Client Alert: Newfound Guidelines and Clarity on Indonesian Data Protection through GR 33/2026

I. Introduction

The Government of Indonesia has issued Government Regulation No. 33 of 2026 on the Implementing Regulation of Law No. 27 of 2022 on Personal Data Protection ("**GR 33/2026**"), which was enacted and promulgated on 16 July 2026. The long awaited GR 33/2026 provides further implementing provisions on certain matters stipulated in Law No. 27 of 2022 on Personal Data Protection (the "**PDP Law**"), which comprises of 225 articles in 12 chapters, together with an elucidation.

Concurrently, it also regulates matters beyond those expressly delegated by the PDP Law, such as the procedure for data subject requests, security and accountability duties, exemptions, supervision and dispute resolution.

The PDP Law provides that its implementing regulation will, *inter alia*, set out further provisions on the following matters:

a. Data subject's submission of objections to automatic processing
b. Violations of personal data processing and the procedure for imposing compensation payable to data subjects
c. Right of data subjects to use and transmit personal data
d. Implementation of personal data processing
e. Impact assessment of personal data protection
f. Notification procedures pertaining to corporate action by the data controller
g. Data protection officers
h. Cross-border data transfers
i. Implementation of administrative sanctions

This Client Alert summarises these provisions together with other key requirements of GR 33/2026

For added context, it should be noted that as of the date of this Client Alert, the Government of Indonesia has not yet established the personal data protection agency to supervise compliance and impose sanctions under the PDP Law and GR 33/2026 (referred to in GR 33/2026 as the "*Lembaga*" and in this Client Alert as the "**PDP Agency**"). Pending its establishment, a number of the operational mechanisms in GR 33/2026 cannot yet be used in practice (see "Other Noteworthy Matters" below).

II. Key Points

A. Scope of Application and Key Definitions

GR 33/2026 applies to any person (individual or corporation), public body and international organisation that carries out legal acts relating to personal data protection (i) within Indonesian jurisdiction, or (ii) outside Indonesian jurisdiction where those acts have legal consequences in Indonesia and/or for Indonesian citizens who are data subjects outside Indonesia (Article 2). Purely personal or household processing by individuals is excluded (Article 3). Offshore businesses that process the data of Indonesian citizens should therefore not assume that they fall outside GR 33/2026, although it does not explain how it will be enforced against entities without a local presence or whether a local representative is required.

Several definitions and classifications are of practical importance:

1. **"Days"** (*Hari*) means **working days** (Article 1(19)). Periods expressed in "days" (for example 30 days for notices on indirectly collected data and 14 days for objections to sanctions) are therefore working-day periods, whereas periods expressed in hours (such as 3 × 24 hours) are not.
2. **"Child"** means a person below 18 years of age who is not married (Article 1(21)).
3. **Specific personal data** comprises health data and information, biometric data, genetic data, criminal records, children's data, personal financial data and other data designated by the relevant ministry or agency in coordination with the PDP Agency (Article 6). While **General personal data** comprises full name, gender, nationality, religion, marital status and data that, when combined, identify a person (Article 7). Notably, religion is classified as general data, whereas the GDPR treats it as a special category.
4. **Identifiability.** Data that identify a person when combined with other information, whether through direct reference, mapping reference, triangulation or other combinations, are personal data, including where public domain data are used (Article 7(2)–(3)). Data collected from public sources (for example by scraping) may therefore remain within scope.
5. **Data protection failure** is defined broadly as any failure to protect personal data in terms of confidentiality, integrity and availability, whether intentional or accidental, including security breaches (Article 1(18)).

B. Data Subject Rights: Request Procedure and Response Timelines

GR 33/2026 introduces a uniform procedure for exercising data subject rights, which the PDP Law did not previously set out (Articles 20–27):

1. Requests must be recorded and submitted electronically or non-electronically through an accessible channel that the controller must provide. Controllers that process data electronically must accept electronic requests, and must respond through the same channel used by the data subject or another easily accessible channel.
2. A request may be made by the data subject, a parent or guardian of a child, the guardian of a person with a disability, or an authorised proxy (the elucidation confirms that a collective proxy for several data subjects is permitted).
3. A request must state the requester's identity (with proof of identity), the right and interest invoked and a description of the request. The controller must verify the request using a proportionate mechanism, and, according to the elucidation, verification must not take longer than necessary.
4. If the controller fails to act on a request, the data subject may report the controller to the PDP Agency.

The response deadlines are very short and are expressed in hours rather than working days:

Right / obligation	Deadline	Article
Access to personal data (including processing trail)	Within 3 × 24 hours of receipt of the request	77(1)
Copy of personal data	Confirm and state the time required within 3 × 24 hours of receipt and verification; deliver at the first opportunity	78
Rectification or update	Within 3 × 24 hours of receipt of the request	71(1)

Right / obligation	Deadline	Article
Delay or restriction of processing	Within 3 × 24 hours of receipt; any rejection (with reasons) within 3 × 24 hours of receipt and verification; notify the data subject within 3 × 24 hours after implementation	99, 100, 103
Stopping processing after withdrawal of consent	Within 3 × 24 hours of receipt of the request	92
Notice of erasure or destruction	Within 3 × 24 hours before or after the erasure or destruction (depending on the ground)	87(5)
Notice for data obtained indirectly	Within 30 working days of collection	64
Data protection failure	Within 3 × 24 hours (see below)	114

C. Data Subject's Submission of Objections to Automatic Processing

GR 33/2026 reiterates what has already been stipulated under the PDP Law, that data subjects have the right to object to decision-making that is based solely on automated processing (including profiling) where such processing produces legal effects or significantly affects the data subject. Furthermore, GR 33/2026's elucidation provides examples: decisions with legal effects include visa refusals, withdrawal of social benefits and contract terminations, while decisions with a significant effect include credit or job application refusals, differential pricing based on personal data and advertising that strongly affects vulnerable groups (Article 93). Such decisions are also a trigger for a mandatory data protection impact assessment (see "Impact Assessment of Personal Data Protection" below).

Furthermore, the data controller must maintain a mechanism to respond to such objections and proactively provide adequate information to the data subject regarding the technology used and the consequences of automated decision-making. Upon receipt of a verified objection, the data controller is obligated to provide an alternative method of processing that involves human intervention and/or is not based solely on automated results.

Notwithstanding the above, the data controller may reject an objection only where both of the following circumstances exist:

1. There are no legal consequences or significant impacts on the data subject; and
2. The controller possesses a highly accurate system with mitigation measures to avoid adverse impacts.

It should be noted that the rejection of an objection does not negate the data subject's separate right to withdraw consent, and the data controller must notify the data subject of any rejection. In practice, the scope for rejection appears narrow: the first condition is in substance a threshold question (a decision without legal or significant effect falls outside the right in the first place), and the second (a "highly accurate system") is undefined and would need to be evidenced, for example by testing and error-rate data. Unlike Article 22 of the GDPR, GR 33/2026 does not prohibit solely automated decisions; it grants a right to object, so such decisions may proceed until an objection is made. Further provisions will be set out in a PDP Agency regulation (Article 96).

D. Violations of Personal Data Processing and Procedures for the Imposition of Compensation to Data Subjects

GR 33/2026 establishes a structured compensation claim mechanism for data subjects, under which claims are submitted directly to the data controller. The compensation claim must contain at minimum:

1. The identity of the data subject;
2. Data, information, and/or documents serving as evidence; and
3. The legal relationship between the data subject and the data controller regarding the processing in question.

The data controller is required to maintain mechanisms and policies for handling such claims, and is required to assess and respond to each claim. GR 33/2026 does not prescribe a deadline for the controller's response.

If the data controller rejects the claim or no agreement on compensation is reached, the data subject may file a lawsuit in accordance with applicable laws and regulations.

Claims against state public bodies must be submitted in accordance with state administrative law (Article 109).

It should be noted that further provisions on handling and settlement of compensation will be stipulated through a regulation issued by the PDP Agency (Article 110). Separately, a dispute may be reported to the PDP Agency, which gives priority to mediation (see "Dispute Resolution and Mediation" below).

E. Right of Data Subjects to Use and Transmit Personal Data

GR 33/2026 elaborates the data portability right under the PDP Law in two dimensions (Articles 111–113).

First, the data subject has the right to obtain and/or use their personal data from the controller in a commonly used or machine-readable format (portability).

Second, the data subject has the right to transmit their personal data to another data controller (interoperability), provided the systems used are capable of secure interoperability in accordance with personal data protection principles.

Both rights are subject to two cumulative conditions:

1. The processing must be based on either explicit consent or the performance of a contract with the data subject (including steps requested by the data subject before entering into a contract); and
2. The processing must be carried out automatically.

In exercising these rights, the data controller must take into account:

1. The controller's capacity to fulfil the rights, as communicated to the data subject; and
2. Applicable competition law prohibitions on monopolistic practices and unfair business competition.

Further provisions on the mechanism for exercising portability and interoperability rights will be stipulated through a PDP Agency regulation. The conditions mirror Article 20 of the GDPR (consent or contract as the basis, and automated processing); the

express reference to competition law and to the controller's own capacity are features specific to GR 33/2026.

