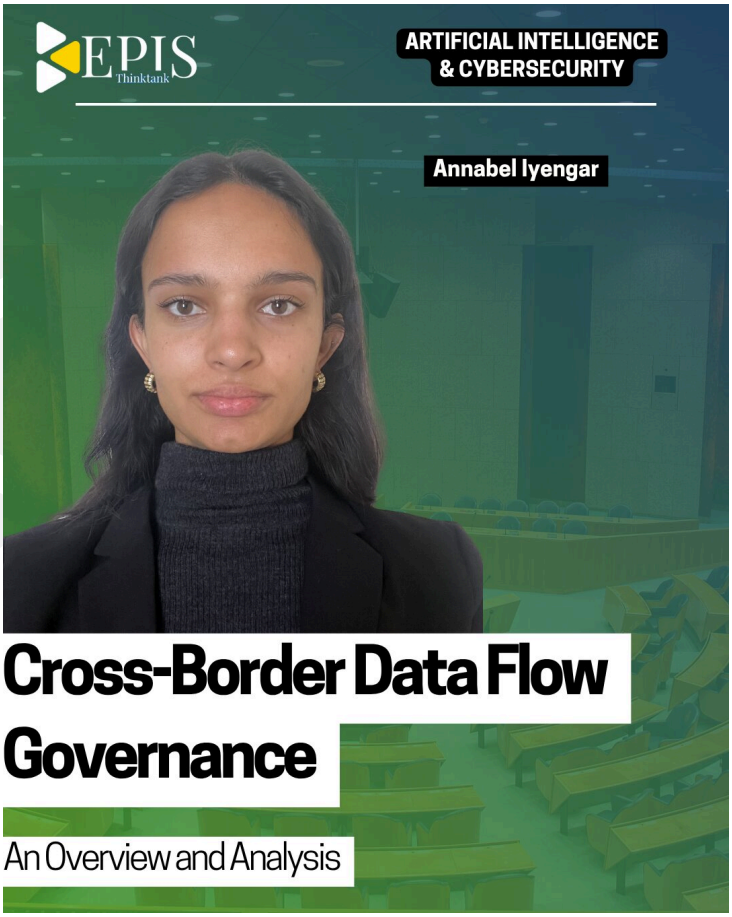
Cross-Border Data Flow Governance

27 MARCH 2026

Annabel Iyengar



1.Introduction:

2.Four Existing Data Governance Frameworks:

2.1 EU Framework for Cross-Border Data Flows

The first regulatory framework is that of the EU, called the General Data Protection (GDPR), which came into effect on May 25th 2018. Founded on EU Privacy Directives, the GDPR prioritizes fundamental rights to privacy and data protection in the regulation of cross-border data flows (Mehmet & Hamza, 2025, p. 222). Importantly, the GDPR imposes strict requirements on international data transfers, namely that such transfers are only permit-

ted when the recipient state has adequate data safeguards in place that are functionally equivalent to digital standards within the EU's framework (Mehmet & Hamza, 2025, p. 222). This means that the GDPR requires 'adequate' protection to follow data, around the globe if necessary. Companies that use the personal data of EU citizens must vet service providers, regardless of how long their chains are, for compliance with the demands of the GDPR framework (Hoofnagle, Sloot, & Borgesius, 2019, p. 68). As a result, multinational corporations must ensure that all service providers using any data belonging to EU citizens have made, and abide by, the requisite contractual agreements (Hoofnagle, Sloot, & Borgesius, 2019, p. 68). The GDPR also further centres user privacy by seeking to improve the requisite quality of consent for sharing personal data with companies, making clear policy preferences for "human-in-the-loop systems" (Hoofnagle, Sloot, & Borgesius, 2019, p. 68). Stricter conditions on cross-border data transfers and consent conditions also expand the notion of 'data breaches' subject to penalisation and in 2022 GDPR fines reportedly totalled 832 million euros (Hoofnagle, Sloot, & Borgesius, 2019, p. 68) (Bologa, 2023). These reasons, amongst others, mean attitudes towards the GDPR framework vary as it boosts data privacy but complicates global data chains and penalises all companies equally, regardless of company size (Bologa, 2023).

