Istituto Affari Internazionali

ISSN 2532-6570

IAI COMMENTARIES 23 | 46 - SEPTEMBER 2023

The EU–US Data Protection Framework: Balancing Economic, Security and Privacy Considerations

by Federica Marconi

The rapid evolution of digital technology has ushered in a data-centric economy, where data accessibility drives marketplace efficiency and economic growth across various industries. However, this shift, while offering numerous benefits, introduces significant privacy and data security challenges, particularly in the context of transatlantic data transfers. Considering the vast economic ties between the EU and the US, the transatlantic data flow vividly illustrates the complexities involved in governing and transferring data. It grapples with the ongoing challenge of striking a satisfactory balance between economic advantages stemming from data utilisation and various concerns pertaining to national security, digital sovereignty and individual rights.

In recent years, the European Commission approved two different frameworks on transatlantic data flow – Safe Harbour in 2000[1] and Privacy Shield in 2016[2] – asserting that the US provided a level of data protection for data transfers essentially equivalent to that guaranteed in the EU. However, despite initial optimism, both adequacy decisions faced a significant setback when the Court of Justice of the European Union invalidated them in what is commonly referred to as the "Schrems saga",[3] named after the

[1] European Commission, *Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce*, http://data.europa.eu/eli/dec/2000/520/oj.

[2] European Commission, *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield*, http://data.europa.eu/eli/dec_impl/2016/1250/oj.

[3] Court of Justice of the European Union (CJEU), *Judgment of the Grand Chamber in Case C-362/14: Maximillian Schrems v. Data Protection Commissioner* [Schrems I], 6 October 2015, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:62014CJ0362; and *Judgment of the Grand Chamber in Case C-311/18: Data Protection Commission v. Facebook Ireland Limited and Maximillian Schrems* [Schrems II], 16 July 2020, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:62018CJ0311.

Federica Marconi is a Researcher in the Multilateralism and Global Governance Programme at the Istituto Affari Internazionali (IAI).

ISSN 2532-6570

Austrian activist who first challenged both frameworks before the European Court. The core arguments centred on the absence of adequate safeguards for personal data within US domestic law and the extent of state surveillance over such data when it was transferred, as initially disclosed by Edward Snowden in 2013.[4]

This legal development led to a period of significant uncertainty and further heightened the ongoing debate concerning the regulation of transatlantic data transfer. To address the consequences of this legal turmoil, both EU and the US committed to establishing "a renewed and sound framework for transatlantic data flows",[5] seeking a long-term solution to address the complexities of data privacy and security, eventually leading to the recently adopted EU–US Data Privacy Framework ("DPF").

Why transatlantic data flows matter

Data flows hold immense significance for the transatlantic economic relationship and impact businesses of all sizes and industries. These data exchanges involve participation from more than 90 per cent of EU businesses that conduct transactions with the US, with a notable 70 per cent being small and medium-sized enterprises.[6] In fact, the volume of transatlantic data flow exceeds that of any other global relationship, contributing to the robust 7.1 trillion US dollars US–EU economic partnership.[7]

Nevertheless, the regulation of data exchange between the EU and the US has been a contentious matter, primarily due to their differing interpretations of fundamental rights and varying data protection standards. In the US, the oversight of how companies handle and secure personal data is predominantly marked by the absence of comprehensive federal legislation. Thus, privacy and data protection regulations vary across industries and are enforced by different agencies, resulting in a diverse and fragmented privacy landscape. In contrast, the EU operates under a comprehensive data protection framework primarily governed by the General Data Protection Regulation (GDPR), which places a strong emphasis on individual rights and imposes stringent obligations on data holders and processors. To this effect, the GDPR unequivocally forbids the transfer of personal data to third countries lacking

[4] Caspar Bowden, *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights*, Brussels, European Parliament, September 2013, https://op.europa.eu/s/y0iF.

[5] European Commission, *Commission Issues Guidance on Transatlantic Data Transfers and Urges the Swift Establishment of a New Framework Following the Ruling in the Schrems Case*, 6 November 2015, https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6015.

[6] DigitalEurope, *Good News for Thousands of Businesses': Reaction to EU Assessment of US Data Protection of Personal Data*, 10 July 2023, https://www.digitaleurope.org/news/good-news-for-thousands-of-businesses-reaction-to-eu-assessment-of-us-data-protection-of-personal-data.

[7] White House, *Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, 25 March 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework.

sufficient data protection measures unless the European Commission issues adequacy decisions certifying whether a country conforms to the requisite standards.

