THINK7 CANADA 2025

G7 2025 KANANASKIS

Policy Brief

Task Force 2: Digitalization of the Global Economy

Tech and Data Governance: Cross-Border Compliance Challenges and Strategy

Lead Author:
Syed Munir Khasru

Co-Author:
Stephanie Diepeveen

April 2025

Key Points

- Multinational corporations face compliance challenges due to fragmented regulations brought about by the absence of a harmonized global data governance framework.
- Geopolitical tensions and data sovereignty policies complicate establishing unified data governance standards.
- Data localization laws disrupt digital trade, raise operational costs, and hinder innovation in AI, cloud computing, and fintech.
- Privacy-enhancing technologies such as federated learning, homomorphic encryption, and decentralized identity verification offer solutions to regulatory fragmentation while ensuring security and compliance.
- Multilateral cooperation through G7, G20, and WTO is essential to developing interoperable frameworks that balance privacy, security, and global economic integration.

Introduction

The digital economy has become a defining force in global commerce, reshaping industries and international economic relations across the G7 and beyond. At its core, data has become a key economic asset, essential for innovation, competitiveness, and cross-border trade (Birch, Cochrane, and Ward 2021). However, the absence of a standardized global data governance framework has resulted in a fragmented regulatory landscape, creating challenges for not just major technology firms, but also SMEs, digital startups, and fintech firms.

Global initiatives, such as the United Nations' Global Digital Compact seek to establish shared principles for an open, secure, and inclusive digital future by addressing regulatory inconsistencies, data governance gaps, and digital divides (Walther 2024). Yet, G7 economies, representing 46% of global GDP, have diverging approaches to data governance. The EU's GDPR imposes stringent privacy rules, resulting in over $4 billion in fines (European Data Protection Board, 2023), affecting companies ranging from Meta to Airbnb and regional e-commerce platforms. Meanwhile, the U.S. CLOUD Act and sector-specific regulations enable broader data-sharing, which creates tensions with privacy-focused regimes (Voss 2020). Japan's Data Free Flow with Trust (DFFT) initiative promotes interoperability, but uptake among other G7 countries has been slow. These varying standards make it difficult for companies to align their global operations, leading to legal uncertainty and constrained digital trade (Potluri, Sridhar, and Rao 2020).

Moreover, data localization laws in emerging economies such as India, Brazil, and China disproportionately affect smaller firms that cannot afford the high compliance costs of maintaining local data storage. A small fintech startup in Canada or Germany may struggle to expand internationally due to these regulatory burdens, while a large multinational corporation possesses the financial and technical capacity to comply.

At the same time, restrictive data policies undermine innovation by limiting access to cross-border datasets, that are critical for AI development, predictive analytics, and digital services. Without a coordinated global response, these regulatory barriers will continue to stifle innovation, increase compliance burdens, and fragment the digital economy (OECD, 2023). The G7, as a collective of leading economies, must take the helm in bridging regulatory divides and establishing an interoperable framework that supports both multinational corporations and smaller enterprises.

Defining the Problem

The rapid digitalization of global commerce depends on seamless cross-border data flows; yet stringent localization mandates have imposed significant burdens on businesses, major technology firms, as well as, small ones. While often justified on national security, privacy, and sovereignty grounds, these regulations increase compliance costs, disrupt innovation, and create cybersecurity risks (Mishra 2016). By early 2023, nearly 100 localization measures were in place across 40 countries, with China, Russia, India, and Brazil enforcing rigid frameworks that require foreign firms to store data domestically (OECD 2023; Taylor 2020). However, there is not necessarily a direct tradeoff between regulation and innovation; regulatory approaches can affect companies of different sizes and jurisdictions differently.

Additionally, GDPR and the Schrems II ruling have further restricted EU-U.S. data flows, complicating compliance for multinational companies (Swire et al. 2024). On the other hand, only 30 countries in Africa have comprehensive data protection laws (Babalola 2023), creating asymmetries in global digital trade. Without a coordinated global response, regulatory barriers are likely to persist, limiting innovation and increasing compliance burdens.

