Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

The EU-U.S. Data Privacy Framework: Background, Implementation, and Next Steps

October 24, 2022

On October 7, 2022, President Biden signed and issued the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities (the Data Protection EO or the EO). The Data Protection EO is the latest U.S. action to implement the new European Union (EU)-U.S. Data Privacy Framework (Data Privacy Framework), which the United States and the EU negotiated to replace the former EU-U.S. Privacy Shield Framework (Privacy Shield). The new Data Privacy Framework and the EO implementing it are key pieces to facilitate transatlantic data flows and enable U.S. companies to comply with EU data protection law while still being subject to U.S. foreign intelligence surveillance laws. This Legal Sidebar explains the circumstances leading to the development of the Data Privacy Framework, U.S. steps to implement the framework, and issues of possible interest to Congress.

Background

In 2018, the EU enacted the General Data Protection Regulation (GDPR), an update to its 1995 Data Protection Directive that imposes obligations for handling personal data in the EU. Among the GDPR's proscriptions are limits on when personal data may be transferred to countries outside the EU. Under Article 45 of the GDPR, an entity may transfer EU personal data to a foreign country that the European Commission has determined ensures an "adequate level of protection" for personal data. The European Commission has recognized 14 different jurisdictions as providing an adequate level of protection to satisfy Article 45. Transfers to a country that does not provide an adequate level of protection may still be lawful under the GDPR: Articles 46 and 49 define the situations in which an entity may transfer EU personal data to a country that has not been deemed adequate.

The United States has attempted to meet Article 45's standard by developing data protection frameworks in coordination with the EU. Privacy Shield provided a mechanism for EU-U.S. data transfers from 2016 until the Court of Justice of the European Union (CJEU) declared it invalid in 2020. Under Privacy Shield, participating commercial entities transferring personal data from the EU to the United States had a number of data protection obligations, including adherence to seven data protection principles and annually self-certifying adherence to these principles to the Department of Commerce. 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),

Congressional Research Service
https://crsreports.congress.gov
LSB10846

enacted in 2008, 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. The CJEU additionally held that EU individuals whose data is collected by U.S. surveillance do not have an adequate administrative or judicial remedy for unlawful use of their data. For a detailed discussion of the decision invalidating Privacy Shield, see this CRS Report. For more on Privacy Shield and EU-U.S. data flows generally, see this CRS Report.

After nearly two years of negotiations, the United States (as represented in negotiations by the Department of Commerce) and the European Commission (the EU's executive, responsible for negotiating on behalf of the EU) announced an agreement in principle in March 2022 outlining a new framework—the Data Privacy Framework—that would replace Privacy Shield. A fact sheet released by the White House summarized the U.S. commitments under this framework, focusing on the government's responsibilities to strengthen privacy safeguards relating to surveillance activities. The fact sheet suggested that the Data Privacy Framework would not displace Privacy Shield's obligations for commercial entities. For more background, see this CRS In Focus.

Implementation of the EU-U.S. Data Privacy Framework

The Data Protection EO, titled "Enhancing Safeguards for United States Signals Intelligence Activities," attempts to address the CJEU's criticisms of Privacy Shield: namely, that U.S. surveillance does not have adequate data protection safeguards and does not provide an adequate legal remedy for non-U.S. individuals whose personal data has been unlawfully obtained. The Data Protection EO creates obligations for all executive agencies involved in signals intelligence activities to conduct such activities only in pursuit of twelve defined "legitimate objectives" and only as necessary to advance such objectives. The EO also lists four "prohibited objectives": suppressing criticism or dissent; suppressing privacy interests; suppressing a right to legal counsel; and disadvantaging individuals based on ethnicity, race, gender, gender identity, sexual orientation, or religion. The EO also directs agencies to limit "bulk" surveillance and to limit the dissemination and retention of personal data obtained through surveillance. The Data Protection EO prescribes oversight responsibilities for intelligence agencies, requiring each agency to have an officer responsible for assessing compliance with the EO and other applicable U.S. law. These requirements may be responses to the CJEU's concern that laws authorizing U.S. surveillance do not "indicate in what circumstances and under which conditions" personal data may be collected or provide "minimum safeguards" for the protection of personal data.

The Data Protection EO also establishes a redress mechanism to allow individuals to challenge unlawful surveillance practices. Under the EO, individuals may submit complaints to the Director of National Intelligence's Civil Liberties Protection Officer (CLPO), who is directed to investigate and, if necessary, remediate complaints. The EO directs the Attorney General to establish a "Data Protection Review Court" through which an individual may seek review of the CLPO's disposition of their complaint. If the Data Protection Review Court disagrees with the CLPO's determination, it may order remediation on its own. In contrast to the Foreign Intelligence Surveillance Court, a judicial body with jurisdiction over surveillance applications brought under Section 702 of FISA, the judges of the Data Protection Review Court are not to be federal judges. The EO requires that judges on the court be selected by the Attorney General from "legal practitioners with appropriate experience in the fields of data privacy and national security law" who are not U.S. government employees and, for the time of their tenure on the court, have no other government duties. The selection criteria for the court's judges may be intended to address the CJEU's concerns that the reviewing entity under Privacy Shield, a State Department official known as the Privacy Shield Ombudsperson, was insufficiently independent from the United States government. The National Security Division of the Department of Justice (DOJ) issued regulations establishing the Data Protection Review Court shortly after the White House announced the EO.

As discussed in this CRS Report, executive orders have the force of law when they rely on a constitutional or statutory power granted to the President. The Supreme Court has understood the President to be responsible for overseeing the foreign relations of the United States. Additionally, the National Security Act of 1947 provides expansive power to the President to supervise intelligence activities. President Reagan relied on this supervisory authority in issuing Executive Order 12333.

Next Steps

The CJEU's decision invalidating Privacy Shield made transfers of EU data to the United States unlawful under the GDPR, unless those transfers relied on the provisions of Articles 46 or 49. The EO and DOJ regulations creating the Data Protection Review Court are necessary steps in the implementation of the new Data Privacy Framework, but several steps remain before commercial entities may rely on the Framework. One outstanding question is what exact obligations will govern commercial entities. As discussed above, because the CJEU's decision rejecting Privacy Shield relied on the insufficiency of safeguards in connection with U.S. intelligence operations, rather than the obligations imposed on commercial entities, Privacy Shield's obligations will likely remain in place for commercial participants: the White House and Department of Commerce have both indicated as much.

On the EU side, the European Commission must determine that the new framework provides an adequate level of protection. A Q&A published by the European Commission lays out the exact steps in this process in more detail, noting that the Commission will adopt a final adequacy decision only after it and several other EU institutions review and approve the framework.

If the European Commission determines that the new framework provides an adequate level of protection to comply with European data protection law, its decision may face legal challenges in EU courts. Maximillian Schrems, the Austrian privacy activist who brought the challenge that led to the CJEU's invalidation of Privacy Shield (and also successfully challenged Privacy Shield's predecessor before the CJEU), issued a preliminary statement through his organization that the EO is "unlikely to satisfy EU law." According to the European Commission's Q&A, the Commission believes the EO's safeguards and redress mechanism appropriately address the CJEU's concerns.

Considerations for Congress

The EO and implementation of the new Data Privacy Framework may raise several issues of potential congressional interest. One issue may be whether Congress wishes to act to authorize U.S. participation in the Framework, given the importance of transatlantic data flows to U.S.-EU trade and economic relations. Presidents may revoke executive orders, and any possible future revocation of the Data Protection EO could leave EU persons without the EO's data protection safeguards and recourse mechanisms. Because the CJEU's decision invalidating Privacy Shield rested on the lack of adequate safeguards and legal recourse, revoking the EO could threaten the viability of the new Data Privacy Framework. Congress could attempt to provide these safeguards through legislation.

A separate but related issue is that the CJEU may determine that the safeguards provided for in the EO are insufficient to assuage the court's concerns with U.S. surveillance. If the CJEU determines that U.S. surveillance as authorized by Section 702 of FISA does not satisfy EU data protection law, even with the EO's safeguards in place, ensuring the legality of EU-U.S. data flows may require amending FISA. Section 702 of FISA is scheduled to expire at the end of 2023. As discussed in this Legal Sidebar, Members of Congress have used past FISA reauthorizations to propose broader reforms to the law.

Author Information

Eric N. Holmes
Legislative Attorney

Disclaimer