F. Implementation of Personal Data Processing

It should be noted that the PDP Law's provisions does not set out the requirements for joint data controllers. In contrast, under GR 33/2026, processing by joint data controllers are acknowledged and must satisfy the following minimum requirements (Article 11):

1. There is an agreement between the data controllers that sets out their roles, responsibilities and relationship (and, at a minimum, each controller's processing basis, the link between their purposes, the agreed processing methods, the types of data processed, the allocation of legal responsibilities and the joint contact person);
2. The purposes of processing are interrelated and the methods of processing are determined jointly; and
3. There is a jointly appointed contact person.

Joint data controllers are jointly and severally liable for the processing (Article 12). A data subject or the PDP Agency may therefore in principle pursue any joint controller for the whole of the processing, irrespective of the internal allocation of responsibilities in their agreement. In addition, in a merger, demerger, acquisition or consolidation, the old and new controllers are treated as joint controllers until the transaction is regarded as completed (see "Notification Procedures Pertaining to Corporate Action" below).

GR 33/2026 also provides further elaboration on the six lawful bases for processing, which was first introduced under the PDP Law. A controller must have a lawful basis before processing begins, must choose it in line with the purpose and necessity of the processing, and must ensure that the processing is not discriminatory (Articles 30–31):

1. Valid explicit consent — must be obtained freely, knowingly, specifically, and unambiguously, with information provided to the data subject before consent is sought. In addition, the controller must be able to demonstrate that consent was given, must offer an easy withdrawal mechanism, must not obtain consent by deceptive or misleading means, and must not reduce the quality of goods or services if consent is refused (unless the service requires the processing). Where consent covers marketing, the third-party recipients, the form of offers and the withdrawal and complaint mechanism must be disclosed. The elucidation indicates that consent bundled with acceptance of terms and conditions is "ambiguous" and therefore not valid (Articles 32–37);
2. Contractual necessity — a valid contract with the data subject (or steps requested by the data subject before contracting) must exist and the processing must be necessary to perform it. The contract must contain prescribed minimum content (including detailed purposes, their link to the purpose of the contract, the data subject's rights, the consequences of not processing, the impact on data subject rights, the parties involved and the controller's guarantees of compliance and of fulfilling data subject rights); otherwise this basis cannot be used. The controller may not process beyond what the contract specifies, may not use clauses that shift responsibility to the data subject, and cannot treat the contract as a substitute for consent (Articles 40–44);
3. Legal obligations — processing necessary for the controller to comply with a legal obligation, which includes (and is not limited to) court orders and decisions and decisions of state administrative officials issued under the law (Article 45);
4. Vital interests — applicable only where there is a threat to the life, physical well-being or property of the data subject or another person and it is difficult to obtain the data subject's consent (for example, where the data subject is unconscious

or the guardian of a child is absent). The data subject must be informed of the processing, including the nature of the threat (Articles 46–47);
5. Performance of duties in the public interest, public services, or exercise of authority — is available only where a law requires the controller to take the relevant action, and requires an adequate policy document setting out the scope and purpose of the processing. Data subjects must be informed when processing begins, subject to limited exceptions (Articles 49–52); and
6. Legitimate interests — subject to balancing assessment between the controller's interests and the rights of the data subject (*i.e.* legitimate interest assessment) and a further assessment that the processing has no legal effect on, and does not harm, the data subject, with mitigation measures in place. Both assessments must be documented, data subjects may request an explanation of the controller's reliance on this basis, and public bodies may rely on it only for purposes other than their public duties (Articles 53–57). This is stricter than the balancing test under Article 6(1)(f) of the GDPR.

GR 33/2026 also elaborates on several other processing principles:

1. **Transparency and notices.** Controllers must provide an easily accessible privacy notice, available throughout the processing period and delivered before processing starts, covering at least the controller's identity and the contact details of its data protection officer ("**DPO**"), the legal basis, purposes, types and relevance of data, retention period, details of the data collected (including sources, recipients and security measures), duration of processing and data subject rights. Changes must be notified before they take effect. Where data is obtained indirectly, the information must be provided within 30 working days of collection. Privacy notices may not contain exoneration clauses (Articles 62–65).
2. **Purpose limitation and data minimisation.** Processing must be limited to the purposes explicitly communicated to the data subject, documented in internal policies and the privacy notice; processing must be limited to data that is relevant, adequate and not excessive; and a new or different purpose requires fresh compliance with GR 33/2026 (Articles 58–59 and 67–68).
3. **Accuracy.** Controllers must verify the accuracy, completeness and consistency of personal data using documented data-quality standards, periodically and as needed, and must keep a record of the results (Article 69).
4. **Retention.** Controllers must adopt a documented retention policy covering, among other things, retention periods, the data subjects and data types covered, de-identification rules for statistics and research, destruction methods, rules for processors, responsible persons and, where retention is legally required, the legal basis (Article 75).

