Legal Update – Technology

KEY ASPECTS OF THE IMPLEMENTATION OF INDONESIA'S PERSONAL DATA PROTECTION LAW

7 October 2026

Personal data is now part of many everyday business activities, from customer interactions and employee management to digital services and business transactions. As the use of personal data continues to grow, so does the need for clear rules on how it should be handled and protected.

In Indonesia, Law Number 27 of 2022 on Personal Data Protection ("**PDP Law**") provides the main legal framework for personal data protection. To further implement the PDP Law and give more detailed guidance, the Government has issued Government Regulation Number 33 of 2026 on the Implementation of the PDP Law ("**GR 33/2026**").

Handling personal data can involve various situations in business activities. The sections below take a closer look at how GR 33/2026 addresses them.

What Are the Key Provisions Under GR 33/2026?

GR 33/2026 further regulates certain provisions under the PDP Law and provides additional requirements that businesses need to know when handling personal data. Here are some of the key points:

a. **Personal data processing**

Businesses may process personal data in many ways, such as collecting customer information, managing employee records, processing transactions, and providing services. Before carrying out these activities, a controller must have a valid basis for processing personal data. The bases include the individual's consent, the performance of a contract, compliance with a legal obligation, protection of vital interests, public interest, or other legitimate interests.

Where consent is used as the basis, it must be given freely, knowingly, specifically, and unambiguously. Before obtaining consent, the controller should provide the relevant information, have a mechanism to obtain consent electronically or non-electronically, and keep evidence of the consent provided. During the processing of personal data, the controller must be able to provide evidence of the consent given by the individual and ensure that the processing of personal data is not discriminatory.

For example, a company may ask customers to agree to receive marketing messages or allow their personal data to be used for a particular service. The customer should be able to understand what they are agreeing to and what their personal data will be used for before giving consent.

For businesses, it is important to ensure that personal data is processed on a valid basis and that any required consent is properly obtained and documented.

b. Automated processing

Automated processing refers to situations where a system or algorithm uses personal data to make a decision without human involvement. For example, a company may use a system to calculate a credit score, determine a price, decide whether an agreement should be terminated, or assess eligibility for certain benefits.

Where a decision is based solely on automated processing, the personal data controller must have a mechanism for responding to an objection from the individual affected by the decision. The controller must also explain the technology used to make the decision and provide an alternative that allows for human intervention.

However, the controller may reject an objection if the automated decision does not have legal consequences or a significant impact on the individual, provided that the system has a high level of accuracy and measures are in place to prevent harm to the individual. This does not affect the individual's right to withdraw their consent to the processing of their personal data. The controller must also notify the individual when an objection is rejected.

For businesses, this means that automated decision-making processes should also be supported by a clear mechanism for handling objections and providing human intervention where required.

c. Compensation mechanism for personal data processing violations

If a personal data processing violation causes harm to an individual, the individual may request compensation from the controller. The request must include the individual's identity, supporting evidence, and information on the legal relationship between the individual and the controller.

The controller must have a mechanism and policy for handling compensation requests. The controller will then assess the request and provide a response to the individual. To meet these requirements, businesses must have a clear process for receiving, assessing, and responding to compensation requests.

d. Corporate action notification

When a company undergoes a merger, spin-off, acquisition, consolidation, or dissolution, personal data may be transferred from the existing controller to a new controller. GR 33/2026 requires the relevant controllers to notify individuals about the transfer of their personal data in connection with these corporate actions.

The notification must include information about the transfer of personal data, the processing activities carried out in connection with the corporate action, the new controller, and when processing by the new controller will begin. It must also explain how individuals can object to the transfer or request that the processing of their personal data be stopped.

For businesses undergoing a corporate action, personal data should be considered as part of the planning process, particularly where personal data will be transferred to a new controller.

e. Cross-border personal data transfers

Businesses may transfer personal data to a controller or processor located outside Indonesia. In carrying out the transfer, the controller is required to:

i. record and map the personal data transfer cycle and its implications;
ii. ensure that the personal data transferred is adequate, relevant, and limited to what is necessary for the purpose of the transfer;
iii. identify the legal instrument used as the basis for the transfer and assess its effectiveness before the transfer takes place;
iv. use additional contractual, technical, or organizational safeguards (if needed), follow the required procedures for using those safeguards, and periodically review the transfer within an appropriate period;
v. inform the individual about the transfer before it takes place, including the purpose of the transfer, the safeguards in place to protect personal data and support the individual's rights, as well as the risks and measures taken to address those risks; and
vi. verify that the country where the recipient controller or processor is located has a level of personal data protection equivalent to or higher than that required under the PDP Law.

The assessment of the legal instrument takes into account matters such as the purpose of the transfer and processing, the parties involved, the sector in which the transfer takes place, the type of personal data being transferred, the transfer mechanism, where the data is stored and accessed, and the possibility of further transfers to other countries.

For businesses, cross-border data transfers require careful planning before personal data is sent outside Indonesia, including reviewing the transfer mechanism, the level of protection in the recipient country, and any additional safeguards that may be needed.

f. Administrative sanctions

Under GR 33/2026, violations may result in several types of administrative sanctions, including:

i. written warnings;
ii. temporary suspension of personal data processing activities;
iii. deletion or destruction of personal data; and/or
iv. administrative fines.

A violation may result in multiple sanctions, and a written warning does not always have to be issued first.

For administrative fines, the amount may be up to 2% of the annual income or revenue of the controller and/or processor. The amount of the fine may depend on factors such as the impact and duration of the violation, the type and number of personal data affected, the number of individuals affected, the scale of the business, and the level of

cooperation and compliance during the examination. In certain circumstances, the fine may be set at Rp0 or 0%.

Businesses can reduce the risk of administrative sanctions by identifying and addressing personal data protection risks early.

What Should Businesses Do?

As GR 33/2026 will take effect on 16 January 2027, businesses can use this time before then to review their current personal data practices and consider the following areas:

a. assess whether each personal data processing activity is supported by a valid basis;
b. identify whether any automated decision-making is used and ensure there is a process for handling objections where required;
c. put in place a mechanism for handling compensation requests;
d. take into account personal data transfers when planning corporate actions such as mergers, acquisitions, or dissolutions;
e. ensure that cross-border data transfers have an appropriate transfer mechanism, legal instrument, safeguards, and level of protection in the recipient country; and
f. address potential risks early to reduce the risk of violations and administrative sanctions.

Given the growing importance of personal data in business activities, staying up to date with regulatory developments can help businesses manage personal data responsibly and in line with applicable requirements. This is particularly relevant for businesses that regularly collect, use, or transfer personal data as part of their operations.

Should you have any questions or require assistance in preparing your business for the requirements under GR 33/2026, please feel free to contact our team.



Daniel Tampi
Managing Partner
+62 2125985130
+62 81280607094
daniel.tampi@clavislawfirm.id



Oliviani Yanto
Associate
+62 2125985130
+62 89625296921
oliviani.yanto@clavislawfirm.id

Disclaimer

This publication is prepared by Clavis Law Firm for general informational purposes only and does not constitute legal advice. It is intended to provide a high-level overview of the relevant legal and regulatory developments as of the date of publication and should not be relied upon as a substitute for specific legal advice.