E-ISSN: 2963-4946
Vol. 3 No. 12 September, 2025
Asian Journal of Social and Humanities
https://ajosh.org/

Policy Capacity of the Indonesian Government in Implementing Cross-Border Data Transfer Within Trade Agreements with the United States

Yuli Anitasari*, Agung Firman Sampurna
Universitas Indonesia
Email: yuli.anitasari@gmail.com*

Keywords:
data transfer, digital sovereignty, public policy, digital economy liberalization, policy capacity.

ABSTRACT

The development of the global digital economy has encouraged the emergence of digital sovereignty issues, especially related to cross-border data transfer. In this context, the trade agreement between Indonesia and the United States announced in July 2025 includes Indonesia's commitment to open access to data transfer abroad. This commitment has strategic implications for national data governance and the protection of citizens' digital rights. This study aims to analyze Indonesia's readiness to implement these commitments using the policy capacity framework, which includes the government's technical, administrative, and political capacity. This study found significant limitations in all three dimensions of capacity, ranging from surveillance infrastructure to cross-agency coordination and political legitimacy. The analysis confirms the need for structured measures to strengthen institutions, procedures, and oversight so that the liberalization of data transfers does not come at the expense of digital sovereignty. This article contributes to the digital public policy literature by showing the application of the policy capacity framework in the issue of cross-border data transfer, which has been studied more from legal and economic perspectives.

INTRODUCTION

The development of the global digital economy places data as a strategic asset that determines the country's bargaining position in international trade. The issue of cross-border data transfer is not only related to the technical aspects of the digital economy but also concerns digital sovereignty and the protection of citizens' rights. Thus, cross-border data transfer is not only a technical issue of trade, but also a public policy that offends the country's capacity to maintain digital sovereignty (Treré, 2019)

In the context of Indonesia, this dynamic is increasingly emerging after the trade deal with the United States in July 2025. The agreement lowers import tariffs but is accompanied by Indonesia's commitment to open up the flow of personal data transfers to the US. This raises a debate considering that Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) stipulates that data transfer can only be carried out if the destination country has equivalent or higher protection standards.

The United States itself does not have comprehensive federal laws on privacy, but rather sectoral and fragmented regulations. This condition raises potential tensions between international trade commitments and the national legal framework. Therefore, the issue of cross-border data transfer cannot be seen as just a technical issue of trade, but also as a public policy issue that touches the capacity of the state to maintain digital sovereignty. (Milan & Treré, 2019)

Thus, an analysis based on a policy capacity framework that includes the government's technical, administrative, and political capacity is needed to assess Indonesia's readiness to implement data transfer commitments without sacrificing the protection of citizens' digital rights.

Although the literature on cross-border data flows has highlighted the economic consequences and global governance dimensions, two key studies leave a gap in understanding domestic policy capacity—particularly in Indonesia. Aaronson (2018) demonstrated how trade regimes created "three data realms" (United States, European Union, China) with conflicting approaches to data protection, generating tensions between trade commitments and data sovereignty. However, this study stops at the global architecture level and does not detail how domestic institutional readiness—such as surveillance capabilities, data protection agency design, and political legitimacy—shapes the implementation of cross-border commitments. In contrast, Ferracane and van der Marel (2018/2021) empirically showed that restrictive data policies negatively affect digital services trade and distinguished between policies regulating cross-border flows versus domestic use. Yet, their quantitative focus did not operationalize the technical–administrative capacities needed for adequacy assessments, compliance management, and inter-ministerial coordination when a country opens data flows to jurisdictions like the U.S., which lacks a comprehensive federal privacy law.

Different from studies that generally highlight purely legal or economic aspects. The purpose is to evaluate Indonesia's readiness so that data liberalization does not undermine digital sovereignty and citizens' rights, while the benefit is providing a policy roadmap grounded in capacity that policymakers can directly adopt to align trade commitments with personal data protection. Moreover, this study offers two main contributions. First, operationalizing the policy capacity framework into measurable indicators for Indonesia-United States data transfer cases. Second, translating the findings into implementable recommendations in the form of a draft adequacy assessment methodology, BPDP institutional design, and a cross-ministry or agency coordination scheme through an implementing arrangement that can be implemented immediately.