GR 33/2026 also sets out the minimum content of a Record of Processing Activities ("**ROPA**"), a requirement stipulated but not further elaborated under the PDP Law. Unlike the GDPR, there is no exemption for small organisations: all controllers must keep a ROPA covering all processing activities (Article 74).

GR 33/2026 stipulates that a data controller's ROPA shall at least contain:

1. Name and contact details of the data controller, joint data controller, and/or data processor;
2. DPO contact;
3. Source of collection and destination of personal data;
4. Basis for the processing of personal data;
5. Purposes of the processing of personal data;
6. Types of personal data;
7. Categories of data subjects;
8. Parties other than the data controller who can access personal data;

9. Fulfilment of the rights of data subjects;
10. Mapping the flow of personal data;
11. Retention period;
12. Technical and organisational measures to secure personal data; and
13. Details of personal data transfers.

Processors must keep their own record (containing at least the processor's name and contact details, the scope of processing, transfer details and a general description of security measures), and controllers must ensure that they do so. ROPAs must be kept up to date and provided to the PDP Agency on request and for audit and supervision purposes (Article 74(3)–(10)).

G. Data Protection Failures (Data Breach Notification)

In the event of a personal data protection failure (*e.g.* data breaches), the data controller must notify both the data subject and the PDP Agency in writing within 3 × 24 (seventy-two) hours (Article 114). While previously the period is unclear under the PDP Law, GR 33/2026 provides further clarification that the period runs from when the failure becomes known in a certain, proper and reasonable manner. According to the elucidation, the controller is deemed to have such knowledge based on the conclusions of its own documentation of the incident, so the timing and quality of internal incident documentation will be critical.

The notification must contain at least the personal data disclosed, when and how it was disclosed, the handling and recovery measures taken by the controller, and the contact details of the DPO or designated contact person (Article 114(3)–(4)). In addition, the controller must notify the public through electronic and/or non-electronic media where the failure disrupts public services and/or has a serious impact on the public interest (Article 115).

The data controller must also prepare documentation of the failure to be submitted to the PDP Agency. The documentation (Article 116) must, at a minimum, contain the following details:

1. The personal data affected;
2. A description of the failure;
3. The impact or consequences of the failure on the data subject and the data controller;
4. Handling and recovery efforts that have been, are being, and will be undertaken; and
5. The timeframe for notification to the data subject and the PDP Agency.

Controllers must also adopt and implement an internal policy or procedure for preventing and handling data protection failures, covering roles and responsibilities, analysis, classification, prioritisation, monitoring and resolution, documentation and reporting to data subjects and the PDP Agency, and periodic review (Article 117). Unlike the GDPR (Article 33) and the PDPA, GR 33/2026 contains no risk or harm threshold: on its wording, any failure affecting confidentiality, integrity or availability triggers notification to both data subjects and the PDP Agency. A rapid triage process, and a contractual obligation on processors to report within hours, are therefore advisable.

H. Impact Assessment of Personal Data Protection

A Data Protection Impact Assessment ("**DPIA**") is mandatory, and must be completed before processing begins, where the processing has a potentially high risk to data subjects (Articles 120–121). GR 33/2026 treats the following as high risk:

1. automated decision-making with legal or significant effects;
2. processing of specific personal data;
3. large-scale processing (assessed by reference to the volume of data, number of data subjects, duration, types of data, purposes and geographic area);
4. systematic evaluation, scoring or monitoring of data subjects;
5. matching or combining of datasets;
6. use of new technologies (the elucidation cites artificial intelligence, machine learning, smart technology and the Internet of Things); and
7. processing that restricts the exercise of data subject rights.

A DPIA must contain, at a minimum:

8. A description of processing activities and purposes;
9. A necessity and proportionality assessment;
10. An assessment of the risks to data subjects' rights; and
11. Protective measures implemented by the data controller to protect data subjects.

The data controller must implement the aforementioned protective measures at the time processing commences. The data controller must also document the DPIA and measures taken, and review it whenever the risk of the processing changes. A controller may (but is not required to) consult the PDP Agency where the processing causes material or immaterial harm to data subjects or where no technical or operational measures are available (Article 122). This is voluntary, unlike the prior consultation required under Article 36 of the GDPR for unmitigated high risk.

