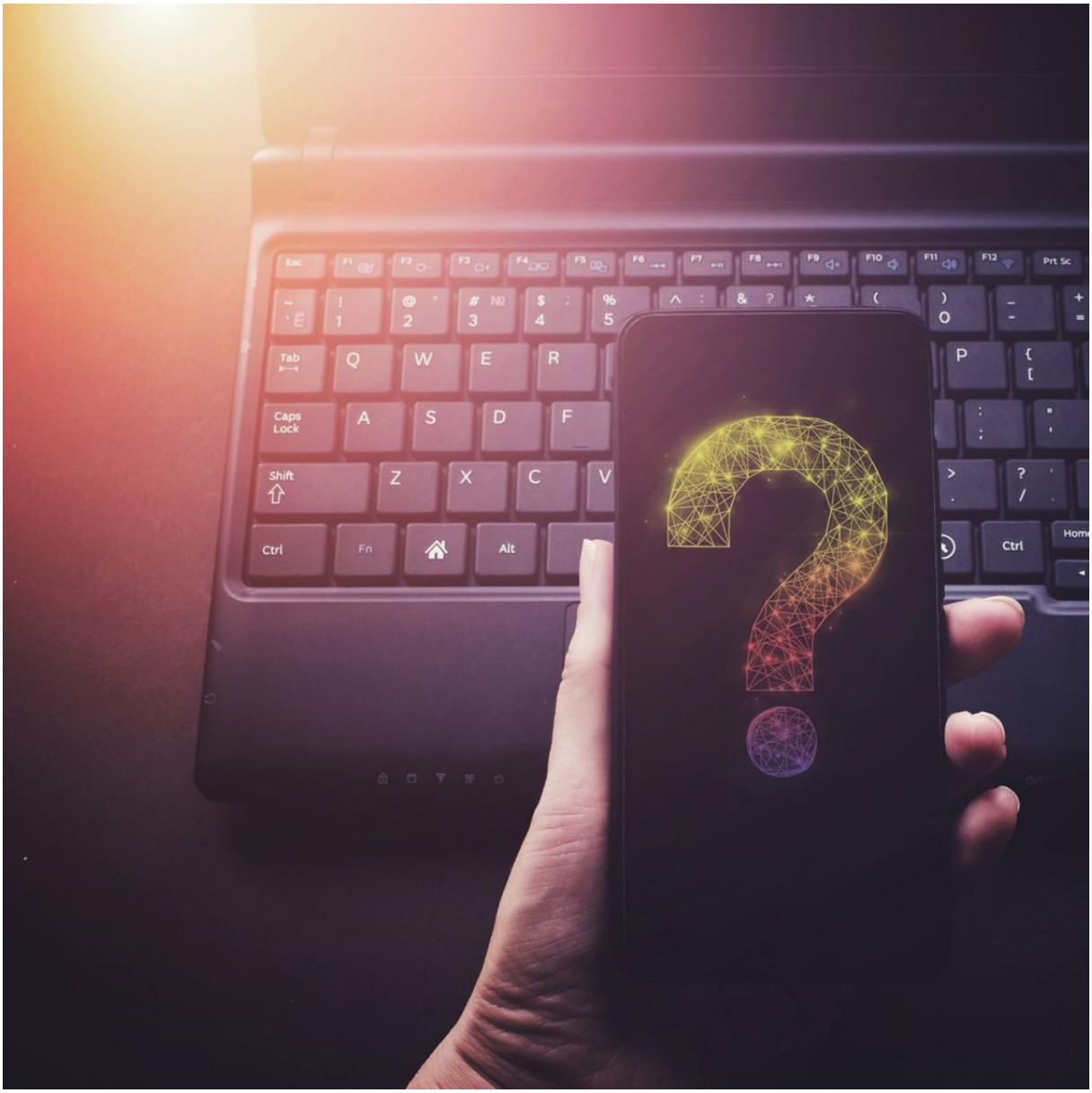
Indonesia Client Update

2 SEPTEMBER 2026

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

PDP Law Updates: The PDP Implementing Regulation Is Out, and It Clarifies Some Key Questions Under Indonesia's PDP Law



