on the relevant Controller.

Cross-Border Personal Data Transfers

In carrying out the cross-border transfer of Personal Data, GR 33/2026 imposes new obligations on Controllers and Processors to, among others, (i) record and map the Personal Data transfer cycle and its implications, (ii) identify and assess the effectiveness of, the legal instrument used as a reference for the Personal Data transfer, and (iii) conduct periodic reviews at appropriate intervals. In addition, the Controller is required to inform the Subject regarding the Personal Data transfer prior to such transfer.

The assessment of the legal instrument, as set out above, must consider certain matters specified under GR 33/2026, including (i) the underlying regulation, (ii) the parties involved in the transfer, (iii) the purpose, scope, mechanism, risk, impact, procedural steps, and evaluation of the transfer, (iv) the category, format, storage and access of the Personal Data to be transferred, and (v) the adequacy, relevance, and limitation of the transferred Personal Data in accordance with the purpose of the Personal Data transfer. From a practical perspective, when undertaking a potential cross-border transfer of Personal Data, businesses could face difficulties in identifying and determining the appropriate legal instrument, particularly depending on the nature and circumstances of the relevant business and the data transfer.

Moreover, GR 33/2026 provides additional requirements for relying on the bases for cross-border transfer of Personal Data, some of which are highlighted below:

(a) **Personal Data Protection level**. Both the PDP Law and GR 33/2026 require a Controller to ensure that the recipient country provides a level of Personal Data Protection equal to or higher than those in Indonesia when transferring Personal Data outside Indonesia. In assessing the level of Personal Data Protection, GR 33/2026

requires the DPA to issue a list of countries with Personal Data Protection level equal to or higher than those in Indonesia. As of the date of this newsletter, this list remains absent as the DPA has not yet been established.

(b) **Adequate and binding Personal Data Protection**. If the condition in point (a) is not fulfilled, the cross-border transfer of Personal Data may nevertheless be carried out, provided that the Controller ensures the existence of adequate and binding Personal Data Protection measures. They may be in the form of (i) legally binding and enforceable instrument, (ii) standard Personal Data Protection contractual clauses stipulated by the DPA, (iii) binding corporate rule for a group of corporates approved by the DPA, and/or (iv) other instruments recognized by the DPA.

(c) **A consent**. If the conditions in points (a) and (b) above are not fulfilled, the Controller may rely on a Subject's consent for the cross-border transfer of their Personal Data. This alternative is only allowed if certain conditions are fulfilled, namely (i) the transfer is not recurring, concerns a limited number of Subjects, and is necessary for a purpose that does not override the interests or rights and freedoms of the Subjects, and (ii) the Controller has conducted a risk assessment, implemented appropriate safeguards, and has informed the DPA and the Subjects of the Personal Data transfer and the legitimate interest concerned.

Joint Controllers Framework

Joint Controllers will be considered by law to bear joint and several liability in the Personal Data processing. On the other hand, the PDP Law requires Joint Controllers to have an agreement covering their responsibilities, roles, and relationship, GR 33/2026 further specifies the specific minimum content required under the agreement, including (i) the allocation of obligations and responsibilities between the existing Controller, the new Controller, and other party(ies) involved in the Personal Data processing, as well as (ii) the respective bases of the Personal Data processing by each Controller.

Affiliated companies and multinational group that have joint control agreements may need to re-assess their potential liabilities due to compliance risk and sanctions.

Personal Data Transfers in Merger and Acquisition and Other Corporate Actions

GR 33/2026 expressly recognizes companies involved in a merger, spin-off, acquisition, consolidation, or dissolution as Joint Controllers of the transferred Personal Data while such corporate action is being undertaken until its completion. From a practical perspective, the identification of the relevant Controllers in case of each corporate action should be assessed on a case-by-case basis as GR 33/2026 does not further specify or distinguish which party should be considered the new Controller or existing Controller in the context of each type of corporate action.

Joint Controllers involved in a corporate action are subject to certain requirements, including their obligations (i) to enter into an underlying agreement, that, among others, allocates the obligations and responsibilities between them and other party(ies) involved, and (ii) to notify the Subjects of any transfer of Personal Data resulting from the corporate action, both before and after the corporate action.