Where a DPO has been appointed, the controller must take into account and document the DPO's recommendations in conducting the DPIA. The DPIA is also the vehicle for other required assessments, such as the age-appropriateness of services offered to children (elucidation to Article 38) and the update required in connection with corporate actions (Article 131(4)).

I. Notification Procedures Pertaining to Corporate Action by the Data Controller

GR 33/2026 establishes notification obligations triggered by corporate actions (specifically merger, demerger, acquisition, consolidation, or dissolution of a legal entity) that involve the transfer of personal data (Articles 131–137).

Both the original data controller and the new data controller must notify the data subjects.

The original data controller's notification must contain, *inter alia*:

1. The facts of the corporate action;
2. The categories and purposes of personal data to be transferred;
3. The identity and contact details of the new data controller;
4. The data subject's rights and the mechanism to exercise them; and
5. A statement that the original controller will destroy transferred personal data upon conclusion of the corporate action.

Subsequently, the new data controller's notification must contain, *inter alia*:

1. Confirmation that the transfer has occurred;
2. Processing activities to be carried out;
3. The new data controller's identity and contact details;
4. Confirmation of purpose consistency;
5. Timing of new processing commencement; and

6. The mechanism for the data subjects to object or request cessation of processing.

Notifications must be made both before and after the corporate action takes effect. For this purpose, a corporate action takes effect once all legal requirements have been met; for an Indonesian limited liability company, the elucidation states that this is the date of the Ministry of Law's approval or notification letter on the amendment of the articles of association (Article 133(5)).

The following further requirements apply:

1. Before the transfer, the controller must assess the data subject rights and the data protection obligations that remain to be fulfilled during and after the transaction, update its DPIA accordingly and prepare technical and operational measures for the transfer (Article 131(3)–(5)).
2. The old and new controllers are treated as joint controllers until the transaction is regarded as completed (Article 131(6)), with the consequences of joint and several liability described above.
3. The new controller may process the data for its own purposes only after the period for data subjects to object to the new controller's storage and processing has ended (Article 135).
4. Data subjects may exercise their rights against the old controller from the time of its pre-transaction notice until the transaction takes effect, and against the new controller after its post-transaction notice (Article 137).
5. The old controller must prepare terms and conditions for access to the data by other parties involved in the transaction (Article 133(6)).

In cases of merger, demerger, acquisition, or consolidation, the original and new controllers must enter into a data protection agreement covering at least:

1. The legal basis for processing by each controller;
2. Compliance with data protection principles;
3. Fulfilment of data subject rights; and
4. Allocation of obligations and responsibilities.

This agreement may form part of the underlying transaction agreement. It must still comply with the joint controller requirements (Article 134(4)).

On a separate note, upon dissolution of a legal entity, the data controller must additionally notify data subjects of:

1. The fact of dissolution and resulting erasure/destruction of personal data;
2. Other parties collaborating in processing; and
3. A contact person or DPO available for a reasonable period post-dissolution. The dissolved entity may appoint another party to act as contact person (Article 136).

J. Data Protection Officers

Controllers and processors must appoint a DPO (referred to in GR 33/2026 as the "PPDP") only in the following circumstances (Article 142):

1. the processing is carried out for public service purposes;
2. the controller's core activities require regular and systematic monitoring of personal data on a large scale; and/or
3. the controller's core activities consist of large-scale processing of specific personal data and/or personal data relating to criminal offences.

"Large scale" is not yet defined for this purpose; the details of the appointment obligation are to be set out in a PDP Agency regulation. The DPO must be appointed based on professionalism, knowledge of law and personal data protection practices, and the ability to fulfil their duties (Article 143). The DPO's minimum tasks are to advise the controller or processor on compliance, monitor compliance with the law and internal policies, advise on the DPIA and monitor performance, and act as the coordination and contact point on processing issues (Article 145).

Further provisions on professionalism and competence of DPOs will be stipulated through the PDP Agency's regulations.

GR 33/2026 also stipulates that the DPO may be an individual or a team, drawn from within or outside the controller/processor organisation – and the appointment must be proportionate to the organisation's structure, size, and needs.

Furthermore, data controllers and/or processors must ensure the DPO:

4. Is involved in all personal data processing activities;
5. Has reporting access to the highest level of management;
6. Operates objectively, without interference, and independently;
7. Has adequate resources and expertise; and
8. Has appropriate access to processing activities and related information.