Case Study: The Impact of Data Localization Laws

- Cloud Computing: Global cloud providers ensure cost efficiency and cyber resilience, but data localization limits these benefits and increases service costs.
- Financial Services: Payment systems like SWIFT and blockchain technologies rely on global data transfers. Localization disrupts banking, lending, and cross-border transactions.

- **E-commerce:** Small businesses and online marketplaces face barriers to reaching international customers due to fragmented regulations.
- **Medical Research:** GDPR restrictions have led EU and EEA researchers to withdraw from a cancer study collaboration with the U.S. National Cancer Institute due to cross-border data transfer concerns.
- **Telecommunications:** 5G infrastructure depends on international expertise and cloud services. Localization increases costs and reduces service quality.
- **Social media & Video Conferencing**: Platforms like Zoom and social networks rely on cross-border data flows. Restrictions limit access to content moderation tools and real-time language translation.
- **Streaming & Gaming:** Streaming services like Netflix, Spotify, etc., depend on international servers. Video game developers struggle with monitoring security and preventing cheating across jurisdictions.
- **Ride-sharing:** Localization disrupts ride-sharing apps, preventing users from accessing trip history and driver ratings across different countries.
- **Agriculture:** Modern farming tech (e.g., John Deere's precision agriculture tools) relies on global data exchange. Localization isolates farmers from valuable insights. (CIPL, TLS, 2023)

Localization mandates increase data management costs by up to 55%, particularly in sectors like cloud computing, fintech, and e-commerce. Additionally, forced localization distorts market competition by favoring domestic firms and limiting international threat intelligence cooperation (OECD 2023). Economically, forced localization distorts market competition by favoring domestic firms, leading to higher costs for consumers and SMEs that rely on cloud solutions (Potluri, Sridhar, and Rao 2020).

G7 Approaches to Data Regulation

G7 nations have taken varied approaches to data governance. The United States promotes free data flows through trade agreements like USMCA while maintaining sector-specific restrictions (Mishra 2016), including the CLOUD Act, which grants U.S. authorities access to foreign-held data. The European Union, under GDPR, restricts data transfers to countries without adequate safeguards, creating compliance burdens for global firms (Birch, Cochrane, and Ward 2021). Cross-border data restrictions complicate digital trade, particularly with the U.S., after the Schrems II ruling invalidated the EU-U.S. Privacy Shield (Swire et al. 2024). While it strengthens consumer privacy, critics argue it increases compliance costs, particularly for SMEs (Mishra 2016). Japan leads the Data Free Flow with Trust (DFFT) initiative, advocating for open yet secure cross-border data flows (OECD 2023). Canada avoids rigid localization but enforces provincial restrictions on public-sector data (Taylor 2020). France and Germany comply with GDPR while promoting European data sovereignty through initiatives like GAIA-X, which aims for independent cloud infrastructure (Marelli, Testa, and Van Hoyweghen

2021). Despite recognizing the need for global data governance, G7 nations remain divided on regulatory priorities, increasing business costs and limiting digital trade across borders. Stronger multilateral cooperation is essential to developing interoperable frameworks that balance privacy, security, and economic growth.

Bridging the Gaps in Data Governance

The divergence in regulatory approaches across G7 and G20 nations underscores the urgent need for standardized global standards on data governance. While data localization policies aim to enhance privacy and national security, their economic and operational repercussions necessitate a more balanced approach. Multilateral efforts, particularly within the G7, G20, and WTO, should prioritize regulatory interoperability, promoting frameworks that facilitate secure data flows while addressing privacy and cybersecurity concerns (Birch, Cochrane, and Ward 2021). There is a need for governments to consider where there is and can be common alignment around data governance to promote more transparent, consistent and secure data flows and use across countries.