2.2 US Framework for Cross-Border Data Flows

The second regulatory environment around cross-border data flows is that of the United States. The primary feature of the US's data regulation and safeguarding framework is that there currently exists "no comprehensive law concerning data privacy on the internet similar to the GDPR" (Tran, 2021). Instead, the US has its own patchwork of regulatory legislation concerning more specific sub- categories of data privacy and safeguarding, as well as emerging privacy statutes enacted by individual states on behalf of their state citizens. In March 2018, the US introduced the Clarifying Lawful Overseas Use of Data (CLOUD) Act (Daskal, 2018, p. 221). The first key feature of this act comprises US extraterritorial data access; US law enforcement can access data held by US- based service providers, even if the data is stored abroad (Daskal, 2018, p. 222). Secondly, by CLOUD the US can sign agreements with trusted foreign governments whereby the foreign governments are then permitted to bypass the standard, and lengthy, mutual legal assistance treaty (MLAT) procedure (Daskal, 2018, p. 222). Furthermore, in December 2024, the US issued 'the final rules' "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (Clyde&Co, 2025). Whilst these 'final rules' represent the first US regulatory move concerning cross-border data flows, they do not cover data transfers to all jurisdictions, as the GDPR does, only transfers to 'countries of concern' (Clyde&Co, 2025). Whilst these rules exemplify a push towards strategic governance of dataflows, the US still lacks a comprehensive data governance framework. As a result, states such as Texas, California, Oregon, and Colorado have begun to enact their

own regulatory consumer privacy statutes (HIPAA, 2021). Overall, whilst US regulation marks an important push towards data privacy and protection, the lack of a comprehensive framework distinguishes it from the GDPR.

2.3 Chinese Framework for Cross Border Data Flows

Digital Sovereignty is a core aspect of China's framework for cross-border data governance ((Jiang, 2022, p. 22). Not only is this considered fundamental for equal global order, but it is also allegedly a response to America's pursuit of data hegemony (Jiang, 2022, pp. 24-25). Beijing also adopts a development-oriented approach, championing safe and organised data flows over involvement in debate around data access or localisation (Jiang, 2022, p. 25). In regulatory measures, this is exemplified by the Measures for Certification of Cross-Border Personal Information Transfer (Measures) which took effect on January 1st, 2026 (Zhou, 2025). These measures complete China's Personal Information Protection Law (PIPL) regulations for cross-border data flows of personal information, under which three legal pathways are outlined for the transfer of personal data overseas (Zhou, 2025). These pathways are either by security assessment, by obtaining a certification for the relevant dataflows, or through signing a standard contract for foreign parties ensuring alignment with conditions set out by the Cyberspace Administration of China (CAC) (Zhou, 2025). In the recent past, China's approach to cross-border data flows and protection has been subject to wide criticism from the West, facing accusations of insufficient legal protection of data coupled with excessive measures against multinationals which unduly hamper data flows (Jiang, 2022, p. 22). However, the CAC's issuance and completion of the PIPL have been internationally recognised as a relaxation on cross-border data flows in the name of greater investment, development and data governance (Gou & Li, 2025). Prioritisation of economic growth has therefore prompted China to better position itself for digital trade through cross-border data flows (Gou & Li, 2025).

2.4 Indian Framework for Cross-Border Data Flows

A final emerging governance framework for data privacy and protection is India's treatment of personal data protection. In 2025 India published the Digital Personal Data Protection Rules, and in November 2025 began operationalising the 2023 Digital Personal Data Protection Act (DPDP) (Kumar, 2025). As an approach to cross-border data transfer governance the DPDP Act marks a divergence from existing global regulatory frameworks as it operates on a "negative list" system rather than the "adequacy" or "whitelist" system of the GDPR and other governance systems (Kumar, 2025). This means that the default position for cross-border data transfers to other jurisdictions is that they are permitted, and only when transfers to certain jurisdictions are explicitly disallowed does this stop being the case. Whilst this less restrictive "blacklisting" method facilitates cross-border data flows, there is continued uncertainty and opacity around the criteria for being 'blacklisted' (Reddy, 2023). It is also the case that, whilst the existing DPDP

regulations establish a governance framework for personal data, non-personal data lacks similar guidance (Reddy, 2023). India's emerging data governance framework aims to address several policy initiatives including protecting privacy rights, enhancing governmental control over data, warding off data colonialism, and nurturing domestic digital investment (Mishra, 2023, p. 240). However, India's current stance has been criticised for over-prioritising data protection from international actors to the detriment of playing a proportionate role in shaping the digital economy (Mishra, 2023, p. 240).

3. Analysis of Cross- Border Data Flow Frameworks:

3.1 Strengths

Having outlined above four of the main existing global frameworks for data governance, I will now outline some key strengths of said frameworks, but more notably I will highlight how misalignment between governance systems is proving an increasing hinderance to interoperability in digital trade. Firstly, many of the existing cross-border data flow frameworks align at least partially with the concept of 'data free flow with trust' (DFFT). This concept was introduced by Japan at the World Economic Forum Annual Meeting in 2019 and was later endorsed by G7 leaders at the 2023 G7 Digital and Tech Minister's Vision for Operationalising DFFT and its Priorities (OECD, 2023). Designed to drive economic and social prosperity whilst managing associated risks and challenges, DFFT is reflected in existing governance frameworks via established pathways through which data can be shared across jurisdictions such as the GDPR's adequacy framework, China's three pathways for data transfers, or India's 'blacklist' mechanism. Furthermore, the emergence of comprehensive and even patchwork governance systems represent development in accountability mechanisms through which the misuse of personal data can be addressed. For example, in 2024 Meta was fined £75 million by the Irish Data Protection Commission for inadequate protection of user passwords against GDPR regulations (BBC, 2024). Furthermore, Texas won its citizens a $1.04 billion settlement against Meta in the largest state data privacy settlement to date (NG, 2024). These cases exemplify how both comprehensive and non-comprehensive governance frameworks for data trade and protection are advancing digital trade policy to better shield citizens from exploitation of personal data.