The data controller and/or processor must also ensure the DPO's duties do not create a conflict of interest. Unlike the PDPA, which requires every organisation to designate at least one responsible individual, the Indonesian obligation applies only in the situations listed above (as under Article 37 of the GDPR). Organisations outside those situations should nonetheless designate a responsible person or contact point, since the data subject request, breach, ROPA and DPIA provisions all assume that one exists.

K. Cross-Border Data Transfers

GR 33/2026 clarifies what constitutes a cross-border data transfer (Articles 160–174). A transfer is cross-border if the following criteria are met:

1. Carried out by the data controller in accordance with laws and regulations;
2. The data controller makes personal data available to the data controller and/or processor receiving the data; and
3. The data controller and/or processor receiving the data is located outside Indonesian jurisdiction.

As under the PDP Law, both the transferring controller and the receiving controller and/or processor must protect the transferred personal data in accordance with Indonesian data protection laws. GR 33/2026 adds that, in the case of onward transfers (*i.e.* transfers subsequent to the initial cross-border transfer), the controller and/or processor involved must remain subject to Indonesian law (Article 160(3)). GR 33/2026 does not explain how this will be enforced against onward recipients, so the obligation should be reflected in contractual flow-down terms.

Before making a cross-border transfer, a data controller must assess the legal instrument it intends to use (Articles 161–163). The assessment must consider the following aspects:

1. The regulatory basis used;
2. Purposes of transfer and processing of personal data;
3. Parties involved in the processing of personal data;

4. The sector covered by the transfer;
5. Categories of data transferred;
6. Choice of data transfer mechanism used;
7. The storage location of the personal data and access to the personal data;
8. The format of the personal data to be transferred (*i.e.* in plain text/obfuscated/encrypted);
9. The possibility that the personal data can be transferred further from the recipient country to another country;
10. An assessment of the risks or impact on data subjects' rights arising from the transfer;
11. Whether the personal data transferred is adequate, relevant and limited to what is necessary for the purpose of the transfer; and
12. Procedural steps and evaluation of the implementation of personal data transfer.

Beyond this assessment, controllers must record and map the transfer lifecycle, assess the effectiveness of the chosen legal instrument before transferring (according to the elucidation, including the possibility that public authorities in the destination country may access the data, with or without the recipient's knowledge), use supplementary contractual, technical and/or organisational measures where needed, and periodically re-evaluate the transfer (Article 161). This resembles the "transfer impact assessment" and supplementary measures approach that developed under the GDPR following the *Schrems II* decision. Data subjects must also be informed, before the transfer, of its purpose, the existence of protective instruments, the mechanisms enabling them to exercise their rights, and the risks of the transfer and how they are mitigated (Article 164).

Furthermore, GR 33/2026 reiterates the tiered, risk-based framework for cross-border data transfers as stipulated under the PDP Law – with additional requirements. The tiers operate as a strict hierarchy: a lower tier may be used only if the higher tier is not satisfied (Article 165).

L. Implementation of Administrative Sanctions

GR 33/2026 establishes a comprehensive administrative sanctions regime applicable to violations of a broad range of provisions, including those on lawful bases, data subject rights, records of processing, impact assessments, security, breach notification, DPO appointment and cross-border transfers (Article 184).

Administrative sanctions may take the form of:

1. Written reprimand;
2. Temporary suspension of personal data processing activities;
3. Deletion or destruction of personal data; and/or
4. Administrative fines.

Multiple sanctions may be imposed simultaneously, and sanctions may be imposed with or without a prior written reprimand. Sanctions will be imposed by the PDP Agency, which may coordinate with the relevant sectoral ministry or agency.

The PDP Agency must issue a sanction decision within 30 (thirty) working days of completing examination and tracing, which must be announced in the PDP Agency's official media and submitted to the data controller and/or processor. The public announcement of sanction decisions means that reputational consequences may be as significant as the sanction itself.

The sanctioned party must implement the decision within 30 (thirty) working days of announcement and may request an extension – subject to the PDP Agency's approval.

Enforcement process. Proceedings may start from a complaint by any person or from the PDP Agency's own supervision (Articles 188–199):

1. A preliminary review of a complaint within 3 working days of receipt; the complainant's identity may be kept confidential in certain circumstances.
2. An investigation (examination and tracing) to be completed within 14 working days, extendable by up to a further 60 working days. The PDP Agency may summon controllers and processors (with at least 3 working days' written notice), request documents and information, and inspect electronic systems, facilities and premises, including through appointed third parties, on the basis of a written statement of legal basis, scope and relevance.
3. A sanction decision within 30 working days after the investigation is completed, to be implemented within 30 working days of announcement.