© ASSEGAF HAMZAH & PARTNERS

In our previous client updates on Indonesia's Personal Data Protection Law (Law No. 27 of 2022) (the "**PDP Law**"), we discussed a number of issues that remained subject to further clarification pending implementing regulations. The long-awaited implementing regulation of the PDP Law has now been issued through Government Regulation No. 33 of 2026 on the Implementation of the PDP Law ("**GR 33**"), which was enacted and promulgated on 16 July 2026. Surprisingly, as of the date of this update, GR 33 has not yet been officially published on the official website of the State Secretariat[1] or formally announced by the Government, although copies have circulated among practitioners since late August 2026. To the extent the circulating version is authentic, we are of the view that its formal enactment is sufficient for GR 33 to be regarded as validly in force under Indonesian law.

It is important to note that GR 33 provides a six-month transition period from its 16 July 2026 promulgation, meaning that as of 16 January 2027, any non-compliance of GR 33 requirements will be subject to administrative sanctions.

GR 33 contains 225 articles. This update highlights the developments most relevant in practice, rather than an article-by-article summary.

1. Data Breach Notification Requirements

GR 33 clarifies that the 72-hour breach notification period begins to run only when a personal data protection failure has been established with certainty and on reasonable grounds (*pasti, patut dan wajar*). In making this determination, a data controller must rely on relevant supporting documentation. In our view, such documentation may include system logs, forensic investigation reports, and other corroborating evidence relating to the incident. This clarification recognises that controllers require sufficient time to assess, verify, and substantiate a suspected incident before triggering their statutory notification obligations. As a result, GR 33 provides welcome certainty that the 72-hour notification clock does not commence until a controller has completed a reasonable assessment and concluded, based on documented evidence, that a personal data protection failure has in fact occurred.

Controllers must also document, for each failure, the data affected, the circumstances surrounding the failure, its consequences, any remediation actions taken, and when notifications were provided. Moreover, controllers must maintain internal policies and procedures for preventing and handling breaches.

2. Lawful Bases for Processing

GR 33 does not change the six lawful bases for processing but clarifies the two bases that generated the most uncertainty: contractual necessity and legitimate interests.

For processing based on contractual necessity, processing must be necessary either to perform an agreement involving the data subject or to fulfil a pre-contractual request. In this case, the agreement must address the purpose of processing, its relationship to the contract, the data subject's rights, and the consequences of not processing.

For legitimate interests, a controller must assess the necessity of the processing, the purpose pursued by the controller, and the balance between its interests and the data subject's rights (commonly referred to as a Legitimate Interest(s) Assessment or "**LIA**"). In addition, the controller must mitigate and document any adverse risks to the data subject. The Elucidation to GR 33 notes that legitimate interests may include

[1] https://jdih.setneg.go.id/produk-hukum/All

security monitoring, health and safety, and crime prevention. Organisations relying on this basis should implement and document an LIA.

3. Cross-Border Transfers

Cross-border personal data transfers have been one of the areas of the PDP Law that generated the practical uncertainty in practice. While the PDP Law established a three-tier transfer mechanism consisting of adequacy decision, appropriate safeguards, and express consent from data subjects, it did not provide significant guidance on how those mechanisms would operate in practice.

GR 33 provides more detail on the implementation of cross-border transfer requirements. One of such clarifications relates to adequacy assessments. The PDP Law previously referred to jurisdictions with an equivalent or higher level of protection but did not specify who would be responsible for making that determination. GR 33 now confirms that adequacy assessments will be conducted by the data protection authority ("**DPA**"), which will maintain a "whitelist" of adequate jurisdictions.

Where adequacy is unavailable, GR 33 recognises appropriate safeguards, which may include Standard Contractual Clauses (SCCs, to be issued by the DPA) and Binding Corporate Rules (BCRs, for intra-group transfers). However, Binding Corporate Rules require prior DPA approval before use.