3.1 Weaknesses of Existing Frameworks

For large multinational companies and even small to medium enterprises (SMEs) the rising number of data localisation measures between governments and different rules concerning cross-border data flows make global business increasingly complex and fraught with legal dilemmas. Data localisation laws require specific data localisation strategy to navigate patchwork frameworks, most importantly to legally comply with data storage requirements, but also because failure to sufficiently establish regional infrastructure and adequate storage arrangements can delay entry into new markets and lead to costly regulatory catch-up on products (Chow, Sim , & Hubert,

2021). For example, under Vietnam's localisation laws 'foreign providers of online services' may have to store data in Vietnam and establish a local office, whereas in Indonesia, its 'public electronic system operators' who must set up a local data centre (Chow, Sim , & Hubert, 2021). Differences in localisation laws can thus lead to multinationals facing large fines for failing to navigate an increasingly complex regulatory environment. Linking back to the above exposition of the EU, US, Chinese, and Indian regulatory frameworks, misalignment between data transfers and access rules can mean that compliance with the rules of one jurisdiction can mean violating the rules of another, particularly as desire for data sovereignty increases. TikTok was fined €530 million in 2025 for lack of data storage compliance with the GDPR rules by failing to keep EU citizen's data stored in the EU and smaller firms could similarly suffer if they lack the manpower and resources to remain compliant across systems (Prescott, 2025). Companies with an existing and established global infrastructure will need to implement costly measures to adjust their operations around diverging demands of jurisdictions.

4. Policy Recommendations in Light of Analysis

The overriding consensus on the existing regulatory landscape for cross-border digital trade is thus that it is 'patchwork' and fragmented. Considering this analysis, recommendations will now be provided for how global trade could be better facilitated by regulatory measures, whilst retaining due protection of data in storage and in transfers.

5.Conclusion:

It is by prioritising interoperability and cohesiveness that all countries, whether mentioned in this article or not, can begin to better capitalise on the ever-increasing value of data in global digital trade. This article has outlined four primary existing and emerging data governance frameworks to highlight both how align, and more significantly how they differ. Whilst the EU prioritises high-quality consent and adequate data protection in an overarching framework, the US has yet to enact a comprehensive federal framework, forcing states to forge their own privacy statutes. China meanwhile has begun to loosen their stance on data protectionism through three established pathways for digital trade, whilst India operates off an almost opposite default transfer system with a 'blacklist' of jurisdictions for whom transfers are prohibited.

Although there are emerging initiatives such as the EU's Digital Simplification Package, many parts of which pertain to GDPR compliance, the global regulatory framework continues to complicate as states race to implement frameworks which protect their data from exploitation and allow them established pathways into digital trade. In the absence of greater drive behind alignment of such frameworks, trade will continue to suffer in the name of data protectionism as fractured regulatory compliance inhibits economic growth and hinders the scaling of firms and states who lack the means of navigating such an environment.

Works Cited

BBC. (2024, September 27). *Facebook parent company fined €91m over password storage.* Retrieved from BBC News: https://www.bbc.co.uk/news/articles/cvgl8lerx85o

Bergsen, P., Caeiro, C., & Moynihan, H. (2022, January). *Opportunities for strengthening US, EU and UK cooperation on digital technology governance.* Retrieved from Chatham House: Digital Trade and Digital Standards: https://www.chathamhouse.org/sites/default/files/2022-01/2022-01-24-digital-trade-digital-technical-standards-bergsen-et-al.pdf

Bergsen, P., Caeiro, C., Moynihan, H., Scheinder-Petsinger, M., & Wilkinson, I. (2022). *Digital trade and digital technical standards: Opportunities for Strengthening US, EU and UK cooperation on digital technology governance.* London: Chatham House.

Bologa, A. (2023, February 7). *Fifty Shades of GDPR Privacy: The Good, the Bad, and the Enforcement*. Retrieved from CEPA: https://cepa.org/article/fifty-shades-of-gdpr-privacy-the-good-the-bad-and-the-enforcement/

Casalini, F., López-González, J., & Nemoto, T. (2021). *Mapping Commonalities In Regulatory Approaches to Cross-Border Data Transfers.* OECD Publishing. Retrieved from OECD.