Consequently, discrepancies in data standards have led to uncertainties for economic actors involved in transatlantic economic relations, prompting individual companies to seek ways to align with European requirements and prevent potential GDPR violations. These violations can result in sanctions of up to 4 per cent of the company's annual revenue, as exemplified by several cases involving tech giants: Meta, for instance, received a record-breaking GDPR fine of 1.3 billion US dollars last May – the largest in GDPR history.[8]

Lastly, positioned at the crossroads of data protection, international trade and national security, the topic of transatlantic data flow is intricately linked to the EU's strategy to assert digital sovereignty and secure strategic autonomy. This strategy places a significant emphasis on the localisation and retention of data belonging to European citizens within the EU borders. This approach is driven by the commitment to ensure that data of European citizens remains under the EU's established laws and regulations, which prioritise privacy protection. Consequently, even though the new framework does streamline the transfer of personal data between the EU and the US, it can give rise to concerns about a departure from the EU's broader goals of advancing its digital sovereignty.

Restoring trust in the digital environment

In response to the legal uncertainties stemming from the Court of Justice's decisions, extensive collaboration between the US and the EU resulted in an agreement in principle in 2022. This agreement, endorsed by US President Joe Biden and European Commission President Ursula von der Leyen, reflected the shared commitment to facilitate data flows between both jurisdictions in a manner that protects individual rights and personal data.

Executive Order 14086, titled "Enhancing Safeguards for U.S. Signals Intelligence Activities", was issued by the Biden administration on 7 October 2022. In conjunction with this executive order, US Attorney General Merrick Garland issued a Regulation to establish a Data Protection Review Court.[9] Through these actions, the US committed to introducing additional protective measures aimed at addressing the concerns raised by the Court of Justice regarding mass personal data collection and the lack of objective criteria for limiting access to and utilisation of this data by public authorities.

In the following months, before finalising its adequacy decision on the DPF, the European Commission sought the opinion of the European

[8] European Data Protection Board, *1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision*, 22 May 2023, https://edpb.europa.eu/node/6052.

[9] US Code of Federal Regulation, Part 201: Data Protection Review Court, https://www.ecfr.gov/current/title-28/part-201.

IAI COMMENTARIES 23 | 46 - SEPTEMBER 2023
ISSN 2532-6570

Data Protection Board (EDPB) on the draft decision.[10] The EDPB recognised the improvements brought about by Executive Order 14086, particularly in terms of restricting access to EU data by US intelligence services to what is necessary and proportionate to protect national security. Nevertheless, it expressed several concerns, including those related to inadequate assurances regarding "temporary bulk collection" and the subsequent storage and sharing of data collected in bulk within the US legal framework. Additionally, on 11 May, the European Parliament conveyed its reservations regarding the content of the DPF.[11] While acknowledging that the capacity to transfer personal data across borders has "the potential to be a key driver of innovation, productivity and economic competitiveness", the Parliament underscored the critical necessity for robust safeguards to be firmly established. These safeguards are essential for protecting privacy rights, preventing illegal mass surveillance by the US and restoring the trust of both EU citizens and businesses in digital services, ultimately preserving the vitality of the digital economy. Taking into consideration the CJEU's reasoning in Schrems II, the European Parliament contended that the DPF did not entirely meet EU legal standards due to its lack of an "objective criterion" to validly justify government intrusion into privacy. Consequently, this raised concerns about the possibility of the CJEU invalidating the DPF, as it had done with previous frameworks.

Despite these concerns, on 10 July, the European Commission adopted the adequacy decision on the DPF, confirming that it provided an adequate level of protection for personal data. Consequently, personal data can now move freely from the EU to US companies that have self-certified their adherence to the DPF principles. Ursula von der Leyen stated that the new framework will "ensure safe data flows for Europeans and bring legal certainty to companies on both sides of the Atlantic",[12] while strengthening economic ties and reaffirming shared values. President Joe Biden also welcomed the adequacy decision, emphasising the joint EU–US commitment to robust data privacy protections and foreseeing increased economic opportunities for both jurisdictions and their companies.

Third time's a charm?

On a positive note, the DPF now allows for the transfer of personal data from the EU to the US through a certification system. US companies commit to a set of privacy principles, eliminating the need for additional transfer mechanisms like Standard Contractual Clauses or binding corporate rules, as well as transfer impact assessments.