The PDP Agency may also issue written orders to controllers and processors, including to stop or restrict processing, to suspend cross-border transfers, to terminate or amend agreements with processors or third parties, or to adopt and report on an action plan (Article 181), and may publish its supervisory findings (Article 183).

In imposing sanctions, the PDP Agency must consider:

1. The level or impact of the violation;
2. Continuity of business activities or public services;
3. Compliance history;
4. Clear basis for consideration and reasons; and
5. Other factors as determined by the PDP Agency.

As under the PDP Law, administrative fines are capped at 2% of the annual income or annual receipts of the controller and/or processor, calculated by reference to the "violation variable". In appropriate cases the fine may be set as low as IDR 0 (Article 185). GR 33/2026 further stipulates that the violation variable is calculated based on ten factors, as follows:

1. Negative impacts;
2. Duration of violation;
3. Type of personal data affected;
4. Number of data subjects affected;
5. How the violation was discovered;
6. Level of openness and cooperation;
7. Business scale;
8. Ability to pay;
9. Compliance; and
10. Other relevant variables.

A sanctioned party may submit a written objection to the head of the PDP Agency within 14 working days of receiving notification of sanctions. However, filing an objection does not suspend implementation of these sanctions. The head of the PDP Agency must decide within 14 working days; if no decision is made within that period, the objection is deemed granted. A rejected objection may be challenged before the State Administrative Court (Article 197).

Administrative sanctions are separate from civil and criminal liability. The PDP Law continues to provide for criminal penalties (imprisonment and fines, with corporate fines of up to ten times the maximum fine for individuals), and data subjects may claim compensation through the courts. Administrative fines are paid to the state and are not

linked to compensation of data subjects. The PDP Agency may request legal assistance from the Attorney General's Office to enforce its decisions (Article 198).

M. Dispute Resolution and Mediation

GR 33/2026 also provides a dispute resolution framework (Articles 200–222). Disputes may be resolved through arbitration, the courts or other alternative dispute resolution mechanisms. In addition, a data subject, controller or processor in dispute may report the dispute to the PDP Agency, which verifies the report and then (i) if there are indications of a criminal offence, asks the reporting party to report to the police, (ii) if there are indications of an administrative violation, processes the matter as administrative enforcement, or (iii) if neither, facilitates resolution, with priority given to mediation (Articles 201–206).

Mediation must be completed within 30 working days of the first meeting, extendable once by up to 30 working days by agreement and with the approval of the head of the PDP Agency. The mediator must be registered with the PDP Agency or come from a registered mediation institution; proceedings are confidential; parties must attend in person (online attendance counts as in person), with or without legal counsel; and a settlement agreement binds the parties and may be submitted to a court for a deed of settlement (Articles 207–220). The PDP Agency's mediation does not apply where the parties have already agreed a dispute resolution mechanism in their contract (Article 206(3)), so controllers and processors should review the dispute resolution clauses in their terms, processor agreements and privacy notices.

N. Other Noteworthy Matters

GR 33/2026 comes into force six months after its promulgation on 16 July 2026 (Article 225). This means that, although GR 33/2026 is not yet in effect, data controllers and processors should be ready to comply with its provisions by **16 January 2027**. This is not a general grace period for the PDP Law itself: the PDP Law has been in force since October 2022, its two-year transition period for controllers and processors ended in October 2024, and its obligations already apply and its criminal provisions can already be enforced.

That being said, we note that some 30 provisions of GR 33/2026 refer further detail to PDP Agency regulations. These include internal processing guidelines (Article 28), the vital interest, public interest and legitimate interest bases (Articles 48, 52 and 57), verification and rectification (Articles 69 and 73), automated decision-making (Article 96), restriction (Article 104), compensation (Article 110), portability (Article 113), breach notification (Article 119), impact assessments (Article 122), DPO appointment and competence (Articles 142–144), adequacy, binding safeguards and consent-based transfers (Articles 168, 172 and 174), supervision, complaints and sanctions procedures (Articles 180, 187, 189, 194 and 199) and mediation (Article 222).

Given that the PDP Agency has yet to be established, the practical operation of several mechanisms (such as the adequacy list, standard contractual clauses, approval of binding corporate regulations, regulatory consultation and the mediation process) will depend on the establishment of the PDP Agency and the issuance of its regulations. In the meantime, Article 223 allows controllers and processors to continue processing personal data provided this does not conflict with GR 33/2026, and Article 224 keeps existing data protection regulations in force insofar as they do not conflict with GR 33/2026. Sector-specific rules issued by other regulators will therefore continue to apply in parallel and may impose different requirements, for example different breach reporting timelines.

