Articles + Publications | December 7, 2023

New Mechanism for Cross-Border Data Transfer: The EU-U.S. Data Privacy Framework

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Nick Elwell-Sutton

RELATED OFFICES

Hartford | London

On June 10, 2023 the European Commission (the "Commission") issued an adequacy decision on the new EU-U.S. Data Privacy Framework (the "DPF"). The decision restored free transfer of data between the EU and U.S. after three years of uncertainty following the *Schrems I* and *Schrems II* decisions, which overturned the preceding Safe Harbor Framework of 2000 and 2016 Privacy Shield.

The DPF (i) reinstated a mechanism for cross-border transfer of personal data, (ii) introduced more extensive limitations on U.S. surveillance agencies' access to EU data beyond what is "necessary and proportionate," and (iii) established an independent dispute resolution mechanism for EU citizens.

International data transfers can resume under the DPF because the adequacy decision deemed the level of data protection for personal data provided by the U.S. comparable to that of the EU. Although the decision now provides enough latitude for international tech companies to continue the flow of over $1 trillion in trade and investment between the EU and U.S.?, it faces rigorous scrutiny from privacy advocates who will seek to have the DPF struck down once again in the Court of Justice of the European Union ("CJEU").

Opposition to the DPF

Legal challenges to the DPF from privacy advocates are already in motion. The CJEU will be responsible for reviewing the Commission's adequacy decision and resolving challenges to the constitutionality of the new Framework. These challenges will likely focus on the CJEU's interpretation of the EU Charter of Fundamental Rights, which limits government surveillance to "what is necessary in a democratic society".

The Commission's 2023 decision is the latest development in a decade-long public policy discourse to determine what constitutes ethical transatlantic data transfer practices, reconciling the stark differences between EU and U.S. data privacy regimes. The Edward Snowden leaks in 2013 began a line of CJEU cases involving the U.S. that address this discourse, including *Schrems I* and *Schrems II*. These cases compared the U.S. limits on surveillance of data that originates outside of the U.S. against the protections afforded to citizens by the EU. In both cases, the CJEU rejected the Commission's adequacy decision for failing on its face to ensure democratic safeguards against surveillance as required by the EU.

As these CJEU cases unfolded, the U.S. repeatedly modified its intelligence law and procedure in response, including increasing transparency about intelligence-gathering in 2013 and extending additional international safeguards against surveillance under former President Barack Obama's January 2014 Presidential Policy Directive. Further, after the CJEU invalidated the Safe Harbor Framework in *Schrems I*, the U.S. created a mechanism for EU residents to complain to the State Department as part of the 2016 Privacy Shield.

The 2016 Privacy Shield provided a mechanism for EU-U.S. data transfers from 2016 until the CJEU declared it invalid in 2020. The CJEU's decision invalidating Privacy Shield relied primarily on the extent of U.S. surveillance of individuals located outside the United States under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), and Executive Order 12333, signed by President Reagan in 1981. Specifically, the CJEU determined that U.S. surveillance under Section 702 and Executive Order 12333 is not limited to what is "strictly necessary" and does not "lay down clear and precise rules" that "impos[e] minimum safeguards" to protect personal data.

These decisions had potentially catastrophic results for U.S. businesses operating within the EU. International tech giants, including Meta, mounted vigorous opposition against the ruling, and publicly ?contemplated shutting down Facebook and Instagram from Europe if privacy restrictions were not ?relaxed. ?

Max Schrems, who initiated the two earlier challenges against the Safe Harbor Framework and the 2016 Privacy Shield, has already announced plans to challenge the 2023 adequacy decision, stating the DPF is nothing more than a "copy" of the Privacy Shield: ?"We currently expect this to be back at the Court of Justice by the beginning of next year," ?Schrems said in a press statement following publication of the most recent adequacy decision.

The 2023 EU-U.S. Data Privacy Framework: What is New?

Despite Schrems' assertion, the Commission's decision holds that the DPF increases standards for both the procedural protections that govern U.S. Foreign intelligence and the implementation of these procedures in intelligence operations, as informed by the deficiencies in the 2016 Privacy Shield identified by *Schrems II*.

?The DPF provides EU individuals whose data would be transferred to participating ?companies in the U.S. with several new rights (e.g. to obtain access to their data, or obtain ?correction or deletion of incorrect or unlawfully handled data). Additionally, the DPF specifically institutes measures to address the following deficiencies identified in the CJEU's 2020 judgment: (a) overly broad grounds for surveillance and restrictions on the scope of surveillance to meet the EU requirement of "necessity and proportionality" and (b) insufficiently independent mechanisms for individual Europeans to seek "redress" relating to surveillance.

Representatives from the EU and U.S. have each implemented measures to address these requirements within the context of their laws and systems of government, arriving at a heightened understanding of the interplay between their respective privacy law regimes and democratic norms regarding allowing government surveillance of domestic and international individuals.

In Executive Order 14086, the U.S. (i) created additional specifications to limit the acceptable grounds for collection enumerated in the FISA to what is "necessary and proper"; (ii) placed heightened prerequisites to authorize "bulk surveillance" by the government; and (iii) established an independent and impartial redress mechanism, which includes a Data Protection Review Court administered by the Justice Department, to provide

an independent avenue of redress for European citizens. Moreover, the order also broadens the scope of these restrictions to include signals intelligence conducted under presidential powers over national security and foreign relations pursuant to Executive Order 12333, which is not subject to the FISA. These measures are more concrete than the measures enacted by the 2014 Presidential Policy Directive and, thus, are more likely to withstand scrutiny by the CJEU.

Compliance Considerations for U.S. Businesses

U.S. companies may continue cross-border data transfers by opting into the EU-U.S. Data Privacy Framework. To opt in, companies must commit to ?comply with a detailed set of privacy obligations, such as purpose limitation, data minimization and data retention, as well as specific obligations concerning data security and the sharing of data with third parties. Only organizations that are subject to the jurisdiction of the U.S. Federal Trade Commission or Department of Transportation are eligible to self-certify, notably this excludes financial services businesses. Significantly, the DPF *does not* apply to many banking, insurance and other companies outside the jurisdiction of the FTC and DOT.

Private U.S. companies may self-certify their participation in the Framework through an online form administered by the Department of Commerce, which processes ?applications for certification and monitors whether participating companies continue to meet the ?certification requirements. Compliance by U.S. companies with their obligations under the EU-?U.S. Data Privacy Framework will be enforced by the U.S. Federal Trade Commission.?

Because the U.K. is no longer a member of the EU, the Adequacy Decision in respect of the DPF does not extend to personal data transferred from the U.K. to the U.S., but in a parallel approval process the U.K. government approved an extension (known as the U.K. Data Bridge) taking effect from 12 October 2023?. U.S. business may also opt-into the UK Data Bridge through the Department of Commerce's online form.

For more on the UK Data Bridge, see U.S.-U.K. Data Transfer Developments.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber