Shape the future with confidence

Indonesia Regulatory Update: Indonesia's issues implementing regulation for the Personal Data Protection Law

September 2026

Tax Alert

News from EY Indonesia Tax Services

The Government of Indonesia has issued Government Regulation No. 33 of 2026 on the Implementation of Law No. 27 of 2022 on Personal Data Protection (GR 33/2026). Promulgated on 16 July 2026 and effective from 16 January 2027, GR 33/2026 introduces detailed operational requirements for personal data processing, data-subject rights, governance arrangements, cross-border transfers, regulatory supervision and administrative enforcement.

Executive summary

On 16 July 2026, the Government of Indonesia promulgated Government Regulation No. 33 of 2026 on the Implementation of Law No. 27 of 2022 on Personal Data Protection (GR 33/2026). GR 33/2026 is scheduled to take effect six months after its promulgation, i.e., on 16 January 2027. It is the principal implementing regulation contemplated by the Personal Data Protection Law (PDP Law).

GR 33/2026 is extensive. It translates the PDP Law's high-level requirements into operational rules covering the classification and processing of personal data, legal bases, data-subject request procedure, processor and joint-controller arrangements, records of processing, retention, breach response, data-protection impact assessments, data-protection officers, corporate transactions, cross-border transfers, regulatory supervision, administrative sanctions and dispute resolution.

However, the regulatory framework is not yet fully self-executing. Several technical and procedural matters remain subject to further regulations to be issued by the institution responsible for personal data protection under the PDP Law (the PDP Institution). Businesses should therefore treat GR 33/2026 as the core operational framework while monitoring the establishment and operation of the PDP Institution and the issuance of further implementing regulations.

Key takeaways include:

- **Operational compliance –** Controllers must document legal bases before processing, maintain internal processing rules, provide accessible notices, record processing activities, adopt retention policies, implement security measures and be able to evidence accountability.
- **Contract remediation –** Joint-controller arrangements and controller-processor appointments must contain prescribed minimum terms. Existing data-processing agreements should be reviewed before GR 33/2026 becomes effective.
- **Data-subject rights –** Controllers must provide accessible electronic and/or non-electronic request channels, verify requests proportionately and meet several 3 x 24-hour response or action deadlines.
- **High-risk processing –** A data-protection impact assessment must be completed before high-risk processing, including certain automated decisions, large-scale or specific-data processing, systematic monitoring, data matching and use of new technology.
- **Cross-border transfers –** The statutory hierarchy is retained: adequacy, binding safeguards, and only then consent. GR 33/2026 adds transfer mapping, risk assessment, advance notices and supplementary measures, but the adequacy country list and standard contractual clauses still require Authority regulations.
- **Enforcement exposure –** Administrative sanctions may include written warnings, suspension of processing, deletion or destruction, and fines of up to 2% of annual revenue or receipts, calculated against specified violation variables.
- **Regulatory dependencies –** Many practical details remain subject to Authority regulations. The effectiveness of supervision and approval also depends on establishment and operation of the Authority.

Background and Regulatory Context

The PDP Law establishes the principal rights of data subjects and the obligations of personal data controllers and processors. Many of its requirements are framed at a high level and require further implementing provisions.

Although GR 33/2026 materially develops the regulatory framework, it does not resolve every implementation issue. Various matters remain subject to further regulations, including procedural requirements concerning cross-border transfer mechanisms, automated decision-making, personal data protection officers, breach notification, data protection impact assessments and administrative enforcement.

Discussion

1. How GR 33/2026 implements PDP Law

The table below highlights the principal statutory mandates and the operational detail introduced by GR 33/2026.

