Policy Note

Indonesia's Strategy for Safeguarding Cross-Border Personal Data Transfers to the United States Without Compromising Digital Sovereignty or Personal Data Protection

Policy Dialogue on Data Governance in Indonesia

Jakarta, 28 October 2025

Context

Indonesia is entering a critical phase in defining how data moves across borders while protecting national interests and individual rights. As digital trade grows, cross-border data transfers are becoming integral to economic cooperation, particularly with partners like the United States.

To address this, LIRNEasia convened a Closed-Door Policy Dialogue in Jakarta, in collaboration with Northbound Strategies and supported by IDRC Canada. The session brought together policymakers, regulators, researchers, private sector leaders, and academics to explore Indonesia's readiness to enable personal data transfers under the Personal Data Protection Law (PDP Law) while safeguarding digital sovereignty and public trust.

Key Insights

Balancing Access, Innovation, and Protection

Discussions underscored that data governance is both a democratic and economic issue. The forum agreed that there is no universal model for data governance; while the EU's GDPR offers lessons, developing economies like Indonesia cannot apply it wholesale due to differing institutional capacity and compliance mechanisms. The key is to forge a proportionate approach that maintains interoperability for innovation while ensuring adequate safeguards.

Participants emphasized that digital sovereignty is not about isolation, but about a nation's ability to engage globally while upholding its principles. They argued that data localization alone does not guarantee security and can create a false sense of protection without robust oversight.

Regulatory Framework and Implementation Gaps

Indonesia's current framework, anchored in the Constitution and key laws on public information disclosure, personal data protection, and electronic governance, provides a solid legal foundation. However, repeated incidents of data breaches highlight ongoing challenges in enforcement and institutional coordination.

Participants emphasized that adequate personal data protection requires not only regulation but also operational capacity, clarity of mandates across agencies, and consistent implementation. Strengthening governance structures and improving cross-agency collaboration are essential steps toward translating policy into practice.

Cross-Border Data Flow: Opportunity and Complexity

Participants recognized cross-border data flows as both a driver of economic growth and a complex governance issue. They highlighted the significant contribution of data flows to global trade and innovation, but also noted the need for trust-based safeguards to ensure accountability across jurisdictions.

Indonesia's approach, guided by the principle of "Data Free Flow with Trust", seeks to balance these interests through a tiered adequacy framework that considers the level of protection in destination countries, the use of binding contractual safeguards, and explicit consent where necessary.

The United States, while a critical digital and economic partner, does not yet fall under an automatic adequacy designation. Future arrangements depend on

demonstrable accountability, independent redress mechanisms, and guarantees of proportional access to data by public authorities.

Trust and Accountability as Foundations of Digital Sovereignty

A recurring theme was that digital sovereignty should reflect a nation's ability to engage globally while upholding its principles of transparency, fairness, and protection. Participants argued that excessive reliance on data localization can create a false sense of security and even expand vulnerabilities if not supported by robust oversight. True digital sovereignty lies in designing governance systems that enable trusted international cooperation while ensuring domestic accountability.

Industry Perspective: Security Through Interoperability

From a private-sector perspective, participants noted that predictable, interoperable data rules are essential to investment and innovation. Overly restrictive or fragmented regimes can raise costs, particularly for small and medium enterprises, and reduce competitiveness in the region.

Experts highlighted that localization does not automatically ensure better security. A risk-based, interoperable approach, supported by strong encryption, tokenization, and AI-driven cybersecurity, is a more effective model for balancing security, compliance, and innovation.

Building Trusted Cross-Border Systems

Discussions also highlighted the need to build trust-based cross-border systems through regional and global cooperation. This approach of cooperation includes developing interoperable standards, pilot frameworks, and certification mechanisms that align with international principles such as the Data Free Flow with Trust (DFFT) and the ASEAN Digital Economy Framework Agreement (DEFA).

Rather than choosing between digital sovereignty and openness, Indonesia was encouraged to position itself as a regional leader in setting trusted data standards that support both protection and competitiveness.

Policy Coherence and Evidence-Based Cooperation

The forum emphasized that coherence across policies and evidence-based design is central to effective governance. International cooperation on personal data protection should focus on process-oriented standards that promote accountability and fairness, rather than rigid product-based requirements that may reinforce vested interests.

Participants also noted that localization without adequate oversight can paradoxically increase exposure by granting multiple authorities access to data without improving protection. Effective regulation, therefore, depends less on where data is stored and more on how the government, as the key stakeholder, governs it.

Policy Directions

Moving forward, Indonesia's cross-border data strategy should emphasize:

- Risk-based regulation rather than blanket restrictions.
- Mutual recognition and cooperative oversight between personal data protection authorities.
- Stronger institutional coordination and clear enforcement responsibilities.
- Evidence-based policymaking, drawing from comparative research and global best practices.
- Inclusive governance, ensuring active participation from government, industry, civil society, and academia.

Conclusion

The policy dialogue reaffirmed that Indonesia's pursuit of digital sovereignty and openness are not conflicting goals but complementary ambitions. Digital sovereignty in the digital era lies in a country's ability to define the terms of openness, to engage globally on its own principles of trust, accountability, and fairness.

By investing in institutional capacity, promoting transparency, and engaging in international cooperation, Indonesia is well-positioned to shape a trusted, sovereign, and globally connected digital future.

*****

PT Jejak Suar Nusantara
Menara BP Jamsostek, North Tower, Jl. Gatot Subroto No.38 Floor 10th, Unit 04, Jakarta Selatan, Daerah Khusus Ibukota Jakarta, 12710

Let's decode Indonesia together!
contact us at decode@northbound.co.id | 0811 265 7167
https://northbound.co.id