Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Google Fined for Violation of EU Data Protection Law

Stephen P. Mulligan
Legislative Attorney

February 22, 2019

In a decision testing what it means to give informed consent to online data collection, a French regulatory body recently fined Google LLC (Google) 50 million euro (approximately 56 million U.S. dollars)— the largest fine issued to date for violating the European Union's (EU's) General Data Protection Regulation (GDPR). Discussed in this CRS In Focus, the GDPR is an EU law that provides rules for protection of personal data throughout the 28-member European Union. The French data protection authority—the Commission Nationale de l'informatique et des Libertés (CNIL)—concluded that Google's lack of transparency and failure to obtain valid consent from Android phone users violated the GDPR. Although the fine arose under EU law (and Google has announced plans to appeal it), the decision could offer lessons for recent congressional efforts to craft more comprehensive federal data privacy policy.

What is the GDPR?

In effect since May 2019, the GDPR provides data protection rules in several interrelated areas: *data privacy* (i.e., how companies and organizations collect, use, and disseminate personal data), *data security* (i.e., how companies guard against and respond to data breaches), and *cross-border data flows* (i.e., when companies are permitted to transfer personal data within and outside of the EU). In terms of data privacy, which Google's fine concerned, the GDPR is more comprehensive than U.S. federal law. Whereas federal data privacy law involves a "patchwork" of separate laws covering different issues and sectors of the economy (discussed in this Legal Sidebar), the GDPR creates a single, unified data privacy regime.

Unless an exception applies, the GDPR applies to all *processing* of personal data, which is broadly defined to include collection, use, storage, disclosure or any other "set of operations" performed on personal data. From a territorial perspective, the GDPR applies to organizations that have an "establishment" in the EU and to non-EU-established entities that offer goods or services to individuals in

Congressional Research Service
7-5700
www.crs.gov
LSB10264

the EU. Because many businesses with an online presence offer goods and services to EU individuals, the GDPR applies to many businesses outside the EU, including many American businesses.

What Does the GDPR Require?

A central pillar of the GDPR's privacy provisions is the requirement that entities rely on one of six legal bases for processing personal data. Individual consent can be a lawful basis, but only if it is "freely given, specific, informed and unambiguous," among other conditions. The GDRP further states that consent is not considered "freely given" if users have "no genuine or free choice" about whether to provide it or are unable to withdraw their consent without detriment.

A second pillar of the GDPR's privacy provisions is its enumeration of eight data protection rights afforded to individuals (unless an exception applies).

1.	Individuals have a *right to be informed* about the collection and use of their personal data.
2.	Individuals have a *right to access* and obtain copies of their personal data.
3.	The *right to rectification* requires entities to correct inaccurate or incomplete data.
4.	The *right to erasure* (also known as the "right to be forgotten") allows individuals to demand that their personal data be erased in certain cases.
5.	Individuals have *right to restrict processing* of their data in some circumstances.
6.	The *right to data portability* allows individuals to obtain the personal data that they provided to an entity in a format that can be transmitted to another entity.
7.	Individuals have a *right to object* to the data processing in some circumstances.
8.	The GDPR provides a separately defined objections rights for data processing that involve *automated decision-making* (i.e., decision-making without human involvement), including profiling (defined in Article 4).

Why Was Google Fined?

After two digital rights advocacy groups filed complaints in May 2018 concerning Google's data privacy practices on its Android mobile operating system, the CNIL deemed Google's practices deficient in two ways.

First, the CNIL found that Google did not comply with its obligations to provide Android users with information about its data processing activities. A complement to the right to be informed, the GDPR requires data controllers (defined in Article 4) to disclose certain information about their activities, such as data retention periods, the purposes for which data is collected, and with whom the data will be shared. According to the CNIL, Google's disclosures lacked key information and were too generic for users to understand. The CNIL also found that Google improperly spread its disclosures across several documents. For example, an individual seeking information about Google's targeted advertising or location tracking practices was required to click through five or more pages to obtain a complete picture of the activities.