III. Outstanding Issues and Uncertainties

The following issues, which are addressed in the GDPR, the PDPA or regulatory practice elsewhere, are not (or not clearly) addressed in GR 33/2026. They may be clarified by PDP Agency regulations, sectoral regulators or practice:

a. **Regulator and timing.** The PDP Agency has not been established, so the adequacy list, standard contractual clauses, approval of binding corporate regulations, consultation, complaints handling and mediation cannot yet operate, and no timetable has been announced.
b. **Calculation of fines.** It is unclear whether the 2% cap applies to total annual revenue or only to revenue linked to the "violation variable", and how the revenue of corporate groups is treated.
c. **Breach notification.** There is no risk-based threshold, no mechanism for phased or provisional notification, and no fixed deadline for processors; the 3 × 24-hour clock depends on when the controller is deemed to have certain knowledge. Sectoral breach rules may impose parallel and different obligations.
d. **Verification and response deadlines.** It is unclear whether the 3 × 24 hours are suspended during verification, how the deadlines apply to complex or voluminous requests, and whether any extension, exception for manifestly unfounded or excessive requests, or fee is available (compare Article 12 of the GDPR).
e. **Right to object.** There is no general right to object to processing based on legitimate interests or public interest, and no right to object to direct marketing outside the consent context (compare Article 21 of the GDPR).
f. **Anonymisation.** GR 33/2026 refers to pseudonymisation and de-identification but does not define anonymisation or confirm that truly anonymised data falls outside its scope; given the broad concept of identifiability, including public domain data, anonymisation claims should be treated with caution.
g. **Employment and power imbalances.** There is no guidance on the validity of consent in employment or other imbalanced relationships, or on employee monitoring.
h. **Cross-border mechanics and offshore controllers.** The timeline for approving binding corporate regulations, the status of certifications or codes of conduct (compared with Articles 40 to 43 of the GDPR and the APEC certifications recognised in Singapore), whether DPOs or representatives must be located in Indonesia, how foreign controllers will be supervised and sanctioned, and the interaction with sector-specific localisation rules are not addressed.
i. **Corporate transactions.** It is unclear whether share acquisitions or asset and business transfers trigger the notification duties, how data room disclosures are treated before signing, and how pre-transaction notices should be timed against signing and regulatory approvals.
j. **Scope of exemptions.** The financial sector supervision and public interest exemptions are framed around state administration; it is unclear how far regulated private institutions (for example banks and fintech companies) may rely on them for fraud prevention and anti-money laundering monitoring.
k. **Retention and erasure.** GR 33/2026 requires retention policies but sets no retention periods, so controllers must reconcile erasure rights with sector-specific retention duties (for example tax, corporate records and anti-money laundering) and legal holds, and it is unclear how erasure from backups should be handled in practice.
l. **Compensation.** There is no deadline for responding to compensation claims, no guidance on quantifying material and immaterial loss, and it is unclear whether a prior claim to the controller is a mandatory step before suing.

IV. Conclusion

GR 33/2026 has provided much-needed detail on certain provisions and requirements of the PDP Law. These elaborations provide the further guidance required for data controllers and data processors operating within Indonesian jurisdiction to demonstrate compliance with Indonesian data protection requirements. At the same time, GR 33/2026 is in several respects stricter than the GDPR and the PDPA, in particular on response and notification deadlines, and it leaves a number of important questions open.

Furthermore, the period until GR 33/2026 comes into force on 16 January 2027 provides a limited window for data controllers and processors to adjust their local data protection practices. Given the volume of documentation, process and contractual changes required, we recommend that businesses begin their gap assessments now.

That being said, as certain subject-matters will be elaborated through regulations issued by a PDP Agency that has yet to be established, we expect that prevailing international good practice, including GDPR-aligned practices, will continue to serve as the practical benchmark in Indonesia until those regulations are issued. Businesses that act early will be better placed to adapt when the details are finalised.

Further Information and Assistance

For more detailed advice or assistance, please contact our legal team:



Naufal Fileindi
Co-Managing Partner
naufal.fileindi@lawghp.com

GHP law firm

World Trade Center 3, Level 27
Jl. Jend. Sudirman Kav. 29-31
Jakarta 12920, Indonesia

T: +6221 50110199

www.lawghp.com

This publication has been prepared by GHP Law Firm for educational and informational purposes only. The information contained in this publication is not intended and should not be construed as a legal advice. Due to the rapidly changing nature of law, GHP Law Firm makes no warranty or guarantee concerning the accuracy or completeness of this content. You should consult with an attorney to review the current status of the law and how it applies to your circumstances before deciding to take any action.