Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated June 2, 2022

U.S.-EU Trans-Atlantic Data Privacy Framework

In March 2022, the United States and the European Union (EU) announced a political agreement on a new Trans-Atlantic Data Privacy (TADP) Framework to safeguard commercial cross-border data flows. For decades, data privacy and protection issues have been sticking points in U.S.-EU relations. The new framework aims to meet EU data protection obligations and facilitate transatlantic trade.

Data Transfers and Surveillance Issues

The EU considers the privacy of communications and the protection of personal data to be fundamental rights, codified in EU law, while U.S. federal policy protects certain data on a sectoral basis. Over the years, the United States and the EU have concluded several data transfer agreements (both in the commercial and law enforcement sectors) that sought to address EU concerns about U.S. data protection practices. Despite U.S. assurances, many in the EU have remained uneasy about U.S. intelligence and surveillance laws and possible U.S. government access to EU citizens' personal data. Resulting tensions and legal challenges have impacted U.S.-EU data transfer accords, threatening bilateral trade for U.S. and EU businesses, and raising congressional concerns.

EU Court Invalidates Privacy Shield

Before the new TADP Framework was announced, the Court of Justice of the European Union (CJEU, also known as the European Court of Justice, or ECJ) had invalidated two U.S.-EU commercial data transfer accords, most recently the Privacy Shield Framework in July 2020. Since 2016, Privacy Shield had provided a mechanism to transfer EU citizens' personal data to the United States while complying with EU data protection rules. Privacy Shield sought to address concerns raised in a 2015 CJEU decision that struck down a similar U.S.-EU data transfer accord, the Safe Harbor Agreement. Privacy Shield also was crafted in anticipation of the EU's General Data Protection Regulation (GDPR), which took effect in May 2018, and created new individual rights and requirements for data protection throughout the EU. Nevertheless, the CJEU found that Privacy Shield failed to meet EU data protection standards given the breadth of U.S. data collection powers authorized in U.S. electronic surveillance laws and the lack of redress options for EU citizens. The CJEU ruling also increased due diligence requirements for data exporters using another EU mechanism—standard contractual clauses (SCCs)—to transfer personal data to the United States.

At the time of its invalidation in 2020, Privacy Shield had 5,380 participants, including U.S. businesses and other organizations, U.S. subsidiaries in Europe, and 250 entities headquartered in Europe. The CJEU ruling created legal uncertainty for many firms engaged in transatlantic trade, both those that relied on Privacy Shield (over 75% of which were small and mid-sized firms, SMEs) and those using SCCs, including many large multinational companies.

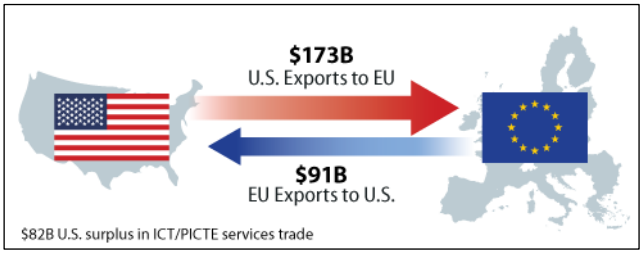
U.S. and Congressional Interests

Many Members of Congress urged the United States and the EU to reach a successor accord to Privacy Shield to guarantee cross-border data flows and protect U.S. business interests. Data flows underlie much of the $7.1 trillion U.S.-EU economic relationship. Some companies, including Facebook's parent company, Meta, raised the potential of withdrawing from the EU market if a new transatlantic data flow agreement could not be reached. The demise of Privacy Shield thus reinforced concerns among some in Congress that the EU approach to data protection creates unfair trade barriers and limits U.S. firms' access to the EU market. Congress may be interested in evaluating the TADP Framework, including its ability to ensure continued data flows for U.S. companies and organizations, its potential implications for U.S. national security, or the extent to which the TADP and U.S.-EU cooperation helps to set international privacy standards and counter China's influence on digital issues globally.

Transatlantic Data Flows

According to the U.S. Bureau of Economic Analysis, the United States and Europe are each other's most important commercial partners for digitally-enabled services. U.S.-EU trade of information and communications technology (ICT) services and potentially ICT-enabled services was over $264 billion in 2020 (see **Figure 1**). Transatlantic data flows account for more than half of Europe's data flows and about half of U.S. data flows globally. Such data flows enable people to transmit information for online communication, track global supply chains, share research, provide cross-border services, and support technological innovation, among other activities. Organizations may use customer or employee personal data to facilitate business transactions, analyze marketing information, discover fraudulent payments, improve proprietary algorithms, or develop competitive innovations.

Figure 1. U.S.-EU Trade of ICT and Potentially ICT-Enabled (PICTE) Services, 2020



Source: CRS with data from the Bureau of Economic Analysis.