To reduce regulatory fragmentation, global leaders must focus on (Mishra 2016):

- Regulatory interoperability: Establishing mutual recognition agreements for compliance.
- Trade agreements: Utilizing economic treaties like USMCA and CPTPP to discourage restrictive localization policies.
- Public-private partnerships: Encouraging collaboration between governments, industry stakeholders, and international bodies like the WTO and OECD.
- Technological solutions: Deploying privacy-enhancing technologies, such as homomorphic encryption, federated learning, and zero-knowledge proofs, to ensure secure yet compliant data flows.

The current trajectory of data localization policies presents formidable challenges for global digital commerce, innovation, and cybersecurity. A coordinated international response, underpinned by standardized regulatory principles, technological advancements, and multilateral cooperation, is essential to fostering a digital economy that is both secure and efficient. Without such coordination, the risk of regulatory fragmentation and digital protectionism will continue to impede the growth and competitiveness of the global digital ecosystem.

Data Policies Beyond the G7

Beyond the G7 and the U.S., several countries have developed distinct data governance frameworks, reflecting national security priorities, privacy concerns, and digital sovereignty strategies. China enforces strict data localization under the Cybersecurity Law (2017), Data Security Law (2021), and PIPL, granting the government broad access to stored data. These regulations have compelled Apple and Tesla to establish local data centers (OECD 2023; Taylor 2020).

Russia mandates domestic storage of citizens' data under the Federal Law on Personal Data (2015), leading to platform restrictions like the blocking of LinkedIn (Mishra 2016). India proposes a graded localization model with sector-specific exemptions, aiming to balance national security with GDPR-style protections (Swire et al. 2024).

Brazil has implemented the General Data Protection Law (LGPD), which aligns with GDPR principles while maintaining strict data transfer requirements. This has posed compliance challenges for multinational firms operating in Latin America (OECD 2023). South Korea, under the Personal Information Protection Act (PIPA), enforces stringent privacy rules and requires regulatory approvals for cross-border data transfers, affecting cloud service providers and e-commerce platforms (Taylor 2020).

These diverse regulatory models serve as proof of the global fragmentation of data governance, underlining the need for Standardized international standards to facilitate secure and efficient data flows.

The Geopolitics of Data Sovereignty

Data governance is no longer just a regulatory concern; it has become a geopolitical tool used by nations to strengthen national security, economic independence, and global influence. China's Cybersecurity Law and PIPL exemplify a state-controlled data model, requiring foreign companies to store and process Chinese user data within the country while allowing government access under certain conditions. The contrast between U.S. and EU regulatory approaches further stresses the complexities of data sovereignty. The U.S. prioritizes a business-friendly, innovation-driven model, while the EU enforces privacy-centric regulations such as GDPR, often creating friction between transatlantic businesses. Meanwhile, BRICS nations are collectively pursuing digital sovereignty policies, reducing reliance on Western cloud infrastructure and establishing alternative digital ecosystems. If these divergent approaches continue, they risk fragmenting the global internet into

regionally isolated digital economies, undermining innovation, and restricting global business operations.

Policy Recommendations

1. Establishing a Prioritization Framework for Global Data Governance

Global data governance demands a coordinated approach that balances privacy, security, and economic efficiency. A structured prioritization framework is necessary to ensure that data governance policies focus on the most pressing and feasible actions. G7 nations should categorize recommendations based on immediacy and long-term impact.

- Immediate Actions:
    - Initiate mutual recognition agreements to streamline regulatory compliance across G7 nations and align with the Data Free Flow with Trust (DFFT) framework (Taylor 2020). This includes developing a clear roadmap for phased implementation to ensure feasibility.
    - Encourage cross-sector partnerships to develop compliance tools that enable firms of all sizes to navigate data regulations efficiently.
- Long term action:
    - Establish a G7 data governance secretariat. The entity will serve as a central advisory body to coordinate best practices, regulatory updates, and stakeholder dialogues on emerging digital governance challenges (Center for AI and Digital Policy 2023).
    - Promote privacy-preserving technologies, i.e., federated learning, and encryption, to ensure secure data access without restrictive localization (Swire et al. 2024).

