

Delegation from the United States of America

Adithi S., Madhav T., Mitansh K. & Vineeth B.

March 2025

The following agenda is under the purview of the General Assembly: extending the framework of European data governance – the General Data Protection Regulation (GDPR), the Data Governance Act (DGA), and the twin Digital Services Act (DSA) and Digital Markets Act (DMA) – to a global scale. The United States of America recognizes the merit of this proposal and looks forward to engaging in meaningful discussions.

The European Union has introduced a comprehensive data governance framework that is reshaping policies beyond the borders of its internal market. Major international companies, many of them American, have adapted their operations worldwide to comply with EU standards, underscoring the framework's global impact. Washington recognizes the dire need to protect personal privacy, autonomy and freedom, but asserts that such one-size-fits-all regulations host the potential to hamper innovation, create barriers to trade and affect US national security.

The United States hosts apprehensions on globalizing the EU's framework wholesale and grounds its position on three key considerations. First, it emphasizes its capacity to fragment international markets and impose heavy compliance costs on businesses [1], with disproportionate effects on American companies. Second, it recognizes that divergent privacy interpretations across jurisdictions threaten to chill the free flow of data that underpins billions in transatlantic digital trade. Lastly, it notes potential national security implications resulting from constrained law enforcement and intelligence cooperation [2].

The United States appreciates, and supports, the European benchmarks for privacy and accountability but contends that its global extension poses complex challenges for innovation, security, and open commerce that it is keen to address. It prefers a flexible, collaborative approach over a strictly prescriptive regulatory model, relying on industry standards and targeted laws, and hosts a philosophical preference for encouraging technological innovation and entrepreneurship, while addressing privacy risks in context. Washington advocates for interoperable solutions developed through multi-stakeholder processes and voluntary international cooperation; it remains cautious about embracing the rigid global adoption of EU regulations and instead promotes alternative models that safeguard data and enable digital trade.

0.1 Discussion on the General Data Protection Regulation

The General Data Protection Regulation, GDPR, sets obligations for handling personal data by setting ground principles like ‘privacy by design’, ‘transparency’, ‘accountability’, ‘right to erasure’, and means to ensure international data interoperability.

The United States recognizes concerns on the effect of such regulations on the emergence of transformative technologies. Among AI business owners, studies show that approximately 70% of the businesses were required to establish new positions for handling GDPR aspects of their operations. Additionally, many firms have raised concerns about the resource-intensive nature of data deletion requirements [4]. The immutable property of data storage in blockchains poses difficulties to GDPR compliance across various undertakings [5]. Variability of interpretations of privacy by different jurisdictions produces major problems in the operation of data clouds. In addition, Washington also emphasizes that too much regulation would make it more difficult to counter criminal activities [6].

The United States prefers a broader perspective towards data management. Industry-specific and a market-led strategy prove to be better than an overarching policy like GDPR. Washington prefers frameworks like USCMA and IPEF in a bid to maintain privacy and establish high digital standards that match its outlook. For maintaining a robust digital economy, there is a requirement to eradicate the legal ambiguities brought about by the GDPR as far as decisions of adequacy for cross-border data transfers are concerned. There is also a necessity for improved protection to firms so as not to weigh them down with compliance and hefty fines, hence freeing them to innovate, and to guide the world towards a new digital era.

The United States reaffirms its dedication to balancing privacy with speed of innovation by implementing policies like CCPA that puts compliance expense on big businesses and CLOUD Act to enable access to data for protecting national independence. The creation of DOGE seeks to improve interoperability among agency networks and systems [11], advancing the objective of seamless data management.

The United States believes that incentives and diplomatic collaboration are key to fostering a thriving digital economy that upholds privacy rights while enabling innovation.” This is smoother and more cooperative. Achieving this balance requires global cooperation, adaptable regulatory approaches, and respect for national sovereignty rather than a one-size-fits-all regulatory model.

0.2 Discussion on the Data Governance Act

The Data Governance Act (DGA) is designed as a comprehensive framework designed to facilitate secure, efficient, and legally compliant data sharing across sectors.

The United States recognizes the positive impacts of the DGA. The DGA

aims to cultivate a culture of data sharing and reuse, which American companies and researchers view as a valuable goal [14]. However, the United States cares against the overreach of strict regulatory requirements, which may unintentionally hinder innovation and create barriers to entry for non-EU companies [15]. The American Chamber of Commerce to the EU warns of unintended consequences and suggests measures to counter it [14].