RESEARCH METHOD

This study used a qualitative approach with a policy study method, as the issue of cross-border data transfer required regulatory, institutional, and political understanding. Data were obtained from national regulations, international documents (including the Indonesia-US agreement of July 2025), academic publications, official reports, and reliable media sources to capture recent developments. Data collection involved documentation, literature review, and source triangulation. Data analysis was conducted using Content Analysis based on the policy capacity framework (Wu, 2015), which includes three main dimensions: technical capacity (indicators: guideline adequacy assessment, supervisory tools, data transfer guidelines), administrative capacity (indicators: supervisory authority, enforcement by supervisory authority, bureaucratic coordination), and political capacity (indicators: political support, public participation, and interest coalition).

RESULTS AND DISCUSSION

The concept of digital sovereignty refers to a country's ability to regulate the data of its citizens, including the storage, processing, and transfer of data outside of national jurisdiction. In this context, cross-border data transfer tests the boundaries between economic openness and state protection of strategic digital assets. Public policy literature emphasizes the importance of policy capacity analysis to measure the ability of states to implement strategic decisions. Skeleton (Arne Hintz, 2019) (Bigo, 2019) (M. Howlett, 2016)*policy capacity* divides this capacity into three dimensions: (1) technical capacity related to the availability of guidelines *adequacy assessment*, monitoring tools, data transfer guidelines for implementing policies; (2) administrative capacity, related to the authority of the supervisory authority, enforcement by the supervisory authority, cross-agency bureaucratic coordination; and (3) political capacity,

namely political support, public participation, and interest coalitions to maintain policy implementation. (Wu, 2015)

Conformity between International Agreements and Domestic Regulations
American Trade Policy

The development of information and communication technology has revolutionized the way countries interact in international trade. Data is now a strategic resource that determines a country's bargaining position in the digital economy. Cross-border data flow (Ncheke, 2020)Cross-border data flow) plays a critical role in supporting innovation, efficiency, and digital business expansion. However, this also poses a major challenge for digital sovereignty, especially in developing countries such as Indonesia. In this context, the United States has consistently encouraged the inclusion of data transfer clauses in every trade deal. The United States' push to include cross-border data transfer clauses in digital trade agreements is in line with global trends that emphasize the need for digital trade governance at both the multilateral and bilateral levels. This approach reflects the importance of the U.S. digital economy that rests on global technology companies. Trade agreements that include commitments to liberalize cross-border data transfers have strategic implications for national data governance and digital trade regulation (Ying Chen, 2022) (Aaronson, 2018)

The United States did the same thing to Indonesia in a trade deal agreed at the end of July 2025. As part of its efforts to protect its digital economy interests, major American tech companies such as Google, Meta, and Amazon rely heavily on cross-border access to user data to support business models based on cloud computing, behavioral analytics, and global digital advertising services. By making the freedom of data flow an issue of trade negotiations, the United States seeks to avoid regulatory barriers such as data localization policies and ensure that partner jurisdictions do not restrict the flow of data to servers located in the jurisdiction of the United States. This data transfer is becoming an important instrument to support business models based on cloud computing, user behavior analytics, as well as the development of artificial intelligence and global digital advertising services. In addition, by acknowledging that the United States has "adequate" data protection standards, the U.S. government seeks to establish legitimacy over its own data protection system, without having to submit to stricter standards such as the European Union's General Data Protection Regulation (GDPR). (UNCDF, 2021) (Leblond, 2024)(DCO, 2023)

The United States' push for Indonesia to open up the flow of cross-border personal data transfers has been going on since at least 2022, when Indonesia joined the US-initiated Indo-Pacific Economic Framework (IPEF). In the IPEF trade pillar, the U.S. actively campaigned for the removal of barriers to cross-border data flows and rejected data localization policies. These efforts will intensify in 2023 through bilateral dialogue, where the United States expressed its concerns over Indonesian regulations, especially after the passage of the (PDP Law) which is considered to have the potential to limit data transfers. The pressure continues in various international forums in 2024 and reaches a peak in 2025 when the issue of data transfer is made part of strategic negotiations within the framework of a reciprocal tariff policy. Thus, the liberalization of data flows must be supported by technical and institutional signs to be in line with the PDP Law. (Chen, 2022) (Council, 2022) (Executive Order, 2025)

Data Protection Provisions in Indonesia

Article 56 of the PDP Law explicitly stipulates that the transfer of personal data abroad can only be carried out if the destination country has a level of data protection equal to or higher than the provisions of the Law, or based on international agreements, or on the basis of the consent of the data subject. The law also establishes basic principles of data protection such as explicit consent, transparency, purpose limitation, accuracy, integrity, and accountability.