2. Develop a G7 Framework for Interoperable Data Governance

Interoperable regulatory frameworks can reduce compliance burdens and enhance cross-border data flows. The G7 should take the lead in negotiating mutual recognition agreements (MRAs) that harmonize data protection, privacy regulations, and cybersecurity protocols.

- Cross-Border Compliance Coordination: Establish a standardized compliance mechanism for compliance monitoring, data-sharing policies, and cross-border regulatory cooperation. It will ensure interoperability across jurisdictions (Mishra 2016), reducing legal uncertainty for businesses operating in multiple regions.

- **Legal and Technical Integration:** Interoperability must align with existing frameworks like GDPR, USMCA, and APEC Cross-Border Privacy Rules (Swire et al. 2024). Coherence will ensure predictable regulatory environments.

3. Strengthening Cybersecurity and Data Resilience

The rising risk of cybersecurity complicates cross-border data flows. The G7 can facilitate cybersecurity collaboration by establishing a dedicated intelligence-sharing mechanism, to prevent cyberattacks targeting critical infrastructure.

- **Resilient Data Storage Strategies:** Promoting secure and redundant data storage mechanisms, i.e., Multi-Region Cloud Storage, Hybrid Cloud Storage Solutions, etc., to ensure that data flows remain protected against cyber disruptions.
- **Cybersecurity Intelligence-Sharing Framework:** Enhance real-time data-sharing between G7, G20, and international cybersecurity bodies to counter cyber threats (Swire et al. 2024), including coordinated incident response mechanisms. By ensuring safe data flow, it will encourage and support innovation across countries with diverse public and private capacities and would enhance cyber defense capabilities.
- **Standardizing Security Protocols:** Develop G7-wide cybersecurity frameworks aligned with EU-U.S. Cybersecurity Partnership, ensuring companies comply with uniform security requirements.

4. Facilitating the Adoption of Privacy-Enhancing Technologies (PETs)

Privacy-enhancing technologies (PETs) offer practical solutions for navigating data localization and compliance challenges. However, adoption barriers such as high costs, lack of expertise, and regulatory uncertainty persist (Micheli et al. 2020).

- **Incentivize PET Development:** Provide funding mechanisms for research into homomorphic encryption, zero-knowledge proofs, and federated learning (Birch et al. 2021), ensuring widespread adoption across industries.
- **Public-Private Innovation Hubs:** Establish joint R&D initiatives between governments, academia, and industry to accelerate the adoption of PETs. Emphasis to be particularly in sectors handling sensitive personal data.
- **Regulatory Integration:** Ensure that PETs are recognized as compliant tools under frameworks like GDPR, CCPA, and APEC Cross-Border Privacy Rules (CIPL 2023), reducing compliance uncertainty.

5. Optimize Cross-Border Data Storage and Processing Mechanisms

To enhance efficiency and security in global data flows, the G7 should establish unified policies on cross-border data storage and processing, ensuring data sovereignty concerns are balanced with innovation.

- **Standardized Data Transfer Protocols:** Implement G7-wide guidelines for secure and efficient cross-border data processing (OECD 2023).
- **Assess the Costs of Localization Policies:** Review and revise data localization regulations that inadvertently increase compliance costs and cybersecurity risks (Mishra 2016), promoting evidence-based policymaking.
- **Encourage Secure and Redundant Data Infrastructure:** Promote policies that support efficient, interoperable, and resilient data storage solutions. The aim is to mitigate risks related to supply chain disruptions and cyberattacks.

6. Advancing Sustainable Data Governance and Green Digital Policies

Sustainable data governance must be integrated into the G7's digital transformation agenda to mitigate the environmental impact of data storage and processing.

- **Promote Energy-Efficient Data Centers:** Encouraging the co-location of data centers with renewable energy sources will help reduce carbon footprints (OECD 2023).
- **Green Digital Infrastructure Incentives:** Governments should implement tax incentives, grants, and regulatory benefits for companies that adopt sustainable computing practices (Architectural Digest 2023).
- **Circular Digital Economy Practices:** Policies should support hardware recycling, e-waste management, and extended IT infrastructure lifecycles (Reuters 2024).
- **Waste Heat Recovery Initiatives:** Expanding initiatives like Finland's repurposing of data center heat for residential heating can contribute to energy efficiency (Architectural Digest 2023).

