GR No. 33/2026: An Important Update to Indonesia's Legal Framework for Personal Data Protection



Introduction

The Indonesian Government has finally issued the long-awaited implementing regulation of Law No. 27 of 2022 on Personal Data Protection (the "**Privacy Law**" – please click here to read our publication on the introduction to the Privacy Law), ie Government Regulation No. 33 of 2026 ("**GR No. 33/2026**"). GR No. 33/2026 does not take effect until six months after the date of its enactment or 16 January 2027, to provide businesses sufficient time to comply with the new requirements.

GR No. 33/2026 transforms fundamental obligations under the Privacy Law into actionable items, such as establishing policies, mechanisms and channels relating to data subjects' rights, verifying and handling requests from data subjects and involving a data protection officer in all processing activities. It also further regulates the provisions under the Privacy Law regarding consent and other legal bases for data processing, cross-border data transfer, data transfer for a corporate action, automated decision making, data protection failure, administrative sanctions and dispute resolution.

GR No. 33/2026 also introduces additional principles drawn from existing principles under the Privacy Law, such as non-discrimination, data minimization and purpose limitation. It clarifies the supervisory and dispute resolution roles of the data protection agency ("**Agency**") as well and delegates further regulation of certain matters to the Agency.

Key Provisions

1. Consent as One of the Legal Bases for Processing Personal Data

GR No. 33/2026 requires that consent be obtained through a mechanism that provides concise, precise and relevant information about data processing. A mechanism for consent withdrawal must also be provided. Essentially, consent must be granted freely, knowingly, specifically and unambiguously by data subjects. If a data controller does not obtain consent from data subjects, it must still continue providing goods or services without reducing their quality, unless the provision of the same requires personal data processing.

GR No. 33/2026 also provides requirements for using other legal bases for processing personal data. Notably, to rely on other legitimate interests as a legal basis, a data controller must (i) conduct a documented analysis and assessment and (ii) explain the use of this legal basis to data subjects upon request.

2. The Rights of Data Subjects

GR No. 33/2026 introduces additional obligations for data controllers to establish policies, mechanisms and channels relating to data subjects' rights. For instance, data controllers are required to (i) establish a retention period policy and a policy for handling claims for compensation and (ii) create a personal data protection notification channel accessible to data subjects. It also requires data controllers to be transparent about which and how personal data is being processed.



Further, GR No. 33/2026 sets a procedure for handling data subjects' requests. It also provides requirements for applying exemptions to data subjects' rights. To apply the exemption for statistics and scientific research purposes, for instance, the purpose must not be commercial.

3. Certain Agreements Involving Data Controllers and Data Processors

GR No. 33/2026 provides the minimum content of (i) agreements between joint data controllers and (ii) agreements for data controllers or joint data controllers to appoint a data processor. It also requires data processors to prepare an agreement if they wish to appoint another data processor.

4. Data Protection Officer

GR No. 33/2026 grants data protection officers more concrete authorities to amongst others (i) be involved in every activity relating to data processing, (ii) report to the highest level of management, (iii) be given proper resources and access in performing their duties and (iv) be consulted in the preparation of a data protection impact assessment.



5. Cross-border Transfer of Personal Data

GR No. 33/2026 grants authority to the Agency to assess whether the level of protection provided by the receiving country is comparable to or higher than that under the Privacy Law, and data controllers must rely on this assessment when transferring personal data. If the receiving country has a lower level of protection, an adequate and binding personal data protection framework (in the form of legally binding instruments, standard contractual clauses, corporate group regulations and/or other instruments recognized by the Agency) would be required.

If the requirements for cross-border data transfers are not satisfied, a cross-border data transfer can still be conducted based on the data subject's consent, provided that (i) the transfer is not repetitive; (ii) the transfer involves a limited number of data subjects; (iii) the transfer is necessary for the purpose of fulfilling the provisions that do not override the rights of data subjects; (iv) the data controller has assessed the risks and implemented relevant protection measures; and (v) the data controller has informed the Agency and the data subject about the transfer and the urgent and legitimate interests fulfilled by such transfer.

6. Transfer of Personal Data in Corporate Actions



GR No. 33/2026 provides clearer requirements for transferring personal data in the event of a merger, spin-off, acquisition, consolidation or dissolution of a legal entity. Prior to transferring personal data, a data controller must conduct an assessment of (i) the data subjects' rights that are still required to be satisfied and (ii) the data controller's obligations that are still required to be fulfilled, during and after the corporate action process.

In addition, both the former and new data controllers must, amongst other things, (aa) notify the data subjects of the transfer before and after the corporate action becomes effective and (bb) enter into an agreement setting out their responsibilities in respect of personal data protection, which may form part of the agreement underlying the corporate action.

7. Automated Decision Making

GR No. 33/2026 elaborates on the right of data subjects to raise an objection against a decision made by automated processing, by requiring the data controller to (i) establish a mechanism for responding to such objection and (ii) inform the data subjects of the technology utilized for automated decision making and its consequences.

If an objection is verified and accepted, the data controller must provide alternative options, such as involving human intervention in automated processing or using manual processing entirely.

8. Data Protection Failure



GR No. 33/2026 retains the 72-hour timeframe provided by the Privacy Law to notify the Agency and the data subjects when a data protection failure occurs. Public notification is also required if such failure (i) disrupts public services and/or (ii) has a serious impact on public interest. Additionally, data controllers must document the failure and submit it to the Agency.

9. Dispute Resolution by the Agency

Data subjects, data controllers and data processors may report a dispute to the Agency, which will then verify the report and determine whether there is any administrative or criminal violation. If the Agency does not find any violation, it will facilitate the parties in resolving the dispute. The Agency prioritizes mediation, which will last for a maximum of 30 days since the first meeting.

SHIFT
COUNSELLORS AT LAW
www.shiftlegal.id

This article was prepared as an overview on the topic discussed and therefore, should not be relied upon as legal advice in any case. We accept no liability whatsoever for any loss or damage, whether due to inaccuracy, error, omission or any other cause. We will be pleased to respond to any questions you may have on this article or advise further on certain aspects of this article or other related matters.