In addition, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP 71/2019), as an umbrella for technical regulations before the birth of the PDP Law, still applies to the control of electronic systems and the obligation to store strategic data in Indonesian territory for the public sector and certain in the private sector. This PP also requires that electronic system operators must ensure the security and confidentiality of data in their processing and storage.

Until now, the implementing regulations of the PDP Law are still in the drafting stage, including more detailed provisions regarding the mechanism for assessing the equivalence of foreign data protection levels (data adequacy), supervision procedures by supervisory authorities (Personal Data Supervisory Agency/BPDP), as well as procedures for submitting and approving cross-border data transfers. The absence of these derivative rules has led to a lack of technical clarity on how international commitments such as those in the Indonesia-United States agreement can be implemented without causing conflict with applicable national law. In practice, trade agreements tend not to concretely detail the equal protection mechanism, thus opening up room for legal uncertainty in the implementation of personal data transfers abroad. (Jakob Edler, 2023) (Costa, 2025) (Kristina Irion, 2021)

Data Protection in the United States

Unlike Indonesia, which already has a single national legal framework through the PDP Law, the personal data protection system in the United States has not been regulated through a comprehensive federal law (Comprehensive). Instead, the United States applies a sectoral approach and fragmented, which means that data protection regulations are structured based on specific sectors or types of data. Some of the sectoral laws that have been issued in the United States include the Health Insurance Portability and Accountability Act (HIPAA) which was issued during the era of President Bill Clinton in 1996. Furthermore, in the consumer data sector of the financial sector, there is the Gramm Leach Bliley Act or also known as the Financial Services Modernization Act, which regulates the obligation of financial institutions to explain how financial institutions publish or protect data (Rubinstein, 2010)(GLBA)Customer-his. As for the data protection sector of children under the age of 13, there is the Children's Online Privacy Protection Act (COPPA) which requires site operators Web and online services aimed at children under the age of 13 to meet certain conditions regarding the collection, use, and disclosure of children's personal information.

In addition to sectoral regulations, several states in the U.S. have adopted more comprehensive personal data protection laws, such as the California Privacy Rights Act (CPRA) which provides access, erasure, and opt-out rights against the sale of personal data, including several laws published in other states such as the Virginia Consumer Data Protection Act (VCDPA), Colorado Privacy Act, Connecticut Data Privacy Act (CTDPA), and the Utah Consumer Privacy Act (UCPA).

The sectoral approach to personal data protection in the United States reflects a public policy tradition that emphasizes deregulation, market freedom, and the protection of free speech. Privacy regulation in the U.S. evolved in response to sectoral scandals, rather than on the principle of privacy as a human right as in Europe. Institutional fragmentation and ideological differences in Congress, between Democrats who support strict regulation and Republicans who oppose overregulation, hinder the birth of comprehensive federal privacy laws. In addition, the dominance of states in regulating consumer protection reinforces the pattern of policy decentralization, which further distances the United States from a centralized data protection model. (Reuters, 2016)

Approach fragmented in the protection of personal data in the United States has serious consequences in the context of international cooperation, particularly regarding the recognition of data protection standards by other countries. The absence of comprehensive federal

legislation makes it difficult to consider data protection standards in the United States (Adequate) by countries with stricter legal regimes, such as the European Union and Indonesia. This creates uncertainty for trading partners who are subject to human rights-based data protection principles, due to the lack of guarantees of consistent treatment of their citizens' data in United States jurisdictions. In addition, the broad access of U.S. intelligence agencies to digital data under the Foreign Intelligence Surveillance Act (FISA), in particular (Avram, 2023)Section 702, reinforcing concerns that alien data transferred to the United States could be leveraged without adequate controls or protections. In situations like this, the differences in legal systems between partner countries and the United States are not only a technical issue, but also concern public trust, policy legitimacy, and cross-border protection of digital rights.(Lantz, 2016)