Conclusion

The rapid growth of the digital economy has made standardized data governance more urgent than ever. Current divergent regulatory policies create regulatory fragmentation, compliance burdens, and cybersecurity risks (OECD 2023). A multilateral approach, led by G7 and G20 initiatives, along with interoperable frameworks, can help facilitate secure data flows while balancing privacy, security, and economic interests (IBM Policy Lab 2023). Meanwhile, advancements in PETs provide technological solutions to reduce reliance on restrictive localization policies. Cybersecurity resilience must remain a priority, requiring collaborative defense strategies across G7 nations.

Without global cooperation, regulatory fragmentation will continue to stifle digital trade and innovation. The G7, G20, and WTO must take the lead in aligning policies. While governments, industries, and civil societies work together to create a balanced regulatory environment that supports innovation, economic growth, and sustainability. The foundation for a secure, inclusive, and future-ready digital ecosystem is already in place. What's needed now is decisive action (CSIS 2023).

Author Biographies

Lead Author

Prof. Syed Munir Khasru, Chairman, IPAG Asia Pacific, Australia

Prof. Syed Munir Khasru is a global thought leader with over a decade of involvement in G7 and G20 communities. He has led around 25 policy briefs and co-chaired task forces for both G7 and G20. An MBA from the Wharton School of Business, University of Pennsylvania, US, Prof. Syed Munir Khasru (www.syedmunirkhasru.org) founded, and successfully built two world-class institutes in the global knowledge industry. The international knowledge outfit, the Institute for Policy, Advocacy, & Governance (IPAG) (www.ipag.org), and the international management consulting firm e.Gen Consultants Ltd. (www.egenconsultants.com).

Under Prof. Munir's leadership, IPAG has become a well-respected international knowledge outfit from the developing Global South addressing global challenges in key policy and strategy in areas like geopolitics & multilateral affairs, sustainable development & green growth, climate change & energy transition, digital transformation & cyber security. His innovative approach has seen leveraging a policy-focused knowledge outfit IPAG with a project implementation wing i.e. e.Gen, creating a unique synergy in the global knowledge industry. Prof. Munir 's active engagement with international forums like G7 and G20 and multidisciplinary expertise has enabled him to lead from the front in translating policies into practices and strategies into impactful solutions on a global scale.

Co-Author

Stephanie Diepeveen, Senior Research Fellow. ODI, & Senior Lecturer, Department of Digital Humanities, King's College, London

Dr Stephanie Diepeveen is a Senior Lecturer at King's College in London's department of Digital Humanities, where her interdisciplinary research examines how digital technologies and data reshape democratic politics, inclusion, and inequalities, with a particular focus on

perspectives from the Global South. Stephanie is currently co-chair of the T20 Taskforce, Inclusive Digital Transformation, under South Africa's G20 Presidency, as well as co-investigator on an ESRC large grant on language, conflict and conflict resolution in Africa, a four-year interdisciplinary project led by the University of Essex.

From 2021 to 2024, Stephanie led the Digital Societies Initiative at ODI, a global affairs think tank, where she conducted research, facilitated convenings, and engaged in policy work on digitalization across politics, gender, humanitarian studies, and social welfare. In 2023, she was also appointed co-chair of the T20 Taskforce, Our Common Digital Future, under India's G20 Presidency. She has co-authored policy briefs for the G20, including Interoperability and Inclusive and Equitable Public Service Delivery (2024) and Mitigating Forms of Exclusion around Digital Public Infrastructure (2023).

Stephanie holds a PhD from the University of Cambridge.

References

Architectural Digest. 2023. "Will Bitcoin and Data Centers Soon Heat Your Home?" *Architectural Digest.* https://www.architecturaldigest.com/story/will-bitcoin-and-data-centers-soon-heat-your-home.