The TADP Framework

In announcing the "deal in principle" on the TADP Framework, the Biden Administration and the European Commission (the EU's executive, responsible for negotiating on behalf of the EU) asserted that the agreement

"reflects the strength of the enduring U.S.-EU relationship." U.S. and European Commission negotiators are working to flesh out the details of the new framework and translate the agreed arrangements into official texts. U.S. commitments are to be formalized in an executive order, signed by the President (congressional approval would not be necessary). The EU would then need to review the official texts before granting final approval of the framework.

Key Provisions

Participating companies and organizations that take advantage of the TADP Framework to protect data flows would continue to be required to adhere to the Privacy Shield Principles and to self-certify through the U.S. Department of Commerce (Commerce). The seven distinct privacy principles include notice; choice; accountability for onward data transfer; security; data integrity and purpose limitation; access; and recourse, enforcement, and liability. Privacy Shield also set out 16 mandatory supplemental principles that included provisions on sensitive data, secondary liability, the role of data protection authorities (DPAs), human resources data, pharmaceutical and medical products, and publicly available data; the new framework is expected to contain these supplemental principles.

To address EU concerns about U.S. surveillance practices, the new framework would increase safeguards and limits on U.S. signals intelligence activities, establish a new redress mechanism with independent and binding authority (the Data Protection Review Court), and add oversight procedures for signals intelligence activities. Press reports suggest a new unit under the U.S. Department of Justice may oversee surveillance of EU persons.

Program Enforcement

The new TADP program would continue to be administered by Commerce and the European Commission. Commerce would monitor firms' effective compliance and investigate complaints. The U.S. Federal Trade Commission (FTC) and the U.S. Department of Transportation would continue to enforce compliance. In June 2020, FTC reported enforcement actions against dozens of companies that made false or deceptive representations about Privacy Shield participation. The FTC's $5 billion penalty against Facebook included holding executives accountable for privacy-related decisions and prohibiting misrepresentations related to Privacy Shield.

Future Prospects

EU officials hope that the new TADP Framework will be finalized and adopted by the end of 2022. Implementation of the new framework may alleviate prior uncertainty created by the CJEU ruling on the former Privacy Shield, but stakeholders will be closely monitoring future enforcement. Potential new legal challenges brought by EU privacy advocates could test the agreement's durability.

Apart from the new framework, U.S. firms have limited options for cross-border data flows with the EU. They include

- Create Binding Corporate Rules (BCRs) that EU officials must approve on a firm-by-firm basis;
- Implement updated EU-approved SCCs and reassess for adequate safeguards according to the CJEU ruling;
- Use commercial cloud services provided by large technology firms that use approved BCRs or updated SCCs (e.g., Microsoft, IBM);
- Store EU citizens' personal data only in the EU or other approved country, an idea advocated by some European DPAs and other stakeholders, but which others view as potential costly data localization trade barriers;
- Obtain consent from individuals for every single transfer of personal data, a likely logistically challenging and costly option for most entities;
- Exit or limit participation in the EU market.

Other alternatives would be for the EU to establish codes of conduct or certifications that meet GDPR requirements, for which organizations could apply. These programs could be U.S.-EU specific or at a broader, global level.

Other international forums and agreements may affect U.S.-EU data flows. In April 2022, the United States and six partners announced the establishment of the Global Cross-Border Privacy Rules (CBPR) to promote interoperability and help bridge different regulatory approaches globally. It is not clear if the Global CBPR system would meet EU legal obligations. Digital trade negotiations at the World Trade Organization also include discussions on cross-border data flows, and law enforcement access to data is a topic of negotiations at the Organization for Economic Co-operation and Development. Data flows and privacy are not included, however, under the U.S.-EU Trade and Technology Council, because the EU views data protection as a fundamental right not open for negotiation in trade discussions.

Issues for Congress

Congressional action in several areas could shape the future landscape for U.S.-EU data transfers. For example

- Exploring changes when authorizing and overseeing surveillance programs to better protect data privacy or otherwise address EU concerns;
- Considering comprehensive federal privacy legislation that includes data protection provisions that may align to some extent with GDPR requirements, to provide some level of certainty to EU businesses and individuals;
- Examining how best to achieve broader consensus on data flows and privacy at the global level, cooperate with the EU and other like-minded partners on alternatives to counter China's influence in the digital space, and hold hearings on U.S. engagement in ongoing bilateral and multilateral digital trade negotiations.

Also see CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick; CRS Report R46724, *EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield*, by Chris D. Linebaugh and Edward C. Liu, and CRS Report R45584, *Data Flows, Online Privacy, and Trade Policy*, by Rachel F. Fefer.

Rachel F. Fefer, Analyst in International Trade and Finance
Kristin Archick, Specialist in European Affairs

Disclaimer