Topic	PDP Law baseline	Key implementation under GR 33/2026
Scope and household exemption	Extraterritorial application where processing has legal effects in Indonesia or on Indonesian citizens abroad; private/household processing is excluded.[1]	Clarifies that the household exemption covers non-professional, non-commercial and non-public processing.[2]
Joint controllers and processors	Requires minimum arrangements for joint controllers; processors act on controller instructions and need written approval for sub-processors.[3]	Prescribes detailed joint-controller and processing-agreement contents; joint controllers have joint and several legal liability.[4]

1 Article 2 PDP Law
2 Articles 2 – 3 GR 33/2026
3 Article 51 PDP Law
4 Articles 11 – 16 GR 33/2026

Legal bases and transparency	Recognizes consent, contract, legal obligation, vital interest, public task and legitimate interest.[5]	Requires a legal basis before processing; specifies consent quality, contract necessity, legitimate-interest analysis and broad notice duties applying to all legal bases.[6]
Data-subject requests	Provides rights of access, correction, erasure, withdrawal, objection to automated decisions, restriction, compensation and portability.[7]	Creates request channels, content and verification rules; elaborates response mechanics and deadlines, including multiple 3 x 24-hour obligations.[8]
Records, retention and accountability	Requires recording of processing activities and accountability for compliance.[9]	Specifies ROPA fields, transfer details, security measures, retention-policy content, audit duties and production of records to the Authority.[10]
Security and breach response	Requires technical and operational safeguards and written notification within 3 x 24 hours to affected data subjects and the Authority.[11]	Specifies pseudonymization/encryption and resilience measures; clarifies notification trigger, content, public notice, incident documentation and processor reporting.[12]
DPIA and automated decisions	Requires DPIA for high-risk processing and permits objection to solely automated decisions with legal or significant effect.[13]	Requires DPIA before processing, minimum contents, review on risk changes and documented DPO advice; requires a human-intervention alternative for accepted objections.[14]
Corporate transactions	Requires notice of personal data transfers before and after merger, demerger, acquisition, consolidation or dissolution.[15]	Adds due diligence, allocation of old/new controller responsibilities, notices, data-protection agreement and treatment as joint controllers during the transition.[16]
Cross-border transfer	Requires adequacy; if unavailable, adequate and binding safeguards; if neither applies, data-subject consent.[17]	Adds transfer mapping, legal-instrument and risk assessments, notices, supplementary measures, adequacy criteria, SCCs, binding corporate rules and restrictive conditions for consent.[18]
Supervision, sanctions and disputes	Authorizes the Authority to supervise, investigate and impose administrative sanctions; disputes may proceed through arbitration, court or ADR.[19]	Sets complaint, examination, sanction and objection procedures; permits fines up to 2%; establishes Authority-facilitated mediation procedures.[20]

5 Article 20 PDP Law
6 Articles 30 – 57 GR 33/2026
7 Articles 5 – 15 PDP Law
8 Articles 20 – 27, 71, 77, 92, 99, 103, 114 GR 33/2026
9 Articles 31 – 47 PDP Law
10 Articles 74 – 75, 138 GR 33/2026
11 Articles 35, 46 PDP Law
12 Articles 114 – 119, 123 – 130 GR 33/2026
13 Articles 10, 34 PDP Law
14 Articles 94, 120 – 122 GR 33/2026
15 Article 48 PDP Law
16 Articles 131 – 137 GR 33/2026
17 Article 56 PDP Law
18 Articles 160 – 174 GR 33/2026
19 Articles 57 – 60, 64 – 66 PDP Law
20 Articles 180 – 222 GR 33/2026