Consent is available only as a narrow fallback, namely where the transfer is one-off (not systematic), involves a limited number of data subjects, serve a purpose that does not override the data subject's interests, follow a risk assessment with safeguards, and be disclosed to both the DPA and the data subject.

4. DPOs

GR 33 formally incorporates the Constitutional Court's clarification in 2025 that a data protection officer ("**DPO**") must be appointed whenever any one statutory condition is met, rather than only where all conditions are met simultaneously (click here to read our previous client update). GR 33 also details the functions of a DPO, which include advising on compliance, monitoring compliance, advising on and being consulted during data protection impact assessments ("**DPIAs**"), and acting as a point of contact.

GR 33 also emphasises DPO independence. The DPO must be involved in all processing activities, have direct access to senior management, operate free from intervention, receive adequate resources and access, and remain free from conflicts of interest, with its activities documented as part of the DPIA. Organisations should reassess whether their existing processing activities trigger the appointment requirement and whether current reporting lines and resourcing meet these standards.

5. ROPA and Accountability Records

Controllers must maintain a record of processing activities ("**ROPA**") covering all processing activities, functioning as both a register of processing activities and a data-flow map within the organisation. At minimum, it must record controller/processor and DPO details, sources of collection, transfer destinations, lawful basis, processing purposes, data categories, third-party access, data subject rights fulfilment, retention periods, security measures, and transfer details.

More broadly, GR 33 requires controllers to demonstrate compliance through appropriate technical and organisational measures, documented processing activities, responsiveness to DPA requests, and internal/external audits.

6. DPIAs

The Elucidation to GR 33 clarifies that "large-scale processing", a DPIA trigger under the PDP Law, is to be assessed contextually, by reference to the volume of data processed, the number of data subjects affected, the duration of processing, the type of data involved, the purpose of processing, and its geographic scope, rather than a fixed numerical threshold. This is a self-assessment exercise for the controller to carry out. Under GR 33, further technical provisions on DPIAs, which we expect to include a self-assessment template with numerical scoring or thresholds, are to be set out in a forthcoming DPA regulation. The Elucidation separately identifies "new technology" as its own DPIA trigger, citing artificial intelligence, machine learning, smart technology, and the internet of things as examples.

GR 33 also details the minimum content of a DPIA: a description of the processing, an assessment of its necessity and proportionality, an assessment of risks to data subjects, and the mitigation measures proposed. A DPIA must be updated where the risk profile of the processing changes. Where a DPO has been appointed, its advice must be documented as part of the DPIA. GR 33 also allows controllers to consult with the DPA (once established) in relation to higher-risk processing.

7. Data Subject Rights

The PDP Law requires controllers to fulfil data subject's requests, including requests to update or correct personal data, access personal data, obtain copies of personal data, withdraw consent, and restrict or suspend processing, within 72 hours. GR 33 reaffirms this 72-hour deadline across each of these rights, and requires controllers to verify both the requesting party's identity and their entitlement to exercise the relevant right, using a mechanism proportionate to the purpose, the technology available, and the time reasonably required.

For most of these rights, that verification requirement is to be carried out within the 72-hour period rather than as a pre-condition to it. The clock starts on receipt of the request, and verification is a step to be completed within that window. Requests to obtain copies of personal data are the exception as GR 33 ties the 72-hour period to verification, so the clock only starts once the request has been both received and verified. This reading, and its implications for how the deadline should be applied in practice, remains subject to further clarification and regulatory development.

8. Corporate Transactions

GR 33 details how personal data must be handled in mergers, acquisitions, consolidations, spin-offs, and dissolutions. As required under the PDP Law, controllers must notify data subjects before and after the transaction. GR 33 clarifies that the notification must include information on the data transfer, the new controller's identity, intended processing, timing, and the mechanism to object. Before transferring data, controllers must assess outstanding and continuing obligations and whether DPIAs need updating, and the transferring and receiving controllers must enter into a data sharing agreement.

Notably, GR 33 treats the parties as joint controllers between signing and legal completion of the corporate transactions.