Comparison in Other Countries

The European Union regulates cross-border transfers of personal data through a strict legal framework under the General Data Protection Regulation (GDPR). Instead of incorporating data transfer clauses into free trade agreements (FTAs), the European Union has consistently separated trade affairs from personal data protection. The transfer of data from EU member states to third countries can only be carried out if the destination country has been recognised to have a high level of data protection "(Union, 2016)Adequate" through the mechanism adequacy decision issued by the European Commission. In the case of the United States, after the cancellation of the mechanism (Macievic, 2024)Privacy Shield by the Court of Justice of the European Union in 2020, the EU and the US negotiated the EU–US Data Privacy Framework, which is voluntary and only applies to American companies that are explicitly certified and subject to data protection obligations as per EU standards. In this way, the EU remains open to data flows to support the digital economy, but still maintains regulatory sovereignty and its citizens' fundamental right to privacy.(European Commission, 2023)

Indonesia's case is not the only example of developing countries facing pressure from the United States on the issue of cross-border data transfers. India and Brazil show similar dynamics, albeit with different policy strategies.

India has been debating the Personal Data Protection Bill (PDPB) since 2018 which emphasizes data localization policies as a form of digital sovereignty. Pressure has come from U.S. tech companies that see the rules as barriers to trade. However, India chose a strategy of resistance by postponing the final discussion of the law and maintaining the narrative that citizen data is "Public Good" which must be protected from the domination of foreign companies. (Rajmohan, 2025)

Meanwhile, Brazil, through the 2020 Lei Geral de Proteção de Dados (LGPD), established a legal framework that is relatively closer to the European GDPR model. U.S. pressure also emerged, but Brazil strengthened the National Data Protection Authority (ANPD) as an independent regulator with full authority. This gives Brazil a stronger bargaining position in trade negotiations while maintaining consistency with international standards. (Erickson, 2019) (JonesDay)

Both cases show that the state's strategy in dealing with data liberalization pressures is greatly influenced by domestic institutional and political capacity. Compared to Indonesia, India is more protective, while Brazil is more cooperative by strengthening supervisory institutions.

Government Policy Capacity in Implementing Trade Commitments

From the perspective of international commitment, our government is bound to be able to implement the results of the agreement that has been made with the American Government. To be able to predict the success or failure of our government in fulfilling the agreement, it can

be seen from the perspective of policy capacity theory. The policy capacity framework divides policy capacity into three main dimensions. First, technical capacity, namely the ability of policy actors to provide adequacy assessment guidelines, monitoring tools, and data transfer guidelines needed in policy formulation and implementation. Second, administrative capacity, which refers to the authority of the bureaucracy and state institutions in coordinating programs, ensuring regulatory compliance at the implementation level, and bureaucratic coordination across agencies. Third, political capacity, namely the ability of the government and policy actors to build legitimacy, gain political support, and form coalitions, including through public participation, is necessary for policies to survive amid interest dynamics. These three dimensions are interrelated and together determine the extent to which public policy can be implemented effectively. The successful implementation of the post-July 2025 cross-border data transfer commitment is highly dependent on the Government's policy capacity to implement the policy. Therefore, the following discussion outlines the main findings and strategic steps needed on each of these capacity dimensions.

Technical Capacity

The implementation of data transfer requires technical competence both in terms of supervision mechanisms and adequate infrastructure, for example an integrated cross-border surveillance system. Monitoring the implementation of data transfer requires an assessment of the adequacy of data protection ((Zhixian Zhuang, 2024)adequacy assessment). This assessment determines whether a country or jurisdiction has an equal or higher level of personal data protection than the country sending the data. Article 56 of the PDP Law has regulated normatively the principle of adequacy assessment. The article stipulates that the transfer of personal data abroad may only be carried out if the destination country has an equivalent or higher level of data protection. However, until now the implementation regulations of the PDP Law that are mandated to regulate the methods and procedures do not exist. The absence of these technical guidelines creates a gap in the implementation of the PDP Law, as well as an obstacle for supervisory authorities to conduct assessments consistently and based on global standards.