The United States aims to ensure against discrimination of American companies with the introduction of new conditions on transferring data to non-EU countries. In addition to such a possibility of a trade barrier, Washington urges the EU to narrowly define ‘highly sensitive’ categories of data, to avoid prevent ambiguity leading to broad localization trends.

The United States believes that data governance should remain open and inclusive. The United States promotes global data governance through coalitions like the APEC CBPR system, which enables voluntary certifications for data flows between economies with interoperable privacy protections between allied nations. Through forums like the OECD and G20, the United States advocates risk-based approaches and mutual recognition of data standards.

The United States contrasts its data governance approach with the more restrictive approaches of certain centralized digital governance models.

A model of ‘cyber sovereignty’ employed by certain governments entails comprehensive state-imposed controls over web access and data flows, which the United States views as restrictive to an open internet. Washington also notes that certain states created challenges for international service providers operating in their regions through controlled internet gateways [18]. The United States suggests that such measures may constrain broader participation in the global digital economy [19].

Earlier, separate ‘Global Initiative on Data Security’ was introduced by such states as an alternative framework, but the United States and its allies raised concerns about its alignment with privacy and openness standards [16] [17].

The United States proposes similar measures such as the Clean Network to enhance digital security in collaboration with like-minded partners, focusing on trusted infrastructure development and effectively establishing criteria that influenced the selection of telecommunications and technology infrastructure providers.

Furthermore, the United States recognizes the possibility that some states may choose to remain independent of any liberal global data governance system. In this situation, Washington says that protecting its own digital networks and important interests is the top priority. This position aligns with its broader commitment to ensuring the security and resilience of the United States digital domain, even if it entails the emergence of a bifurcated internet structure.

0.3 Discussion on the twin Service and Market Acts

The Digital Services Act (DSA) and the Digital Markets Act (DMA) are the regulatory frameworks implemented by the European Union to promote competition and accountability in the digital world.

The United States champions mutual recognition of nations' data protection regimes. It suggests frameworks such as the OECD that work to harmonize privacy and artificial intelligence legislation as well as to balance various approaches in nations. In doing this, the U.S. aims to help facilitate international data governance that is secure and allows the free flow of data across the globe. Similarly, it supports frameworks such as CBPR that are voluntary and dynamic. The U.S. views this model as a way to encourage innovation and regulatory effectiveness without sacrificing national sovereignty.

The United States also notes that although the DSA and DMA are posed as neutral, their application has caught a number of high-profile American firms, such as Google, Apple, Meta, Amazon, and Microsoft. The imposition of "gatekeeper" status on some firms carries specific regulatory responsibilities. Within the scope of trade deals, negotiation over digital policies remains in a perpetual state of transformation.

The United States remains committed to fostering innovation, maintaining economic resilience, and ensuring fair competition in international digital markets.

The United States recognizes the merits of the European data governance framework but asserts that its global adoption presents the risks of stifling innovation, fragmenting trade and introducing excessive compliance burdens. Washington remains steadfast in its commitment to safeguarding privacy and security while ensuring that regulatory frameworks do not hinder technological advancement or economic dynamism. It champions a flexible, risk-based approach that upholds national sovereignty, fosters industry-led standards, and facilitates open digital trade. The United States will continue to advocate for interoperable solutions through strategic cooperation, ensuring that digital governance evolves in a manner that preserves both innovation and economic resilience.

0.4 Citations

- [1] Indo-Pacific Economic Framework and Digital Trade in Southeast Asia
- [2] What is GDPR?
- [3] GDPR and Constraints for AI Startups
- [4] GDPR Right to be Forgotten vs Blockchain
- [5] Fact Sheet: President Donald J. Trump Issues Directive to Prevent the Unfair Exploitation of American Innovation
- [6] EU content law incompatible with US free speech tradition, says FCC's Carr
- [7] US lawmakers rip EU over big tech fines that target American companies
- [8] Donald Trump executive orders signed list
- [9] Executive Order 14158: Establishing and Implementing the President's Department of Government
- [10] Removing Barriers to American Leadership in Artificial Intelligence
- [11] Reforming the U.S. Approach to Data Protection
- [12] Data Governance Act: Position Paper
- [13] China's Evolving Data Governance Regime
- [14] China Data Governance Update
- [15] Key Barriers to Digital Trade
- [16] The Real National Security Concerns over Data Localization