9. Privacy Notices

GR 33 extends notice obligations to personal data collected indirectly (e.g., from affiliates, vendors, public sources, or corporate transactions). Here, controllers must notify the data subject within 30 business days of collection. Notices must disclose the controller's identity, lawful basis, processing purposes, data categories, retention periods, sources, recipients/transfers, security measures, processing lifecycle, and data subject rights. This notice must be accessible and updated.

GR 33 also prohibits exoneration clauses, i.e., provisions that reduce, limit, or exclude a controller's obligations. Organisations should review existing privacy notices and third-party onboarding to remove any such language and address indirect collection scenarios.

10. **Administrative Fines**

GR 33 confirms fines of up to 2% of annual revenue apply across the PDP framework (lawful bases, notice, data subject rights, breach notification, cross-border transfers, ROPA, DPIAs, DPO appointment, security, and accountability). The Elucidation to GR 33 also clarifies that "revenue" means gross economic inflows, not net profit. The fine amounts may also take into account the categories and number of data subjects affected.

Beyond the fine calculation framework, GR 33 sets out procedures for complaints, investigations, and objections. However, an objection does not automatically suspend enforcement.

Key Takeaways and Next Steps

GR 33 gives organisations meaningfully greater certainty across these areas, but a number of operational details, such as the adequacy decisions, SCC templates, BCR approval, DPIA methodology, and enforcement mechanics, remain subject to future DPA guidance, most of which depends on the DPA's formal establishment. Organisations should use the transition period to review breach response procedures, lawful basis assessments (particularly legitimate interests), DPO governance, ROPA and DPIA practices, cross-border transfer arrangements, data subject request workflows, privacy notices, and data handling in any pending corporate transactions.

If you have any queries on the above, please reach out to our team set out on this page.

For regional Technology, Media & Telecommunications matters, please see Rajah & Tann Asia's Regional Technology, Media & Telecommunications Practice for more information.

Contacts

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

Zacky Zainal Husein

PARTNER

D +62 21 2555 9956
zacky.husein@ahp.id

Muhammad Iqsan Sirie

PARTNER

D +62 21 2555 7805
iqsan.sirie@ahp.id

Contribution Note

This Legal Update is contributed by the listed Contact Partners, with the assistance of Associates **Daniar Supriyadi** and **Owen Gavriel Suherman**.

Please feel free to also contact Knowledge Management at RTApublications@rajahtann.com.

Regional Contacts

Cambodia
Rajah & Tann Sok & Heng Law Office

T +855 23 963 112 | +855 23 963 113
kh.rajahtannasia.com

China
Rajah & Tann Singapore LLP
Representative Offices

Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820

Shenzhen Representative Office
T +86 755 8898 0230
cn.rajahtannasia.com

Indonesia
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

Lao PDR
Rajah & Tann (Laos) Co., Ltd.

T +856 21 454 239
la.rajahtannasia.com

Malaysia
Christopher & Lee Ong

T +603 2273 1919
F +603 2273 8310
www.christopherleeong.com

Myanmar
Rajah & Tann Myanmar Company Limited

T +951 9253750
mm.rajahtannasia.com

Philippines
Gatmaytan Yap Patacsil Gutierrez & Protacio
(C&G Law)

T +632 8248 5250
www.cagatlaw.com

Singapore
Rajah & Tann Singapore LLP

T +65 6535 3600
sg.rajahtannasia.com

Thailand
Rajah & Tann (Thailand) Limited

T +66 2656 1991
th.rajahtannasia.com

Vietnam
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2673 | +84 28 3521 2832