Babalola, Olumide. 2023. "Data Protection Legal Regime and Data Governance in Africa: An Overview." In *Springer eBooks*, 71–96. https://doi.org/10.1007/978-3-031-24498-8_4.

Birch, Kean, D.T. Cochrane, and Callum Ward. 2021. *Data as Asset? The Measurement, Governance, and Valuation of Digital Personal Data by Major Technology Firms.* Big Data & Society. https://doi.org/10.1177/20539517211017308.

Center for AI and Digital Policy. 2023. "G7 and the Future of Digital Governance." *CAIDP.* https://www.caidp.org/resources/g7/.

Centre for Information Policy Leadership (CIPL). 2023. "Data Localization and Government Access to Data Stored Abroad." *CIPL, TLS.* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_ii_data_localization_and_government_access_to_data_stored_abroad__29_march_2023__2_.pdf.

Center for Strategic & International Studies. 2023. "Advancing Data Governance in the G7." *CSIS.* https://www.csis.org/analysis/advancing-data-governance-g7.

European Data Protection Board (EDPB). *EDPB Annual Report 2023.* Accessed January 18, 2025. https://www.edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2023_en.

IBM Policy Lab. 2023. "Japan's Data Governance Leadership in the G7." *IBM Policy.* https://www.ibm.com/policy/japan-data-g7/.

Marelli, Luca, Giuseppe Testa, and Ine Van Hoyweghen. 2021. Major Technology Firms Platforms in Health Research: Re-Purposing Big Data Governance in Light of the General Data Protection Regulation (GDPR). https://doi.org/10.1177/20539517211018783.

Micheli, Marina, Marisa Ponti, Max Craglia, and Anna Berti Suman. 2020. "Emerging Models of Data Governance in the Age of Datafication." *Big Data & Society* 7 (2). https://doi.org/10.1177/2053951720948087.

Mishra, Neha. 2016. *Data Localization Laws in a Digital World: Data Protection or Data Protectionism?* SSRN Electronic Journal. https://ssrn.com/abstract=2848022.

OECD. 2023. The Nature, Evolution, and Potential Implications of Data Localization Measures. OECD Trade Policy Paper No. 278. Paris: OECD Publishing.

Potluri, Sai Rakshith, V. Sridhar, and Shrisha Rao. 2020. *Effects of Data Localization on Digital Trade: An Agent-Based Modeling Approach.* Telecommunications Policy. https://doi.org/10.1016/j.telpol.2020.102022.

Reuters. 2024. "AI Boom Spurs Major Technology Firms to Build Clean Power Sites." *Reuters.* https://www.reuters.com/business/energy/ai-boom-spurs-big-tech-build-clean-power-site-2025-02-05/.

Sustainability Directory. 2023. "Economic Benefits of Sustainable Digital Practices." *Sustainability Directory.* https://sustainability-directory.com/question/what-are-the-economic-benefits-of-sustainable-digital-practices/.

Swire, Peter, DeBrae Kennedy-Mayo, Drew Bagley, Sven Krasser, Avani Modak, and Christoph Bausewein. 2024. *Risks to Cybersecurity from Data Localization: Organized by Techniques, Tactics, and Procedures*. *Journal of Cyber Policy* 9 (1): 20-51. https://doi.org/10.1080/23738871.2024.2384724.

Taylor, Richard D. 2020. *Data Localization: The Internet in the Balance. Telecommunications Policy.* https://doi.org/10.1016/j.telpol.2020.102003.

Voss, W. Gregory. 2020. *Cross-Border Data Flows, the GDPR, and Data Governance. International Data Privacy Law.* https://ssrn.com/abstract=3629348.

Walther, Cornelia C. 2024. "The New UN Global Digital Compact. What It Is, and Why We Matter." *Forbes*. September 22, 2024. https://www.forbes.com/sites/corneliawalther/2024/09/22/the-new-un-global-digital-compact-what-it-is-and-why-we-matter/.