2. Selected provisions requiring priority implementation

- **Legal basis, notices and consent** | GR 33/2026 requires the controller to determine a lawful basis before processing. Consent must be freely given, informed, specific and unambiguous. A refusal to consent may not reduce the quality of goods or services unless the requested processing is necessary to provide them. Privacy information must be concise, accurate, accessible and generally available throughout processing; where data is collected indirectly, notice is due within 30 business days.[21]
- **Data-processing agreements and governance** | Controller-processor agreements must address scope, method, purpose, data categories, data-subject categories, duration, parties' rights and obligations, oversight, documentation, audit and inspection, disputes, sub-processors and a contact person. Joint-controller agreements must allocate legal bases, purposes, methods, data categories and responsibilities.[22]
- **ROPA, retention and deletion** | The required record of processing activities includes controller/processor details, DPO contact, source and destination, legal basis, purpose, data categories, recipients, rights handling, data-flow mapping, retention, security measures and transfer details. A written retention policy must cover retention periods, archival rules, de-identification, destruction methods, processor requirements, responsibility and legal basis. Deletion and destruction also require documented operational steps and an official record.[23]
- **Security, incidents and DPIA** | Security measures should include pseudonymization, encryption or other controls, system resilience, timely restoration and periodic testing. Breach notification is due within 3 x 24 hours after the incident is known with sufficient certainty, reasonableness and propriety. DPIAs must precede high-risk processing and be revisited when risk changes.[24]
- **DPO/PPDP governance** | The appointment thresholds remain based on public services, regular and systematic large-scale monitoring, and large-scale processing of specific or criminal-offence data. GR 33/2026 adds organizational requirements: appropriate resources, access to top management, objective and independent operation, involvement in processing activities, access to information and avoidance of conflicts of interest.[25]

3. Cross-border Transfers

GR 33/2026 confirms a three-tier transfer mechanism and adds pre-transfer governance obligations. The controller should not treat consent as a routine substitute for adequacy or safeguards analysis.

Tier	Transfer route	GR 33/2026 detail	Outstanding dependency
1	Equivalent or higher protection	The Authority assesses foreign jurisdictions using the existence of data-protection laws, independent supervisory authority and relevant international commitments.	The Authority must establish the country and/or international-organization list and issue the assessment procedure.
2	Adequate and binding safeguards	Permitted instruments include legally binding and enforceable arrangements, standard contractual clauses, binding corporate rules and other Authority-recognized safeguards.	The Authority must issue SCCs, further implementation rules and approvals for binding corporate rules.
3	Data-subject consent	Consent is available only if the transfer is non-recurring, involves a limited number of data subjects, is necessary for a compelling legitimate interest that does not override rights, is risk-assessed and safeguarded, and is notified to the Authority and data subject.	Further rules on consent-based transfers must be issued by the Authority.

21 Articles 30 – 37, 61 – 66 GR 33/2026

22 Articles 11 – 16 GR 33/2026

23 Articles 74 – 75, 82 – 89 GR 33/2026

24 Articles 114 – 130 GR 33/2026

25 Articles 142 – 147, Elucidation of Article 161(d) GR 33/2026

Before any transfer, controllers must map the transfer lifecycle, ensure data minimization, identify and assess the relevant legal instrument, assess transfer risk and the receiving-country context, consider supplementary contractual, technical or organizational measures, notify the data subject of the transfer and periodically reassess effectiveness. The explanatory text expressly includes the risk of access by public authorities in a third country in the legal-instrument assessment.[26]

4. Matters that remain dependent on further regulation

GR 33/2026 materially narrows many gaps in the PDP Law but does not finalize all operational points. The most important dependencies are summarized below.

Outstanding matter	Current position under GR 33/2026	Further instrument required
PDP supervisory authority	GR 33/2026 repeatedly assigns assessments, approvals, supervision and sanctions to the "Authority", but does not establish the institution.	Presidential Regulation under PDP Law Article 58(5).
Adequate countries/ organizations	Sets assessment criteria and requires the Authority to publish a list.	Authority regulation and adequacy list under Article 168(2) and (4).
Standard contractual clauses (SCC) and binding safeguards	Recognizes SCCs, binding corporate rules (BCR) and other safeguards.	Authority-issued SCCs and implementation rules under Articles 170 and 172; Authority approval for BCRs under Article 171(3).
Automated decision-making	Provides objection, disclosure and human-intervention requirements.	Authority regulation under Article 96.
DPO/PPDP thresholds and competence	Retains appointment tests and sets governance duties.	Authority regulations under Articles 142-144.
Data-subject rights procedures	Creates general requests, verification and response rules.	Authority regulations for notices, correction, termination/deletion, restriction, compensation and portability under Articles 66, 73, 89, 104, 110 and 113.
Breach notification and DPIA	Sets substantive duties and minimum contents.	Authority regulations under Articles 119 and 122.
Processing, security and oversight standards	Requires internal policies, verification, security, accountability and controller supervision.	Authority guidance/regulations under Articles 28(2), 69(9), 123(7) and 128.
Administrative enforcement	Sets sanction types, variables, investigation and objection process.	Authority regulations under Articles 187, 189(5), 194 and 199.
Mediation and dispute facilitation	Provides Authority-facilitated mediation and procedural timelines.	Authority regulations under Articles 202(4), 207(6) and 222.