Chow, P., Sim , C., & Hubert, C. (2021, December 9). *Increasing localisation of data in Asia: Why this matters for tech.* Retrieved from Hebert Smith Freehills Kramer: https://www.hsfkramer.com/insights/2021-12/increasing-localisation-of-data-in-asia-why-this-matters-for-tech

Clyde&Co. (2025, February 19). *U.S. Issues Final Rules Regulating Cross-Border Flow of Data for the First Time*. Retrieved from Successful Risk Navigation: https://www.clydeco.com/en/insights/2025/02/us-issues-rules-regulating-cross-border-data-flow

Cory, N., & Dascoli, L. (2021, July 19). *How Barriers to Cross-Border Data Flows Are Spreading Globally, Whatc They Cost, and How to Address Them.* Retrieved from Information Technology and Innovation Foundation: https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

Daskal, J. (2018). Unpacking the CLOUD Act. *European Law Forum*, 220-225.

Dewaranu, T., Hodgson, G., & Audrine, P. (2022). *Regulating Cross-Border Data Flows in the Development Context.* Indonesia: Center for Indonesian Policy Studies . Retrieved from Center for Indonesian Policy Studies: https://www.cips-indonesia.org/publications/regulating-cross-border-data-flows-in-the-development-context?lang=id

Du, Z. (2022). Human Rights Violations by Multinational Corporations and the Outlet to Judical Difficulties. In Z. Du, *Proceedings of the 2022 2nd International Conference on Entreprise Management and Economic Development (ICEMED 2022)* (pp. 679-685). Atlantic Press.

Gou, S., & Li, X. (2025). Cross-border data flow in China: Shifting from restriction to relaxation? *Computer Law and Security Review* .

HIPAA. (2021, November 2). *Summary of the HIPPA Security Rule*. Retrieved from U.S. Department of Health and Human Services: https://www.hhs.gov/hipaa/forprofessionals/security/laws-regulations/index.html.

Hoofnagle, C., Sloot, B., & Borgesius, F. (2019). The European Union General Data Protection Refugulation: what is it and what does it mean? *Information and Communications Technology Law* , 65-98.

Jiang, X. (2022). Governing Cross-Border Data Flows: China's Proposal and Practice. *China Quarterly of International Strategic Studies* , 21-37.

Kumar, J. (2025, November 14). *Cross-Border Data Transfers Under the DPDP Act, 2023 and DPDP Rules 2025: Navigating India's New "Negative List" Regime.* Retrieved from King Stubb and Kasiva: https://ksandk.com/data-protection-and-data-privacy/indias-new-cross-border-data-transfer-framework/

Medine, D. (2024). *Data Localization: A "Tax" on the Poor.* London, Washington: Center for Global Development.

Mehmet, K., & Hamza, S. (2025). Cross-border data flows and digital sovereignty: Legal dilemmas in Transnational governance. *Interdisciplinary Studies in Society, Law, and Politics* , 219-233.

Mishra, N. (2023). Data Governance and Digital Trade in India: Losing Sight of the Forest for the Trees? In A. Chander, & H. Sun, *Data Sovereignty: From the Digital Silk Road to the Return of the State* (pp. 240-263). New York: Oxford Academic.

NG, A. (2024, July 30). *Meta agrees to pay Texas $1.4 billion in largest state data privacy settlement.* Retrieved from Politico: https://www.politico.com/news/2024/07/30/meta-texas-settlement-00171823

OECD. (2023, April 27). *Moving Forward on data free flow with trust: New evidence and analysis of business experiences.* Retrieved from OECD Digital Economy Papers: https://doi.org/10.1787/1afab147-en

Prescott, K. (2025, May 2). *TikTok fined over EU users' information kept in China.* Retrieved from The Times: https://www.thetimes.com/uk/social-media/article/tiktok-fined-over-eu-users-information-kept-in-china-0xpdhxl28?gclsrc=aw.ds&&utm_source=google&utm_campaign=17515457033&adgroupid=&utm_medium=cpc&utm_content=&utm_term=&gad_source=1&gad_campaignid=213440639

Reddy, S. (2023, December). *Why Localise Data? India's Approach to Cross-Border Data Flows.* Retrieved from Goethe-Institut: https://www.goethe.de/ins/in/en/kul/fmd/afu/25298606.html

Tran, H. (2021, November). *Issue Brief- Competing Data Governance Models Threaten the Free Flow of Information and Hamper World Trade.* Retrieved from Atlantic Council Geoeconomics Center.

Zhou, Q. (2025, October 24). *China Releases Certification Measures for Cross-Border Data Transfers- The Last Piece of the Regulatory Puzzle.* Retrieved from Dean Shira and Associates: https://www.china-briefing.com/news/china-cross-border-data-transfer-certification/?utm_