NO. 2025-11, OCTOBER 2025
ISSN: 2086-8154

Economic Research Institute for ASEAN and East Asia

Policy Brief

Between Trade and Trust: Rethinking Indonesia–US Cross-Border Personal Data Transfer

Fikri Adib Rianto

Indonesia's recent decision to recognise the United States as an adequate jurisdiction for personal data protection – made under a new bilateral trade deal – permits the transfer of Indonesian personal data to US private entities without additional safeguards. This move, taken before Indonesia's Personal Data Protection Authority (PDPA) is established and before adequacy criteria are formally defined, raises concerns over legal legitimacy and data governance. Given persistent systemic risks in the US – ranging from corporate misuse and cybersecurity vulnerabilities to expansive surveillance powers and fragmented privacy laws – the decision appears premature. To safeguard privacy while supporting trade interests, Indonesia should complete its domestic data protection framework, clarify adequacy criteria, and temporarily recalibrate its adequacy determination until more robust bilateral governance mechanisms are in place.

Key Messages:

- Indonesia's adequacy decision for the United States was premature, given incomplete domestic legal and institutional frameworks.
- Systemic risks in the US – such as commercial exploitation, cybercrime, government surveillance, and fragmented laws – pose threats to Indonesian privacy rights.
- The Indonesian government should expedite implementing regulations for the PDP Law, operationalise the Personal Data Protection Authority, and establish transparent adequacy criteria.
- In the short term, adequacy recognition should be paused, relying instead on binding contractual mechanisms such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs).
- In the long term, Indonesia should pursue a reciprocal, enforceable, and federally consistent privacy framework with the United States.

Fikri Adib Rianto
Research Associate, ERIA

Background

In July 2025, Indonesia and the United States concluded a trade arrangement that aimed to liberalise both tariff and non-tariff barriers, providing reciprocal access to each other's markets (The White House, 2025). A notable provision was Indonesia's recognition of the United States as an 'adequate' jurisdiction for data protection, thereby allowing US private firms – spanning cloud services, e-commerce, social media, research, and digital innovation – to transfer Indonesian personal data out of its territory without additional legal safeguards.

While this development signals Indonesia's openness to digital trade and regulatory alignment with key partners, it also raises governance and sovereignty questions. The adequacy recognition effectively allows cross-border personal data transfers even though Indonesia's domestic data protection regime remains incomplete and its oversight authority non-operational.

Indonesia's Impetuous Decision

US technology companies have long voiced frustration over Indonesia's regulatory ambiguity regarding cross-border data transfers. Government Regulation No. 71/2019 created uncertainty

about whether private electronic system operators must maintain local data centres, while Ministerial Regulation No. 20/2016 imposed burdensome procedural requirements for offshore personal data transfers, including data subject consent and detailed reporting obligations (Chow, Sakurayuki, and Cognard, 2021).

Law No. 27/2022 on Personal Data Protection (PDP Law) sought to modernise this system. Article 56 introduced three legal bases for international personal data transfer: (i) an adequacy decision, (ii) the use of binding legal instruments (such as SCCs or BCRs), or (iii) explicit data subject consent. However, as of October 2025, implementing regulations for technical procedures and the establishment of the Personal Data Protection Authority (PDPA) – the agency mandated to determine criteria, evaluate, monitor, and enforce adequacy – remain under ministerial harmonisation.

Without an operational PDPA or published adequacy criteria, Indonesia's decision to recognise US adequacy appears **legally premature and procedurally weak.** What US firms sought was legal clarity under the new PDP Law, not an adequacy shortcut. The move thus risks undermining Indonesia's own institutional development by prioritising short-term trade convenience over the long-term consolidation of digital sovereignty and regulatory credibility.

Systemic Risks and Regulatory Gaps in the United States

Recognising US adequacy without due diligence exposes Indonesian citizens' personal data to significant risks. Large-scale offshore data concentration creates opportunities for commercial exploitation – through targeted advertising, political profiling, and unauthorised use in artificial intelligence training. Cases such as Twitter's misuse of security data, the Facebook–Cambridge Analytica scandal, and Adobe's AI training controversy illustrate persistent gaps in US data governance.

Beyond private misuse, **external and institutional risks** remain substantial. The United States consistently ranks amongst the top global sources of cybercrime activity, accounting for one of the highest volumes and costs of data breaches globally (Bruce et al., 2024). Compounding this vulnerability, data held by US entities is subject to expansive surveillance powers under the **Foreign Intelligence Surveillance Act (FISA) Section 702, Executive Order 12333**, and **Presidential Policy Directive 28**. These allow intelligence agencies to access non-US citizens' data regardless of where it is stored. Although Executive Order 14086 introduces 'necessity' and 'proportionality' principles, their interpretation remains broad and discretionary.

Equally concerning is the **fragmented nature of the US privacy regime**. Unlike the European Union, the United States lacks a comprehensive federal privacy law, relying instead on a patchwork of sectoral statutes – such as HIPAA (healthcare), GLBA and FCRA (financial services), COPPA (children's data), and FERPA (education) – each with differing enforcement standards (Kirvan, 2024). At the state level, only 24 of 50 states have enacted or drafted comprehensive privacy laws, while major data-centre hubs such as Illinois, Ohio, Georgia, Arizona, New York, and Washington remain unregulated (Kibby, 2025). This uneven landscape undermines predictability, leaving Indonesian data subject to inconsistent standards of consent, rights, and oversight.

