Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated February 7, 2019

EU Data Protection Rules and U.S. Implications

Data Privacy and Protection in the United States and Europe

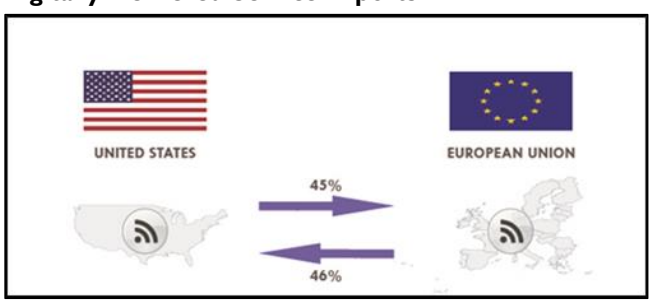
U.S. and European citizens are increasingly concerned about ensuring the protection of personal data, especially online. A string of high-profile data breaches at companies such as Facebook and Google have contributed to heightened public awareness. The European Union's (EU) new General Data Protection Regulation (GDPR)—which took effect on May 25, 2018—has drawn the attention of U.S. businesses and other stakeholders, prompting debate on U.S. data privacy and protection policies.

Both the United States and the 28-member EU assert that they are committed to upholding individual privacy rights and ensuring the protection of personal data, including electronic data. However, data privacy and protection issues have long been sticking points in U.S.-EU economic and security relations, in part because of differences in U.S. and EU legal regimes and approaches to data privacy. The GDPR highlights some of those differences and poses challenges for U.S. companies doing business in the EU.

The United States 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. Europe's history with fascist and totalitarian regimes informs the EU's views on data protection and contributes to the demand for strict data privacy controls. The EU regards current U.S. data protection safeguards as inadequate; this has complicated the conclusion of U.S.-EU information-sharing agreements and raised concerns about U.S.-EU data flows.

The transatlantic economy is the largest in the world, with goods and services trade of $2.7 billion a day and annual digital services trade of $260 billion. The United States and EU are each other's largest customers of digitally delivered services exports (see **Figure 1**).

Figure 1. Transatlantic Trade as a Percentage of Digitally-Delivered Service Exports



Source: Kati Suominen "Where the Money Is: The Transatlantic Digital Market," CSIS, October 12, 2017.

What Is the GDPR?

The GDPR establishes a set of rules for the protection of personal data throughout the EU. It seeks to strengthen individual fundamental rights and facilitate business by ensuring more consistent implementation of data protection rules EU-wide. The EU hopes the GDPR will further develop the EU Digital Single Market (DSM), aimed at increasing harmonization across the bloc on digital policies.

The GDPR identifies what is a legitimate basis 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).

The potential high penalties for noncompliance have attracted significant attention since a company or organization can be fined up to 4% of its annual global turnover or €20 million (whichever is greater). 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.

Possible Impact on U.S. Companies

Many U.S. firms have made and are making 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 will apply across the EU. Also, companies established in the EU that engage in cross-border data processing primarily only have to liaise with the supervisory authority of the EU country where the firm is based (the "lead" authority), possibly decreasing administrative costs. However, firms are still subject to oversight and enforcement by the supervisory authority of every country where it does business.

The GDPR and U.S.-EU Privacy Shield

Under the GDPR, the U.S.-EU Privacy Shield will continue to serve as a mechanism to transfer data for U.S. and EU firms that meet EU data protection requirements. However, participation by a company in Privacy Shield does not necessarily guarantee full GDPR compliance.

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 U.S. (and European) firms also argue that the GDPR's restrictions on the use and sharing of data could limit opportunities for analysis of global data sets and might chill innovation.

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. They also note the potential for localization trade barriers in areas where divergence is allowed.

Since the GDPR took effect, European DPAs have received a range of GDPR complaints. In the fall of 2018, several GDPR enforcement actions and fines were announced. In January 2019, the French DPA (or CNIL) issued the largest penalty to date for a data privacy breach, imposing a €50 million fine on Google for a "lack of transparency, inadequate information and lack of valid consent regarding the ads personalization." Analysts contend that the high fine may set a benchmark for future enforcement. Google is appealing the decision.

Policy Implications

While the United States has traditionally regulated privacy at a sectoral level to cover certain types of data, some U.S. policymakers and Members of Congress are considering whether comprehensive national legislation may be needed to better safeguard privacy, especially online. Stakeholders representing consumer and industry groups have issued proposals and frameworks, with some advocating for the United States to adopt an approach similar to GDPR. The United States has played an important role in international discussions and has begun to address data privacy and data flows in recent free trade agreements. With no multilateral rules on cross-border data flows, experts contend that the GDPR may effectively set new global data privacy standards, since companies and organizations will strive for compliance to avoid being shut out of the EU market or penalized, and other countries may introduce rules that imitate the GDPR. It may also be easier and cheaper for some U.S. companies to apply GDPR protections to all users rather than maintain different policies for different users. Such developments could limit U.S. influence in future trade negotiations on issues related to digital trade and cross-border data flows.

In addition to compliance costs, other elements of the GDPR are controversial. For example, the GDPR's right to be forgotten requires data controllers to delete personal data when it is no longer needed or when an individual requests it. Some question whether the right applies only to those accessing the Internet from the EU, or if the GDPR requires that a company delete specific information globally. Another issue is that the GDPR right to erasure could clash with freedom of information, and, for U.S. firms, with the First Amendment. The GDPR includes exceptions and recognizes the need to balance the right to personal data protection with freedom of expression, but advocates worry that Internet companies may be quick to grant erasure requests to avoid possible legal challenges, which, over time, could erode information online. Many stakeholders view the GDPR as pitting the "right to be forgotten" against the "right to know."

U.S. officials voice concerns about the GDPR's impact on the WHOIS database (managed by the Internet Corporation for Assigned Names and Numbers, or ICANN) used by law enforcement and cybersecurity researchers to identify hackers and malicious Internet domains. To comply with the GDPR, ICANN restricted the amount and types of data available on WHOIS, potentially limiting its effectiveness.

The GDPR and ePrivacy Regulation

The EU is considering a new ePrivacy Regulation to ensure privacy of electronic communications in the digital era that would complement the GDPR's data protection requirements. The draft regulation would apply to traditional telecom providers as well as messaging services such as WhatsApp and SnapChat, require providers to obtain explicit user consent for online tracking (use of cookies), and limit the amount of time a company can store tracking data. Some analysts suggest this could hinder the online advertising industry and others dependent on tracking data.

Also see, Law Library of Congress, *Online Privacy Law (2017 Update)*, December 2017, https://www.loc.gov/law/help/reports/pdf/2018-015633.pdf

Rachel F. Fefer, rfefer@crs.loc.gov, 7-1804
Kristin Archick, karchick@crs.loc.gov, 7-2668

IF10896