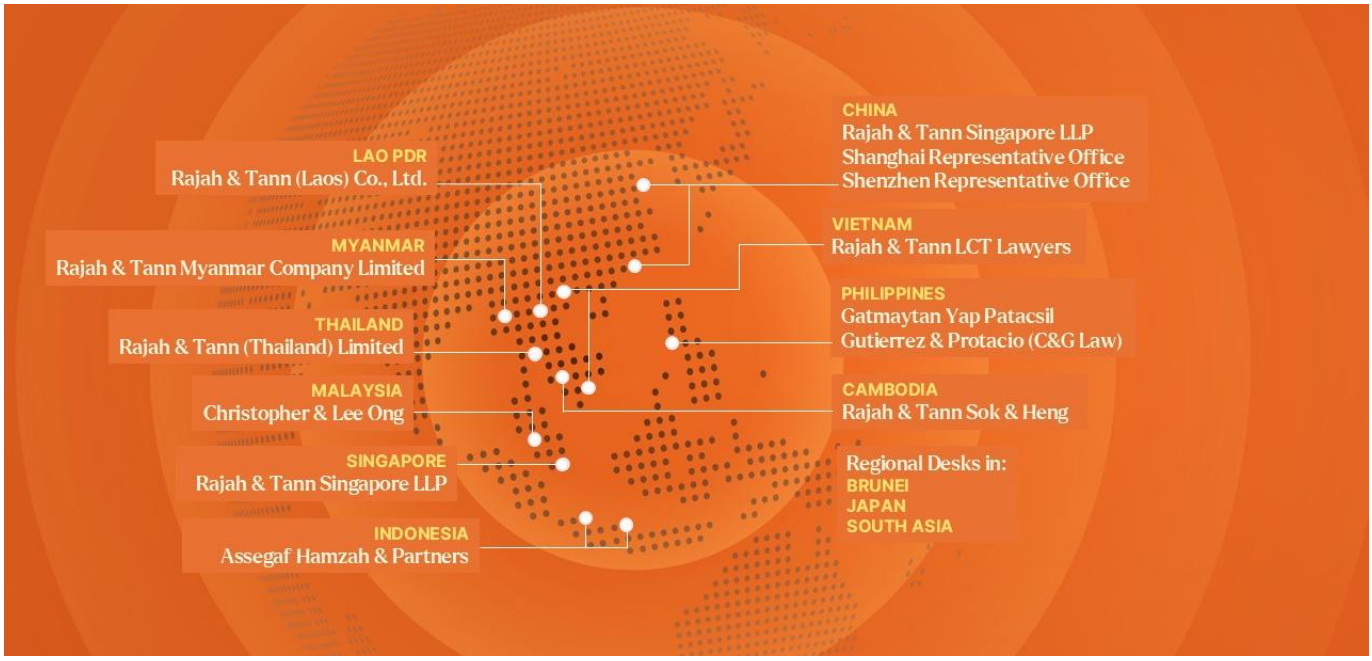
Hanoi Office
T +84 24 3267 6127 | +84 24 3267 6128
vn.rajahtannasia.com

Rajah & Tann Asia is a network of legal practices based in Asia.

Member firms are independently constituted and regulated in accordance with relevant local legal requirements. Services provided by a member firm are governed by the terms of engagement between the member firm and the client.

This update is solely intended to provide general information and does not provide any advice or create any relationship, whether legally binding or otherwise. Rajah & Tann Asia and its member firms do not accept, and fully disclaim, responsibility for any loss or damage which may result from accessing or relying on this update.

Our Regional Presence



Based in Indonesia, and consistently gaining recognition from independent observers, Assegaf Hamzah & Partners has established itself as a major force locally and regionally, and is ranked as a top-tier firm in many practice areas. Founded in 2001, it has a reputation for providing advice of the highest quality to a wide variety of blue-chip corporate clients, high net worth individuals, and government institutions.

Assegaf Hamzah & Partners is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.

The contents of this Update are owned by Assegaf Hamzah & Partners and subject to copyright protection under the laws of Indonesia and, through international treaties, other countries. No part of this Update may be reproduced, licensed, sold, published, transmitted, modified, adapted, publicly displayed, broadcast (including storage in any medium by electronic means whether or not transiently for any purpose save as permitted herein) without the prior written permission of Assegaf Hamzah & Partners.

Please note also that whilst the information in this Update is correct to the best of our knowledge and belief at the time of writing, it is only intended to provide a general guide to the subject matter and should not be treated as a substitute for specific professional advice for any particular course of action as such information may not suit your specific business and operational requirements. It is to your advantage to seek legal advice for your specific situation. In this regard, you may contact the lawyer you normally deal with in Assegaf Hamzah & Partners.