The adequacy assessment mechanism serves as a legal prerequisite for secure cross-border data transfers, thereby preventing privacy violations or misuse of data in destination countries. One of the adequacy assessment concepts that can be referenced is the adequacy decision framework regulated in Article 45 of the European Union's General Data Protection Regulation (GDPR). The adequacy assessment process is carried out by the European Commission based on a series of criteria, including an assessment of the principles and rights of data protection regulated in the laws of the destination country, the existence of an independent supervisory authority that has effective authority in law enforcement, the availability of international commitments and the participation of the destination country in multilateral agreements relevant to data protection, including the law enforcement mechanisms that are relevant to data protection. provide a path of redress for the data subject. Based on these criteria, the European Commission has determined several countries with adequacy status from the European Union, including Japan, South Korea, Canada, and the United Kingdom. This process typically involves comprehensive evaluation, public consultation, and periodic monitoring to ensure that standards are maintained. To be able to carry out adequacy assessment, integrated cross-border supervision is a technical competence that Indonesia needs to have.

From an infrastructure perspective, Indonesia does not yet have an integrated cross-border surveillance system, such as Real-time data flow monitoring, Compliance Dashboard, or the mechanism Data Flow Mapping which allows for technical tracking of data flows. In comparison, the European Union through the European Data Protection Board (EDPB) has

developed the European Data Protection Authorities Network framework that facilitates the exchange of information in a timely manner. Real-time Anthrariality, including Early Warning System for potential cross-border violations and Data Breach Notification Platform that are directly connected to Compliance Dashboard in each member state. On the other hand, Singapore through the Personal Data Protection Commission (PDPC) uses (Board, 2023)Data Protection Trustmark and Automated Compliance Monitoring Tools to ensure business actors' compliance with data transfer standards, which are integrated with Incident Response System national. In addition, formal channels for information exchange and law enforcement coordination with other countries' authorities. for example, through Mutual Legal Assistance or Data Protection Cooperation Agreement, it is not yet available systematically.(Singapore, n.d.)

Domestically, the government also needs to issue guidelines for cross-border data transfer that are operational in nature as an auditable reference for actors and officials. These guidelines ensure consistency in the implementation of the PDP Law, provide certainty for perpetrators, and strengthen measurable enforcement and are in line with international schemes without lowering domestic protection standards

To deal with the pressure of liberalizing data transfer in trade agreements, as happened in the 2025 Indonesia-United States agreement, Indonesia still needs to ensure that its implementation does not conflict with the PDP Law. The preparation of a follow-up agreement document that regulates the technical aspects of the implementation of data exchange is a prerequisite for the technical infrastructure that must exist. One solution that can be applied is to negotiate a derivative agreement in the form of an implementing arrangement or Memorandum of Understanding (MoU) that technically regulates the parameters for the implementation of data transfer. In the derivative agreement, Indonesia can require that only American companies that are willing to comply with the equivalent data protection standards of the PDP Act are allowed to receive personal data from Indonesia. For example, Indonesia could establish a certification mechanism like the Data Privacy Framework between the European Union and the United States, which requires voluntary compliance with certain protection standards.

Administrative Capacity

The implementation of the post-July 2025 data transfer commitment requires an adequate monitoring system. For this reason, the role of an independent supervisory authority is needed that reflects the administrative capacity of the Government of Indonesia in carrying out its commitments. The position of this supervisory authority is crucial in ensuring the effectiveness of the implementation of personal data protection policies, both at the national level and in the context of international cooperation. As a regulatory body, this authority is responsible for ensuring that the basic principles of data protection, such as transparency, explicit consent, restriction of purpose and accountability, are enforced by all controllers and data processors, both in the public and private sectors. Institutional independence provides legitimacy and neutrality in the law enforcement process, while avoiding conflicts of interest that may arise if oversight is under executive or industry control. In addition to being a regulator, this authority is also an official representative in international forums and plays a strategic role in the recognition of the principle of adequacy between countries. In practice, the existence of a credible supervisory authority is one of the main prerequisites for international recognition of a country's data protection system.

In Indonesia, the Personal Data Supervisory Agency (BPDP) mandated by the PDP Law has a central role in maintaining a balance between economic interests and the protection of citizens' fundamental rights. As an independent authority, BPDP is tasked with evaluating data transfer requests to other countries based on the principle of equality or adequacy of protection.

The agency is expected to be able to conduct an objective assessment of the level of data protection in partner countries, including the United States, which to date do not have comprehensive federal privacy laws.

More than just an administrative licensor, BPDP plays the role of a digital sovereignty guardian who must ensure that no data transfer practices endanger the country's privacy, national security, or strategic interests. The authority also needs to cooperate with supervisory authorities in other countries, follow developments in international standards, and issue guidelines or decisions that are binding on the public and private sectors. In cases such as the Indonesia-US trade agreement, BPDP has the authority to assess whether the provisions in the derivative agreement are adequate in ensuring the protection of Indonesian users' data. If a discrepancy is found, BPDP may postpone or reject the implementation of data transfer until the destination country meets the criteria set by the PDP Law and its implementing rules. Therefore, the independence, institutional capacity, and legal legitimacy of this authority are key in ensuring that the liberalization of digital trade does not sacrifice the data rights of Indonesian citizens. (Roberto Baldoni, 2025)

Although the PDP Law has mandated the establishment of the BPDP, the absence of this institution has created a vacuum in the functions of supervision, complaint processing, and the mechanism for assessing the equivalence of foreign data protection. Without an independent and capable institution, the effectiveness of national regulations and Indonesia's credibility in cross-border cooperation will be difficult to realize optimally. (Huw Roberts, 2021) (Voss, 2020)

By comparison, the European Union has long implemented a strong and independent data surveillance system through authorities such as the European Data Protection Board (EDPB) and European Data Protection Supervisors (EDPS), as well as Data Protection Authorities (DPAs) in each member state. These authorities not only carry out supervisory and law enforcement functions but are also involved in decision-making mechanisms such as the European Commission's Adequacy Decisions, which is an official assessment of third countries whether they have an adequate level of data protection. This principle is enforced through the jurisdiction of the European Court of Justice, as reflected in the Schrems I and II rulings, which invalidated two data transfer frameworks with the United States as not being deemed to provide adequate protections. Institutional commitments, strong oversight mechanisms, and the integration of the principle of the right to privacy as part of human rights in the Charter of Human Rights provide a solid foundation that allows the EU to maintain its bargaining position in upholding the principle of adequacy on the global stage. (Hijkman, 2016) (Commission, 2022)

Political Capacity

To ensure that the implementation of the data transfer clause in the Indonesia-United States trade agreement remains in line with the provisions of national law, especially the PDP Law, political capacity is needed through synergy across ministries and government agencies. The Ministry of Trade (Kemendag) plays the role of the main coordinator in the negotiation and drafting of derivative agreements, given its mandate in formulating international trade policies and agreements. The Ministry of Communication and Information Technology (Kominfo) has technical authority in terms of data governance, data protection equivalency assessment, and security supervision of electronic systems, so it must be actively involved in formulating technical standards and supervision mechanisms. The Ministry of Foreign Affairs plays a strategic role in bridging diplomacy between countries and ensuring that the implementation of agreements remains within the corridor of mutually beneficial international relations. Meanwhile, BPDP as an independent authority mandated by the PDP Law, will play a central role in evaluating the adequacy of data protection in destination countries, giving

approval to cross-border data transfers, and overseeing compliance with data protection principles. Close and sustainable coordination between these institutions is essential for Indonesia to implement its trade agreement commitments without compromising the principles of digital sovereignty and the protection of its citizens' personal data rights.

Political capacity is also needed in harmonizing tensions between the two policy coalitions. The digital trade liberalization coalition supported by digital business actors, economic ministries, and foreign investors is pushing for the opening of data access. Meanwhile, a protectionist coalition consisting of data protection agencies, civil society, and some policymakers is pushing for protection of national control. Political decisions in July 2025 are taken in the context of high external pressure, potentially causing resistance from pro-data protection groups. Public awareness of the implications of this policy is still low, while the mechanism for public participation is not structured. Facing this, political ability is needed to build a transparent public narrative regarding the benefits and risks of policies. With transparency, it is hoped that there will be space for the public to be involved in the drafting of derivative rules, as well as establish periodic evaluation mechanisms involving the House of Representatives and the public to maintain accountability. (Alliance, 2025) (Mehmet. Kaya, 2025)

Table 1. Comparison of Indonesia's Policy Capacity with Other Countries

Policy Capacity Dimension	Indonesia	European Union (EU)	Singapore
Technical	There is no adequacy assessment mechanism in place; the cross-border surveillance infrastructure is not yet integrated	Adequacy decisions are clear through GDPR, a periodic evaluation mechanism by the European Commission	Trustmark Data Protection, Automated Compliance Monitoring Tools, national incident response system
Administrative	BPDP is not yet fully operational; Cross-agency coordination is still weak	Member States' EDPB, EDPS, and DPAs function independently and integrated.	Independent PDPC with full authority as regulator and mediator
Politics	There is a tug-of-war between trade liberalization vs. data protection coalition; public legitimacy is still weak.	Privacy is positioned as a fundamental human right in the EU Charter of Human Rights so that political legitimacy is high	Strong support from governments and industry; trust-based digital economy narrative successfully builds public and investor legitimacy

From the description above, there is basically quite a lot of homework that must be taken by our government in fulfilling its commitments in the trade agreement with America. When compared to the European Union or Singapore (Table 1), there is a gap that must be filled by our government to be able to secure Indonesia's position in the trade agreement.

CONCLUSION

The analysis revealed that Indonesia's implementation of the Indonesia-US cross-border data transfer commitments faces significant limitations in technical, administrative, and political capacities. Technical capacity suffers from the lack of adequacy assessment mechanisms and cross-border supervision infrastructure, while administrative capacity is hindered by the non-operational status of BPDP as an independent authority. Politically, there is tension between the digital trade liberalization coalition and the data protection coalition. To address these challenges and maintain digital sovereignty, the government should expedite derivative regulations of the PDP Law, empower BPDP with full legitimacy, establish a Memorandum of Understanding ensuring compliance with the PDP Law for US data recipients,

and foster a transparent, participatory policy narrative. Future research could explore the effectiveness of these measures in enhancing Indonesia's policy capacity and the broader impacts on citizen rights and global data governance.

REFERENCES

Aaronson, S. A. (2018). Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows. CIGI Papers.

Alliance, G. D. (2025, July 23). Global Data Alliance. Retrieved from Global Data Alliance: https://globaldataalliance.org/news/gda-welcomes-us-indonesia-agreement-to-remove-indonesian-digital-customs-restrictions/

Arne Hintz, L. D.-J. (2019). Digital Citizenship in a Datafied Society. Florida: Polity Press.

Avram, A. (2023). International Data Transfer Challenges: Lack of Trust in U.S. Data Protection Mechanisms. Cornell International Law Journal.

Bigo, D. I. (2019). Data Politics. Oxford: Taylor & Francis.

Board, E. D. (2023, March 28). EDPB. Retrieved from EDPB: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf?utm_source=chatgpt.com

Chen, L. (2022). The Indo-Pacific Partnership and Digital Trade Rule Setting: Policy Proposals. Economic Research Institute for ASEAN and East Asia.

Commission, E. (2022). European Commission. Retrieved from European Commission: European Commission

Costa, G. D. (2025, July 24). Indonesia Business Post. Retrieved from Indonesia Business Post: https://indonesiabusinesspost.com/4823/society-environment-and-culture/indonesia-asked-to-reassess-data-privacy-terms-in-new-u-s-trade-deal?utm_source=chatgpt.com

Council, I. T. (2022). ITI's Comments Regarding Foreign Trade Barriers to U.S. Exports for 2023 Reporting. Information Technology Industry Council.

DCO. (2023). Enabling Cross-Border Data Flows Amongst the Digital Cooperation Organization Member States. Digital Cooperation Organization.

Erickson, A. (2019). Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD. Brooklyn Journal of International Law, 859.

European Commission. (2023). EU–US Data Privacy Framework: Questions & Answers. Retrieved from EU–US Data Privacy Framework: Questions & Answers: https://commission.europa.eu/

Executive Order. (2025). Regulating Imports with a Reciprocal Tariff to Rectify Trade Practices that Contribute to Large and Persistent Annual United States Goods Trade Deficits. Executive Order 14257.

GLBA. (n.d.). Gramm Leach Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999). U.S..

Hijkman, H. (2016). The European Union as Guardian of Internet Privacy.

Huw Roberts, J. C. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. Internet Policy Review.

Indonesia, P. R. (2022). Law Number 27 of 2022 concerning Personal Data Protection.

Jakob Edler, K. B. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. Research Policy.

JonesDay. (n.d.). Brazil Amps Up Enforcement of Data Protection Law. Retrieved from JonesDay: https://www.jonesday.com/-/media/files/publications/2024/09/brazil-amps-up-enforcement-of-data-protection-law/files/brazil-amps-up-enforcement-of-data-protection-law/fileattachment/brazil-amps-up-enforcement-of-data-protection-law.pdf?rev=a8617d4aad5b403f

Kristina Irion, M. E. (2021). Privacy Peg, Trade Hole: Why We (Still) Shouldn't Put. The University of Chicago Law Review.

Lantz, A. (2016). The EU-US Privacy Shield An insufficient level of data protection under EU Fundamental Rights Standards. Stockholm University: Stockholm University.

Leblond, P. (2024). Trade Agreements and Data Governance. cigionline, 91.

M. Howlett, M. R. (2016). The two orders of governance failure: Design mismatches and policy capacity issues in modern governance. Policy and Society, 157–169.

Macievic, L. (2024). A Diversity of Adequacy: The European Commission's 11-Country Adequacy Review. American University Washington College of Law.

Mehmet. Kaya, H. S. (2025). Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance. Interdisciplinary Studies in Society, Law, and Politics, 219-233.

Milan & Treré. (2019). Big data from the South(s): Beyond data universalism. Television & New Media. Sage Journal, 319-335.

Ncheke, T. R. (2020). Cross-border data flows in the digital economy: an analysis between the European Union General Data Protection Regulation and the Southern African Development Community Data Protection Model law. South Africa: University of Pretoria.

Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. (n.d.).

Rajmohan, K. (2025, January 23). TechPolicy.PRESS. Retrieved from TechPolicy.PRESS: https://www.techpolicy.press/data-localization-indias-tryst-with-data-sovereignty/

Reuters. (2016, June 26). Retrieved from Reuters: https://www.reuters.com/world/us/federal-data-privacy-laws-gain-support-us-congress-critics-remain-2024-06-26/?utm_source=chatgpt.com

Roberto Baldoni, G. D. (2025). Sovereignty in the Digital Era: The Quest for Continuous Access to Dependable Technological Capabilities. IEEE Security & Privacy, 91-96.

Rubinstein, I. S. (2010). Privacy and Regulatory Innovation Moving Beyond Voluntary Codes. A Journal of Law and Policy for the Information Society, 355.

Singapore, P. (n.d.). Data Protection Trustmark. Retrieved from PDPC Singapore: https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-trustmark?utm_source=chatgpt.com

Treré, S. M. (2019). Big Data from the South Towards a Research Agenda. DATACTIVE Working Paper Series.

UNCDF. (2021). Cross-border data flows and development: For whom the data flow,. supra, 105.

Law Number 27 of 2022 concerning Personal Data Protection. (n.d.).

Union, E. (2016). General Data Protection Regulation (Regulation (EU) 2016/679).

Voss, W. G. (2020). Cross-Border Data Flows, the GDPR, and Data Governance. Washington International Law Journal, 485-532.

Wu, X. R. (2015). Policy capacity: A conceptual framework for understanding policy competences and capabilities. Policy and society, 165-171.

Ying Chen, Y. G. (2022). Comparative analysis of digital trade development strategies and governance approaches. Journal of Digital Economy, 227-238.

Zhixian Zhuang, X. L. (2024). CBCMS: A Compliance Management System for Cross-Border Data Transfer. IEEE International Conference on Big Data (BigData), (pp. 4789-4798).