Lessons from the European Union

The European Union offers a more balanced model for managing cross-border personal data transfers. It grants adequacy status only when the recipient country ensures a **reciprocal, enforceable, and comprehensive** data protection framework. The EU–US **Data Privacy Framework (DPF)**, introduced in 2023, exemplifies this approach. Under the DPF, the US Department of Commerce manages a self-certification system, with compliance enforced by the Federal Trade Commission and monitored through an independent redress mechanism – the **Data Protection Review Court.**

The EU retains the authority to suspend or revoke adequacy status if US authorities breach agreed standards. This arrangement replaced the earlier **EU–US Privacy Shield**, which the Court of Justice of the European Union invalidated in the **Schrems II** decision due to excessive US surveillance and lack of effective legal redress.

Indonesia could draw valuable lessons from this cautious, reciprocity-based approach. The EU model demonstrates that **functional adequacy** – balancing trade facilitation with strong governance – is possible when supported by clear institutional mandates, transparent criteria, and mechanisms for periodic review. In contrast, Indonesia's unilateral adequacy recognition of the US, without a competent authority or legal safeguards, risks undermining trust in its nascent data protection regime.

Policy Recommendations

1. Accelerate the Domestic Regulatory Framework

Indonesia should immediately finalise implementing regulations of the PDP Law and operationalise the Personal Data Protection Authority (PDPA). The PDPA should have a clear mandate to:

- define adequacy assessment criteria and procedures;
- evaluate countries' eligibility for adequacy determination;
- conduct periodic reviews of partner countries' compliance; and
- manage international enforcement and dispute resolution with foreign regulators.

A well-defined domestic regulatory base would strengthen Indonesia's credibility and negotiating leverage in international data governance.

2. Recalibrate the Adequacy Decision for the United States

Given persistent risks in US data governance, Indonesia should **reconsider and temporarily suspend** its adequacy decision. During the interim, personal data transfers between Indonesia and the US should rely on **Standard Contractual Clauses (SCCs)** or **Binding Corporate Rules (BCRs)**, consistent with international best practice.

In the longer term, negotiations with the United States should aim for a **reciprocal, enforceable, and federally consistent** privacy framework, akin to the EU–US Data Privacy Framework, before reinstating adequacy recognition.

3. Embed Digital Sovereignty in Trade Negotiations

Future trade agreements should incorporate **privacy and data protection clauses** that align with Indonesia's national interests and constitutional right to privacy. Data-related provisions must be negotiated jointly with the PDPA and relevant ministries to ensure consistency with domestic law. Such alignment will reinforce Indonesia's strategic position as both a digital trade partner and a defender of individual privacy rights.

4. Strengthen Regional Cooperation on Cross-Border Data Flows

Indonesia should actively promote ASEAN-wide coordination on adequacy and interoperability frameworks. Leveraging ASEAN's Model Contractual Clauses and the Digital Economy Framework Agreement (DEFA), the region can establish consistent compliance standards and bridge legal differences for cross-border personal data transfers with trading partners.

Conclusion

Indonesia's recognition of the United States as an adequate jurisdiction for personal data transfer represents a bold yet risky experiment in digital trade policy. While the decision may reduce short-term uncertainty for US firms, it exposes Indonesia to governance risks that could weaken public trust and institutional coherence.

To reconcile trade facilitation with data protection, Indonesia must first **build its domestic foundation** – through the operationalisation of the PDPA, the clarification of adequacy criteria, and the strengthening of cross-border regulatory capacity. Only after establishing these pillars should Indonesia revisit adequacy recognition and engage the United States in negotiating a reciprocal, enforceable, and transparent data governance framework.

Such an approach would affirm Indonesia's dual ambition: to be a **trusted digital trade partner** and a **sovereign guardian of data privacy** in the evolving global digital economy.

References

Bruce, M. et al. (2024), 'Mapping the Global Geography of Cybercrime with the World Cybercrime Index,' *PLOS ONE*, 19(4): e0297312. https://doi.org/10.1371/journal.pone.0297312

Chow, P., Sakurayuki, and C. Cognard (2021), 'Cross-Border Data Transfers – An Indonesian Law Update.' *Herbert Smith Freehills Kramer*. https://www.hsfkramer.com/notes/indonesia/2021-05/cross-border-data-transfers-an-indonesian-law-update

Kibby, C. (2025), 'US State Privacy Legislation Tracker,' *International Association of Privacy Professionals (IAPP)*, 7 July. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

Kirvan, P. (2024), 'US Data Privacy Protection Laws: 2025 Guide,' *Search Security*. https://www.techtarget.com/searchsecurity/tip/State-of-data-privacy-laws

The White House (2025), *Fact Sheet: The United States and Indonesia Reach Historic Trade Deal*. https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-the-united-states-and-indonesia-reach-historic-trade-deal/

Sentral Senayan II, 5th, 6th, 15th floors
Jalan Asia Afrika No. 8
Senayan, Central Jakarta 10270, Indonesia
Tel: (62-21) 57974460
E-mail: contactus@eria.org