26 Articles 160 – 174 GR 33/2026

Insights and Practical Implications

- **By the effective date:** Complete a gap assessment against GR 33/2026; priorities high-risk processing, customer/employee notices, request handling, breach response and cross-border transfers.
- **Data inventory:** Create or update the ROPA, data-flow maps, legal-basis register, retention schedule and international-transfer register.
- **Contracts:** Review controller-processor, sub-processor, joint-controller, intragroup and M&A documentation against the mandatory content.
- **Rights and incidents:** Implement verified intake channels, 3 x 24-hour escalation timelines, breach decision records and notification templates.
- **Cross-border transfers:** Do not wait for the country list to map transfers. Identify destinations, recipients, remote-access locations, transfer mechanisms and supplementary measures now.
- **Regulatory watch:** Monitor the Presidential Regulation establishing the Authority and subsequent Authority regulations.

Contact us

Tax Services Leader	E-mail
Bambang Suprijanto	bambang.suprijanto@id.ey.com

Partner/Director/Senior Advisor	E-mail
Abraham Siahaan	abraham.siahaan@id.ey.com
Agung Wicaksono	agung.wicaksono@id.ey.com
Anna Tasya Daru Pratiwi	anna.pratiwi@id.ey.com
Anita Priyanti	anita.priyanti@id.ey.com
Ben Koesmoeljana	ben.koesmoeljana@id.ey.com
Cindy P. Galag	cindy.p.galag@id.ey.com
Dany H. Karim	dany.karim@id.ey.com
David Setiyawan	david.setiyawan@id.ey.com
Dodi Suryadarma	dodi.suryadarma@id.ey.com
Elly Djoenaidi	elly.djoenaidi@id.ey.com
Fahrul S. Yusuf	fahrul.yusuf@id.ey.com
Henry Tambingon	henry.tambingon@id.ey.com
Ihsan Muttaqien	ihsan.muttaqien@id.ey.com
Iman Santoso	iman.santoso@id.ey.com
Jonathon McCarthy	jonathon.mccarthy@id.ey.com
Kartina Indriyani	kartina.indriyani@id.ey.com
Markus Hidajat	markus.hidajat@id.ey.com
Melyana Trisanty	melyana.trisanti@id.ey.com
Micky M. Soeradiredja	micky.mintarsyah@id.ey.com
Nathanael Albert	nathanael.albert@id.ey.com
Nitya Citra Ayu	nitya.ayu@id.ey.com
Novita Fitriawatie	novita.fitriawatie@id.ey.com
Peter Mitchell	peter.mitchell@id.ey.com
Peter Ng	peter.ng@id.ey.com
Regina R. Sugianto	regina.riani@id.ey.com
Roy M. Sibuea	roy.m.sibuea@id.ey.com
Ryosuke Seto	ryosuke.seto@id.ey.com
Santoso Goentoro	santoso.goentoro@id.ey.com
Sharala Panjanadan	sharala.panjanadan1@id.ey.com
Triadi H. Mukti	triadi.mukti@id.ey.com
Yan Hardyana	yan.hardyana@id.ey.com
Yudie Paimanta	yudie.paimanta@id.ey.com

Ernst & Young LLP (United States), Indonesia Tax Desk, New York	E-mail
Myrna S. Ryzkiria	myrna.s.ryzkiria1@ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

ey.com/id

For other services contact: