TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

Indonesia's PDP Law Updates: DPA, U.S. Trade-Related Data Transfers, and Recent Court Rulings

 © ASSEGAF HAMZAH & PARTNERS

As discussed in our previous Client Update on Indonesia's Personal Data Protection Law (Law No. 27 of 2022, "**PDP Law**"), the regulatory landscape and enforcement environment continue to evolve rapidly. In that update, we examined recent clarifications on when organisations are required to appoint a data protection officer, as well as key constitutional court cases concerning cross-border data transfers and the criminalisation of unlawful data disclosure.

This update highlights three further developments that are relevant to organisations operating in or dealing with Indonesia:

1. The issuance process of a draft Presidential Regulation on the Data Protection Authority ("**DPA**"), which will formally establish Indonesia's long-awaited supervisory authority;

2. Indonesia's cross-border data transfer commitments to the United States under the U.S.-Indonesia Agreement on Reciprocal Trade dated 19 February 2026 ("**Trade Agreement**"); and

3. Recent court rulings that continue to shape compliance expectations under the PDP Law.

We explain each of these developments below.

Data Protection Authority

Article 58(5) of the PDP Law mandates the establishment of a DPA through a presidential regulation. In line with this requirement, the Government has formulated a draft Presidential Regulation ("**Draft Regulation**"), which was finally made public at the end of February 2026, nearly four years after the enactment of the PDP Law.

The Draft Regulation, prepared by the Ministry of Communication and Digital Affairs ("**MOCD**"), has been submitted to the Ministry of State Secretariat and is currently awaiting presidential approval. Once enacted, it will formally establish Indonesia's DPA, an institution long contemplated under, but previously absent from, the PDP Law framework. The DPA will oversee compliance with and enforcement of the PDP Law.

Under the Draft Regulation, the DPA will be classified as a non-ministerial government agency reporting to the President through the MOCD. While the MOCD will serve as the reporting and accountability channel, it will not exercise operational supervisory authority over the DPA. The DPA will be led by a Head appointed by the President and supported by three deputies responsible for (i) policy and guidance, (ii) dispute resolution, and (iii) compliance and enforcement.

Articles 3 and 4 of the Draft Regulation set out the DPA's mandate, which includes policy formulation and implementation, regulatory oversight, administrative enforcement, out-of-court dispute resolution, and any additional functions assigned by the President.

The Draft Regulation also contains transitional provisions intended to ensure that the DPA becomes operational immediately upon its establishment. During this transition period, the DPA Head will employ the personnel and use other resources from the personal data protection unit within the MOCD's Directorate General for Digital Space Oversight until its own organisational capacity is fully established. Separately, to prevent duplication and overlapping functions within the Government, the Draft Regulation further requires that personnel from that unit be transferred to and integrated into the DPA.

U.S.-Indonesia Reciprocal Trade Agreement

The reciprocal trade agreement reached between the United States and Indonesia includes a notable commitment relating to cross-border data flows. Under Article 3.2 of Annex III (Specific Commitments), Indonesia is required to provide legal certainty for the transfer of personal data to the United States by recognising the United States as a jurisdiction that offers adequate data protection under Indonesian law. In practical terms, this commitment appears to imply that the United States is automatically regarded as a country whose data protection standards are equivalent to, or exceed, those of Indonesia.

The Trade Agreement does not, however, have immediate legal effect under Indonesian law. Under Article 84 of Law No. 7 of 2004 on Trade (as amended), the Trade Agreement must first undergo a ratification process, which requires its submission to the House of Representatives (*Dewan Perwakilan Rakyat*) within a prescribed timeframe. The House will then determine whether parliamentary approval is required and, if so, whether ratification must be implemented through a Law (*Undang-Undang*) or a Presidential Regulation.

A separate issue arises under the PDP Law itself. Article 56 of the PDP Law requires data controllers to ensure that the destination jurisdiction affords a level of personal data protection equivalent to or higher than that of the PDP Law. Based on the forthcoming implementing regulation of the PDP Law, this obligation is expected to be discharged through a formal adequacy assessment and decision by the DPA, an assessment that the Trade Agreement, as an international trade instrument, cannot replace. At this stage, it remains unclear how the Government will operationalise this requirement in respect of transfers to the United States, including whether this will be addressed through a formal adequacy determination by the DPA, amendments to implementing regulations, a formal assessment process, or another regulatory mechanism.

Recent Court Rulings

Since the PDP Law came into effect in October 2022, enforcement activity and litigation have steadily increased across three forums: criminal courts, civil courts, and the constitutional court. Based on our review of publicly available court registries and government directories, to date, there have been at least 23 criminal cases, 7 civil cases, and 6 constitutional court decisions involving the PDP Law. This dataset may not be exhaustive, as certain cases may not yet have been published.

The section below summarises selected cases decided between 2025 and 2026, together with key observations relevant to organisations subject to the PDP Law.

Criminal Proceedings

Three notable personal-data related criminal cases were decided by different district courts in 2025. These cases involved:

1. The misuse of identity information to create Telegram accounts and monetise one-time passwords (OTPs);
2. Unauthorised access to government systems to extract and sell employee data on the dark web; and
3. The misuse of personal data to unlawfully reactivate a dormant account.

In each case, the courts found the defendants guilty of unlawful use of personal data under Article 65(3) of the PDP Law and unlawful data collection for personal gain under Article 65(1). However, with the exception of the Telegram

case, the PDP Law was applied only as an alternative legal basis, with the courts relying primarily on the Electronic Information and Transactions Law (Law No. 11 of 2008, as amended) in reaching their decisions.

Two points are particularly relevant for businesses:

1. Articles 65(1) and 65(3) of the PDP Law are fully operational as criminal provisions. The courts have applied them in practice, confirming that unlawful collection and misuse of personal data can give rise to genuine criminal exposure; and

2. The PDP Law currently operates as a secondary enforcement framework, with courts continuing to rely primarily on the Electronic Information and Transactions Law. This reflects the transitional nature of PDP Law enforcement and the gradual integration of its criminal provisions into judicial practice.

Civil Proceedings

One notable civil case was filed before West Jakarta District Court in January 2026. The case was brought by three former contract employees against a data controller, alleging unlawful personal data processing practices.

The core dispute concerns the controller's conduct of credit-history checks on contract workers without consent or a contractual basis. The claim also includes unilateral contract termination, failure to participate in bipartite mediation, and a range of alleged labour law violations, including abrupt end-of-contract notices, sudden loss of system access, unverified compensation calculations, and unpaid entitlements such as leave pay and payslips.

Although the court has yet to issue a decision, the case is nonetheless instructive in highlighting the compliance risks that litigation of this kind may raise. In particular, the claimants allege that data controllers are expected to provide employees with a privacy notice at the outset of the employment relationship. Such notice should clearly explain the purposes of data processing, including any use of financial or credit information, as well as the applicable legal basis. Regardless of the eventual outcome, the case underscores that internal HR data processing activities, especially credit or background checks on employees or job applicants, may give rise to civil liability lawsuits if they are not carried out in compliance with the PDP Law.

The case also illustrates that data related disputes may be pursued as general tort claims before the district courts, rather than being framed solely as contractual disputes.

Constitutional Court Decisions

Three constitutional challenges to the PDP Law were filed in 2025,[i] all of which were rejected by the Constitutional Court.

The first challenge concerned the cross-border data transfer framework under Article 56. The Court held that adequacy assessments fall within the Government's executive-administrative authority and that the tiered transfer framework under the PDP Law is constitutionally sound.

The second challenge targeted the criminal liability provisions under Articles 65(2) and 67(2). The Court found that journalistic, academic, and artistic activities are already protected through existing sectoral laws and PDP Law exemptions, making additional carve-outs unnecessary.

The third challenge addressed Article 20(2)(a) on explicit consent, proposing that consent should only be valid if provided through certified electronic signatures. The Court rejected this argument as legally unreasonable and

clarified that such technical requirements should be addressed through implementing regulations, not constitutional interpretation.

Three key points emerge from these decisions:

1. The PDP Law's cross-border transfer framework, covering adequacy, contractual safeguards, and consent, is now constitutionally settled, making further judicial challenge unlikely.

2. The PDP Law's criminal liability regime on unlawful disclosure remains intact without explicit industry-specific exemptions. The Court confirmed that the concept of "unlawful" disclosure must be interpreted in conjunction with other PDP Law provisions and relevant sectoral laws. As a result, activities such as journalism, academia, and arts continue to be protected under existing laws (for example, the Press Law), without the need for express exclusions under the PDP Law.

3. Finally, consent requirements remain subject to further elaboration through implementing regulations. The Government, acting through the DPA, retains discretion to introduce more detailed or technically specific rules on how consent must be recorded and evidenced.

Key Takeaways

The developments outlined in this update mark an important inflection point for data protection enforcement in Indonesia. The forthcoming establishment of the DPA will, for the first time, introduce the supervisory body responsible for overseeing compliance with, and imposing administrative sanctions under, the PDP Law.