[10] European Data Protection Board, *Opinion 5/2023 on the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data under the EU-US Data Privacy Framework*, 28 February 2023, https://edpb.europa.eu/node/5132.

[11] European Parliament, *Resolution of 11 May 2023 on the Adequacy of the Protection Afforded by the EU-US Data Privacy Framework*, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html.

[12] European Commission, *Data Protection: European Commission Adopts New Adequacy Decision for Safe and Trusted EU-US Data Flows*, 10 July 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

ISSN 2532-6570

Companies are required to complete their self-certification by October 2023 to be included on the DPF List, maintained by the US Department of Commerce. Additionally, the DPF introduces various safeguards, such as restricting US surveillance access to data that is "necessary and proportionate" for national security, the establishment of a Data Protection Review Court to address concerns about access to personal data by US intelligence agencies and mandating US companies to delete personal data when it is no longer needed for the original purpose of collection.

Despite significant progress, however, the path towards establishing a stable and reliable framework for transatlantic data transfers remains fraught with difficulties. Persistent concerns revolve around how the US will interpret the concept of "proportionate" access to data by US authorities and its adherence to the CJEU's criteria.

Moreover, there are concerns about the Data Protection Review Court's composition: while made up of members from outside the US government, there are doubts about its appointment process, leading to potential issues with fair and transparent decision-making. Furthermore, the European Parliament has highlighted an additional weakness in the framework, which lies in its failure to address data accessed by public authorities through alternative avenues.[13] This includes methods such as the US Cloud Act or the US Patriot Act, data acquisition through commercial transactions or voluntary data sharing agreements.

Privacy activist Max Schrems argues that the new framework is "largely a copy" of previous ones.[14] The US Department of Commerce also considers that it "does not create new substantive obligations for participating organizations with regards to protecting EU personal data" and "[t]he privacy principles and the process to initially self-certify and annually re-certify remain substantively the same".[15] Moreover, Schrems stresses that substantial changes in US surveillance law are needed for true effectiveness and has signalled his intention to bring "the new deal back before the CJEU".[16]

A legal challenge has therefore been announced, possibly reaching the CJEU by late 2023 or early 2024 which may result in a temporary suspension of the DPF. While EU Justice Commissioner Didier Reynders remains confident in the framework's resilience against legal challenges, many companies are choosing to stick with EU-approved standard contractual clauses to maintain GDPR compliance, despite the associated challenges and expenses, in the face of ongoing risks and uncertainties.

[13] European Parliament, *Resolution of 11 May 2023*, cit.

[14] NOYB, *European Commission Gives EU-US Data Transfers Third Round at CJEU*, 10 July 2023, https://noyb.eu/en/node/1324.

[15] Data Privacy Framework Program website: *FAQs - EU-U.S. Data Privacy Framework (EU-U.S. DPF)*, last updated 17 July 2023, https://www.dataprivacyframework.gov/s/article/FAQs-EU-U-S-Data-Privacy-Framework-EU-U-S-DPF-dpf.

[16] NOYB, *European Commission Gives EU-US Data Transfers Third Round at CJEU*, cit.

ISSN 2532-6570

Striking the delicate balance between privacy concerns, free trade imperatives and national security interests within the realm of data remains a formidable challenge, although recent trends around transatlantic data flows are encouraging. The Schrems saga has vividly highlighted the imperative to bridge legal disparities between the EU and the US, emphasising the importance of creating a digital international environment founded on trust, cooperation and regulatory alignment.

19 September 2023

ISSN 2532-6570

ISSN 2532-6570

IAI COMMENTARIES 23 | 46 - SEPTEMBER 2023

Istituto Affari Internazionali (IAI)

The Istituto Affari Internazionali (IAI) is a private, independent non-profit think tank, founded in 1965 on the initiative of Altiero Spinelli. IAI seeks to promote awareness of international politics and to contribute to the advancement of European integration and multilateral cooperation. Its focus embraces topics of strategic relevance such as European integration, security and defence, international economics and global governance, energy, climate and Italian foreign policy; as well as the dynamics of cooperation and conflict in key geographical regions such as the Mediterranean and Middle East, Asia, Eurasia, Africa and the Americas. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*AffarInternazionali*), two book series (*Global Politics and Security* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via dei Montecatini, 17
I-00186 Rome, Italy
Tel. +39 066976831
iai@iai.it
www.iai.it

Latest IAI COMMENTARIES

Editor: Leo Goretti (l.goretti@iai.it)