GR 33/2026 sets out the required content of the notification, distinguishing between notifications to be provided before and after the corporate action. The notification must cover, among others, (i) mechanism, procedure, and timeline for submitting objections to, or requesting to cease, Personal Data processing, as well as for objecting to the transfer of Personal Data and (ii) timeline for the commencement of Personal Data processing in relation to the

activities of the new Controller commences. Notably, GR 33/2026 does not provide specific timeline within which these notifications must be provided. Given the specific notification requirements under GR 33/2026, it indicates that the notification requirement is intended to apply separately to each corporate action involving a transfer of Personal Data.

Irreversible Destruction of Personal Data

GR 33/2026 requires the destruction of Personal Data to be carried out by removing, eliminating, or destroying the Personal Data, whether electronically or non-electronically, such that it can no longer be used to identify the relevant Subject. It suggests that the destruction process should render the Personal Data incapable of being recovered or reconstructed in a manner that would allow the relevant Subject to be identified. In addition, GR 33/2026 confirms that the destruction of Personal Data based on the relevant Subject's request may still be carried out even if the Retention Period has not yet expired.

Implementation of this requirement may need to take into account potential third-party liabilities and compliance to other prevailing regulations.

Mediation Framework

While the PDP Law generally addresses dispute resolution, GR 33/2026 introduces a dedicated mediation framework. Under GR 33/2026, in the event of a Dispute between a Subject, Controller, and/or Processor, a report of the Dispute may be submitted to the DPA. If neither criminal nor administrative violations are identified during the DPA's verification, the DPA will facilitate dispute resolution between the parties, with mediation as the prioritized mechanism. GR 33/2026 further sets out the detailed process and timeline for mediation. Notably, the mediation process is private and confidential and concludes when the Disputing Parties and the Mediator execute a Settlement Agreement. The Settlement Agreement may subsequently be submitted by the Disputing Parties to the competent court to obtain a deed of settlement (*akta perdamaian*), in accordance with applicable laws and regulations.

Administrative Sanctions: Fine-calculation Variables and Objection Mechanism

GR 33/2026 expressly authorizes the DPA to impose administrative sanctions for violations of Personal Data Protection laws and regulations.

In relation to the administrative fines, the PDP Law does not specify the basis for determining the amount of such fines. GR 33/2026 fills this gap and identifies ten violation variables for determining the severity of administrative fines, namely:

(a) the negative impact resulting from the violation;

(b) the duration of the violation;

(c) the type of Personal Data affected;

(d) the number of affected Subjects;

(e) the discovery process of the violation;

(f) the level of transparency and cooperation during the investigation;

(g) the business scale of the Controller and/or Processor;

(h) the ability of the Controller and/or Processor to pay;

(i) the compliance of the Controller and/or Processor; and/or

(j) other relevant variables stipulated by the DPA.

GR 33/2026 remains silent on the specific calculation methodology for translating these variables into the amount of an administrative fine. We expect that, subject to any further implementing regulations, the actual calculation of the fine will ultimately depend on the DPA's assessment of the relevant variables as DPA is the authority authorized in imposing the sanctions under GR 33/2026.

For context, both the PDP Law and GR 33/2026 specify that one of the administrative sanctions thereunder is an administrative fine of up to 2% of the annual revenue or annual income of the violating Controller and/or Processor, calculated based on the relevant variables of the violation. Given the DPA's authority in imposing administrative sanctions, further clarity on the DPA's establishment and its subsequent approach to the assessment and calculation of fines will be important to understanding how this provision will be applied in practice.

In addition, an administrative fine may also be reduced to zero in certain circumstances, although these circumstances are not detailed.

On the other hand, GR 33/2026 also establishes an objection mechanism where a party subject to an administrative sanction may submit a written objection to the DPA.

Transitional Provision

GR 33/2026 will enter into force on 16 January 2027, six months after its enactment on 16 July 2026.

CONCLUSION

The matters set out above are intended to highlight key areas that businesses should consider in anticipating the implementation of GR 33/2026, rather than to serve as an exhaustive summary of GR 33/2026. With the transition period under GR 33/2026 now having less than 5 months remaining, businesses should begin assessing the applicability of GR 33/2026 to their Personal Data processing activities and prepare for the operational and technical implementation that may be required to achieve compliance.

Even though the absence of the DPA remains the deciding factor on how GR 33/2026 will be interpreted and enforced, businesses will need to be prudent in this current environment.