Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated July 17, 2020

EU Data Protection Rules and U.S. Implications

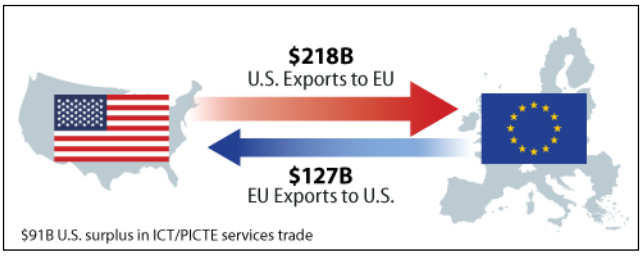
Data Privacy and Protection in the United States and Europe

U.S. and European Union (EU) policymakers are focused on protection of personal data online with recent and proposed legislation and enforcement actions. Data breaches at companies such as Facebook, Apple, and Marriott have contributed to heightened public awareness. The EU's General Data Protection Regulation (GDPR)—which took effect on May 25, 2018—has drawn the attention of Congress, U.S. businesses and other stakeholders, prompting debate on U.S. federal and state data privacy and protection policies.

Both the United States and the 27-member EU assert that they are committed to upholding individual privacy rights and ensuring the protection of personal data, including electronic data. Differences in U.S. and EU approaches to data privacy and protection, however, have long been sticking points in U.S.-EU economic and security relations. The GDPR highlights some of those differences and poses challenges for U.S. companies doing business in the EU. Although no longer a member of the EU, the United Kingdom (UK) remains bound by GDPR through 2020 and intends to incorporate GDPR into UK data protection law.

The U.S. does not broadly restrict cross-border data flows and has traditionally regulated privacy at a sectoral level to cover certain types of data. The EU considers the privacy of communications and the protection of personal data to be fundamental rights, which are codified in EU law. The EU regards current U.S. data protection safeguards as inadequate. Since 2000, many entities used U.S.-EU negotiated agreements for cross-border data flows, but the EU's top court has invalidated successive accords due to concerns about U.S. surveillance laws (most recently, striking down Privacy Shield in July 2020).

Figure 1. U.S.-EU Trade of ICT and Potentially ICT-Enabled (PICTE) Services, 2018



Source: Bureau of Economic Analysis interactive data Table 3.3.

The transatlantic economy is the largest in the world, with goods and services trade of $1.3 trillion in 2019; the UK accounted for 20%. U.S.-EU trade of information and communications technology (ICT) services and potentially ICT-enabled services, including the UK, was over $345 billion in 2018 (see **Figure 1**).

What Is the GDPR?

The GDPR establishes a set of rules for the protection of personal data throughout the EU to strengthen individual rights and facilitate business. The EU hopes the GDPR will further develop the EU's Digital Single Market (DSM), aimed at increasing harmonization across the bloc on digital policies. The EU also views the GDPR as underpinning efforts to foster the EU's digital transformation and bolster the EU's technology sector vis-à-vis Chinese and U.S. competitors, while protecting European values.

The GDPR identifies legitimate bases for data processing and sets out common rules for data retention, storage limitation, and record keeping. The GDPR applies to (1) all businesses and organizations with an EU establishment that process (perform operations on) personal data of individuals (or "data subjects") in the EU, regardless of where the actual processing of the data takes place; and (2) entities outside the EU that offer goods or services (for payment or for free) to individuals in the EU or monitor the behavior of individuals in the EU. Processing certain sensitive personal data is generally prohibited.

Stronger and new data protection requirements in the GDPR grant individuals the right to:

- Receive clear and understandable information about who is processing one's personal data and why;
- Consent affirmatively to any data processing;
- Access any personal data collected;
- Rectify inaccurate personal data;
- Erase one's personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data (the "right to be forgotten");
- Restrict or object to certain processing of one's data;
- Be notified without "undue delay" of a data breach if there is a high risk of harm to the data subject; and
- Require the transmission of one's data to another controller (data portability).

A company or organization can be fined up to 4% of its annual global turnover or €20 million (whichever is greater) for noncompliance. Fines are assessed by the national supervisory authority (a Data Protection Authority, or DPA) in each member state and subject to appeal in national courts. The GDPR also requires some companies to hire data protection officers.

GDPR Implementation

Many U.S. firms have made changes to comply with the GDPR, such as revising and clarifying user terms of agreement and asking for explicit consent. While it creates more requirements on companies that collect or process data, some experts contend that the GDPR may simplify compliance for U.S. firms because the same set of data

protection rules apply across the EU. Also, companies established in the EU that engage in cross-border data processing primarily only have to liaise with the DPA of the EU country where the firm is based (the "lead" authority), possibly decreasing administrative costs. However, a firm is still subject to oversight and enforcement by the DPA of every country where it does business. Some member states and privacy activists have criticized the system as many of the largest digital firms are based in a few countries and overseen by those states' DPAs, creating enforcement delays and logjams due to limited resources.