Second, the CNIL determined that Google did not obtain valid consent from its Android users. Requiring that users opt-out of targeted advertising by selecting a "more options" feature and then unchecking a pre-ticked box did not comport with the requirement that consent be *unambiguous*, according to the CNIL. Nor was consent *specific*, the CNIL concluded. Before creating an account, Google required users to agree to its terms of service in full rather than allowing users to provide consent for each distinct way Google processed user data. Lastly, the CNIL reasoned that user consent was insufficiently *informed* because Google's disclosures were incomplete and "diluted" across several documents.

The Fine in Context

Although the CNIL's 50 million euro fine is the largest penalty for violation of the GDPR to date, the advocacy groups that brought the action sought a much larger fine. Article 83 of the GDPR allows fines of up to 4% of a company's total worldwide annual revenue, which, in Google's case, exceeds 100 billion U.S. dollars. Based on this revenue, the privacy groups urged the CNIL to issue a multi-billion penalty, but the GDPR does not require that data protection authorities impose the maximum penalty. Instead, the regulation states that fines must be "effective, proportionate, and dissuasive," and that data protection authorities must consider a host of factors, including the nature, gravity, and duration of the offense. In Google's case, the CNIL found that the 50 million euro penalty was justified based on the severity of the infringements, but the CNIL did not explain in detail why it declined to impose a steeper penalty.

In the context of U.S. law, Google's data processing practices appear unlikely to run afoul of existing federal data protection laws. Although federal law contains certain sector or data-specific consent requirements, discussed below, it generally does not dictate the manner in which entities must disclose their data collection and use, provided their data privacy practices are not unfair or deceptive.

Lessons for Congress

The CNIL's fine may offer lessons for congressional efforts to craft data privacy policy at the federal level. In addition to upcoming hearings on the subject, several data privacy bills have been introduced in the 116th Congress (and previously in the 115th Congress). The National Telecommunications and Information Administration (NTIA) also recently sought comments on proposals to "advance consumer privacy while protecting prosperity and innovation." Policy options vary widely, and, while some commentators advocate for the U.S. to adopt a more comprehensive model based on the GDPR, other observers, including officials in the Trump Administration, have criticized the EU's approach. Despite the breadth of approaches, a common thread among many data protection policy proposals in the U.S. (both legislative and from the NTIA) is the aim to increase the level of *transparency* and *control* afforded to individuals that transmit their data online. The CNIL's fine of Google implicates both objectives.

With regard to transparency, the CNIL's decision demonstrates that mandatory disclosure requirements may present complex issues related to not only *what* information companies must disclose, but *how* they provide that information to Internet-users. In Google's case, Articles 13 and 14 of the GDRP describe in detail the information that data controllers must provide to individuals. But the CNIL found that the manner in which that Google presented the information was too vague and difficult to access. Some proposed legislation seeks to anticipate this dynamic by placing contours on the "form of disclosure," but other proposals are silent on the subject or direct the Federal Trade Commission to prepare more detailed regulations.

The Google fine also reveals complexities in legislative efforts to give individuals control over their data through consent requirements. Legal models for obtaining consent differ in legislative proposals and the patchwork of existing federal law. For example, the Video Privacy Protection Act prohibits "video tape service providers," including video streaming services like Hulu and Netflix, from disclosing protected information unless consumers affirmatively "opt-in" by electing to provide consent. Financial institutions, by contrast, can disclose protected information under the Gramm-Leach-Bliley Act if they provide consumers with advance notice and opportunity to "opt-out." The GDPR generally uses the opt-in model, and the CNIL fined Google, in part, because it required users to opt-out by deselecting pre-checked boxes. Some commentators debate which approach is optimal, while others argue that neither method effectively gauges user consent due to the inherent complexity in modern data processing and limits of consumer choice.