In parallel, Indonesia's adequacy commitment under the Trade Agreement, once incorporated into domestic law, is expected to reshape how organisations manage cross-border data transfers, particularly those involving US-based counterparties. At the same time, the increasing number of criminal judgments and emerging civil claims demonstrates that data protection risk under the PDP Law is no longer theoretical.

In light of these developments, organisations should closely monitor and take steps in relation to the following:

1. The issuance of the Draft Regulation, including any implementing regulations governing enforcement procedures and administrative fine levels;

2. The ratification of the Trade Agreement, together with the adoption of any corresponding implementing regulations or adequacy-assessment measures; and

3. The strengthening of internal data protection governance, including:

    - Reviewing the lawful basis for each data processing activity;
    - Ensuring that each processing purpose is necessary and conforms with the organisation's actual business operations; and
    - Training and supervising personnel involved in data processing to ensure compliance with internal policies.

Taken together, these measures will assist organisations in preparing for an increasingly active and complex data protection regulatory environment in Indonesia.

[i] Constitutional Court Decisions No. 137/PUU-XXIII/2025; 135/PUU-XXIII/2025; and 284/PUU-XXIII/2025.

Contacts

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

Zacky Zainal Husein

PARTNER; HEAD

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 Contact Partners listed above, with the assistance of **Daniar Supriyadi** (Associate, Assegaf Hamzah & Partners) and **Ryan Armandha Andri Anwar** (Associate, Assegaf Hamzah & Partners).

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
F +856 21 285 261
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
F +66 2656 0833
th.rajahtannasia.com

Vietnam
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382
F +84 28 3520 8206

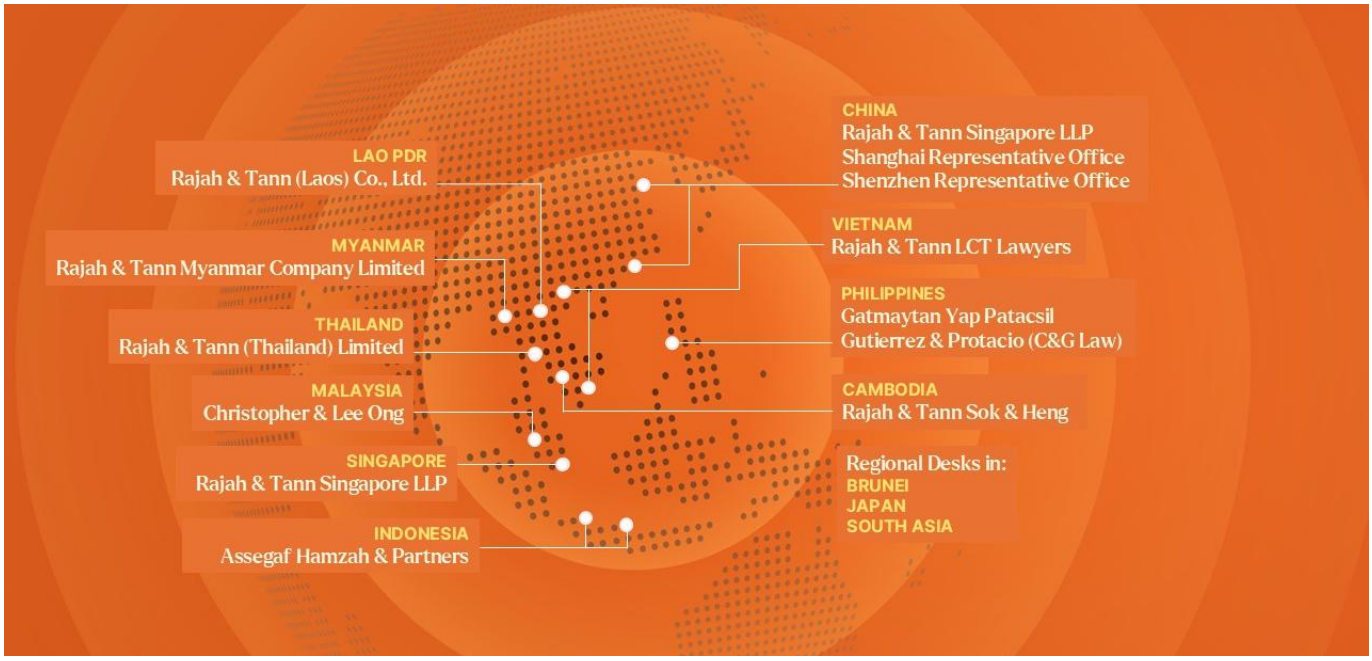
Hanoi Office
T +84 24 3267 6127 | +84 24 3267 6128
vn.rajahtannasia.com

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 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.