U.S. firms have voiced several concerns about the GDPR, including the need to construct a compliance bureaucracy and possible high costs for adhering to the GDPR's requirements. While large firms have the resources to hire consultants and lawyers, it may be harder and costlier for small and mid-sized enterprises (SMEs) to comply, possibly deterring them from entering the EU market and creating a de facto trade barrier. Some U.S. businesses, including several newspaper websites and digital advertising firms, opted to exit the EU market rather than confront the complexities of GDPR. Some industry surveys show that GDPR's restrictions on the use and sharing of data may be limiting the development of new technologies and deterring potential mergers and acquisitions.

Although the GDPR is directly applicable in EU member states, implementing legislation is required to enact certain parts of the GDPR (e.g., appointment of a supervisory authority; ability to levy penalties). Critics note that the GDPR permits diverging national legislation in specified areas (e.g., employment data) and contend that this could lead to uneven implementation or enforcement.

U.S.-EU Data Flows and GDPR

To transfer personal data outside the EU, a firm must comply with GDPR by transferring data (1) to a country the EU deems has adequate data protection, (2) through EU-approved standard contractual clauses (SCCs), or (3) using legally binding corporate rules. A July 2020 decision by the European Court of Justice invalidated the U.S.-EU Privacy Shield framework as a mechanism for data transfers and raised questions about the use of SCCs for U.S. companies subject to U.S. surveillance laws.

Two-Year Anniversary

In its two-year review, the European Commission (EC) stated the GDPR "met its objectives of strengthening the protection of the individual's right to personal data protection." The EC review noted success in raising EU public awareness on data privacy, but raised concerns about some implementation differences among member states, lack of DPA cooperation and adequate resources, and localization requirements.

As part of its review, the EC solicited external comments. The U.S. Administration asserted that the GDPR has made citizens less safe by hindering the sharing of data needed for health research, criminal investigations, and countering terrorism. The U.S. Chamber of Commerce and industry groups also raised concerns about international data transfer limits and the lack of coordination between DPAs.

According to the EU review, in its first two years, almost 300,000 complaints have been filed. DPAs have levied 273 GDPR fines—totaling about €150 million—for a range of violations against companies such as Equifax and Facebook, as well as smaller entities. Belgium fined Google €600,000 for not complying with the 'right to be forgotten'.

The GDPR and ePrivacy Regulation

The EU is debating an ePrivacy Regulation to ensure privacy of electronic communications in the digital era that would complement the GDPR's data protection requirements. The regulation would require traditional telecom providers, as well as messaging services (e.g., WhatsApp and SnapChat), to obtain explicit user consent for online tracking (use of cookies), and limit the amount of time that tracking data may be stored. Some analysts suggest this could hinder the online advertising industry and others dependent on tracking data. The regulation has proved controversial in the EU and remains pending.

GDPR and COVID-19

To help track the spread of Coronavirus Disease 2019 (COVID-19), several EU governments ask people to download a mobile tracking app, but uptake has been slow. The scope of data collected varies by country. The EU Data Protection Supervisor has stated that limited data collection with certain constraints (e.g., temporary data retention) is GDPR compliant and that the "right to the protection of personal data is not an absolute right." Some privacy advocates raise concerns that such data collection will set a precedent that lasts past the pandemic.

Policy Implications

While the United States has traditionally regulated privacy at a sectoral level to cover certain types of data, in 2018, California passed a consumer privacy law and other states are considering similar legislation with varying rules. While the state laws have similarities with the GDPR, they do not fully replicate it. U.S. policymakers and some Members of Congress are assessing the need for comprehensive national legislation, and multiple online privacy bills have been introduced. Some consumer and industry groups have advocated for a U.S. approach similar to the GDPR.

The U.S. plays an important role in international discussions on data protection and has begun to address data privacy and data flows in free trade agreements, including in the U.S.-Mexico-Canada Agreement. With no multilateral rules on cross-border data flows, the GDPR may effectively set new global data privacy standards, as firms and organizations strive for compliance to avoid being shut out of the EU market or penalized, and as other countries seek to introduce rules modeled on the GDPR. Such developments could limit U.S. influence in trade negotiations, such as in the ongoing World Trade Organization plurilateral negotiations related to e-commerce. Also see 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

IF10896

Disclaimer