One Year In: GDPR Fines and Investigations against U.S.-Based Firms

Brian Daigle, Office of Industries, (202) 205-3458, brian.daigle@usitc.gov
Mahnaz Khan, Office of Industries, (202) 205-2046, mahnaz.khan@usitc.gov

On May 25, 2018, the European Union (EU) implemented the General Data Protection Regulation (GDPR), which requires businesses to protect the personal data and privacy of data subjects who physically reside or are located within the EU. Since the GDPR went into effect, EU member states authorities have initiated enforcement actions and imposed large fines particularly on U.S. firms for data breaches and unlawful data processing. This EBOT seeks to describe the nature of these regulatory actions against U.S. firms.

GDPR Enforcement Trends

The GDPR is a new EU regulation that protects the personal data of EU residents or those located within the EU. GDPR differs from the previous Data Protection Directive (Directive) because the GDPR applies to any firm, regardless of geographic location, that processes personal data of EU residents, even if these firms are not physically located in the EU or processing takes place on servers located outside the EU. GDPR has a stronger enforcement mechanism than the Directive, and EU data authorities can assess fines up to €20 million ($22.1 million) or 4 percent of a company's worldwide annual revenue, depending on the specific GDPR provision violated.

GDPR enforcement against U.S. firms varies by EU member state. Western European countries such as the UK, France, and Ireland have been aggressive in imposing fines and initiating investigations against U.S. companies. Data protection authorities (DPAs) in the UK and Ireland have publically stated that more GDPR fines will be imposed in the near future, in addition to "a couple of very large cases, [which are] in the pipeline." In contrast, data authorities in Eastern European countries have focused enforcement efforts on local firms. The primary focus of enforcement by EU data protection authorities thus far has been breaches of data protection related to "lawful processing" and transparency of data processing.

GDPR Fines against U.S. Companies

Since May 2018, EU member state data regulators have imposed fines on many companies for GDPR violations. Although a majority of these fines have been low in value, the EU has collectively imposed more than €380 million ($417 million) in total fines under GDPR.[1] The second and third largest fines were imposed on U.S.-based multinational companies Google and Marriott (table 1), while the largest so far was a £183 million ($229 million) fine imposed by the UK Information Commission Office (UK ICO) against British Airways. In July 2019, the UK ICO issued a £99 million ($118 million) fine against Marriott after the company discovered an earlier data breach in November 2018; this breach originally occurred in late 2014 in affiliate firm Starwood's data before Starwood was acquired by Marriott, and before GDPR was implemented. This breach ultimately compromised the passwords and credit cards records of 30 million EU residents. The UK ICO's fine against Marriott represented 3 percent of its worldwide annual revenue, which is close to the maximum penalty allowed by GDPR. Marriott stated that it plans to appeal the fine.

In January 2019, French data authorities fined Google €50 million ($56 million) after finding Google's use of blanket consent forms and pre-ticked boxes are not sufficient as valid and clear consent under GDPR. At the time, this was the largest fine issued for a GDPR violation. Google's fine represented approximately 0.4 percent of its worldwide annual revenue, which is substantially less than GDPR's maximum penalty of

[1] France, the UK, and the Netherlands imposed other data privacy fines not under GDPR against several U.S. firms for having inadequate measures to protect client data; some U.S. firms fined were Facebook (UK: $610,000), Uber (France: $449,000, UK: $469,000, Netherlands: $680,000), Dailymotion (France: $58,000), Optical Center and Bouygues Telecom (France: $280,000).

4 percent (in this case, 4 percent would amount to more than $4 billion for Google). Google is in the process of appealing the fine in France. Additionally, Greece fined U.S. consulting company PwC for failing to gain employee consent for the use of their personal data for analytics purposes.

Table 1. EU GDPR: Selected Fines levied against U.S. firms for GDPR violations, May 2018 – July 2019

Date	U.S. firm	EU country	GDPR clause violation	Fine issued
January 2019	Google	France	Art. 6, Consent and transparency, pre-checked consent on personalized advertising	€50 million ($56 million)
July 2019	Marriott	United Kingdom	Art. 33, Data breach, impacting 30 million EU residents	£99 million ($123 million)
July 2019	PwC	Greece	Art. 83, violation of fairness and transparency principles on data use of employees for commercial purposes	€150,000 ($165,400)

Source: GDPR Enforcement Tracker, http://www.enforcementtracker.com/ (accessed August 27, 2019).

Ongoing GDPR Investigations against U.S. Companies

In addition to the fines listed above, there are currently several ongoing GDPR investigations of U.S. firms. Many of these investigations are directed at U.S.-based tech companies, given tech firms' frequent use of personal data to conduct daily operations. Ireland, the country in which many U.S. tech firms base their European operations, is leading many of these investigations (table 2). France, the UK, and German states are also conducting investigations.

Table 2. Selected Ongoing Irish DPC Investigations of Prominent U.S. firms, May 2018-Aug 2019

U.S. firm	Alleged GDPR violation
Facebook	• *Right of access*: whether Facebook's Hive database observed obligations to ensure user data is transferrable. • *Lawful processing*: whether Facebook's terms of service respect the "lawful basis" for processing personal data; Facebook's use of personal data for behavior analysis and targeted advertising. • *Data breach*: 5 ongoing investigations regarding whether Facebook met breach notification requirements as well as technical/organizational obligations prior to and directly following breaches, in addition to whether Facebook violated GDPR in keeping user passwords in plain text on internal servers.
WhatsApp[1]	• *Lawful processing:* whether WhatsApp's terms of service follow lawful basis for processing personal data • *Transparency:* whether WhatsApp meets transparency obligations on information provided to users.
Instagram[1]	• *Lawful processing:* whether Instagram's terms of service follow lawful basis for processing personal data.
Twitter	• *Right of access:* whether Twitter's ability for users to access links meets GDPR right of access obligations • *Data breach:* whether Twitter met technical/organizational obligations to safeguard data following a breach.
LinkedIn	• *Lawful processing:* LinkedIn's use of personal data for behavior analysis and targeted advertising.
Apple	• *Lawful processing:* Apple's use of personal data for behavior analysis and targeted advertising. • *Transparency:* whether Apple meets its transparency obligations with respect to its privacy policy • *Data access:* whether Apple meets its data access request obligations under GDPR.
Google	• *Lawful processing:* Google's use of personal data for behavior analysis and targeted advertising. The investigation will also look at *transparency* and *data minimization* obligations under GDPR.
Quantcast	• *Lawful processing:* Quantcast's use of personal data for behavior analysis and targeted advertising.
Verizon	• *Lawful processing:* Whether Verizon's use of online cookies complied with lawful processing requirements.

[1] Both WhatsApp and Instagram are owned by Facebook, Inc.

Source: Irish Data Protection Commission website; Ireland DPC, "Annual Report: May 25-December 31 2018," February 2019.

Selected Sources: John Timmons, "UK ICO Continues Heavy GDPR Enforcement Trend with £99 Million Fine," White & Case, July 10, 2019; Baker McKenzie, "GDPR: One Year On," June 4, 2019.