

EUROPEAN DATA PRIVACY WATCHDOGS TAKE NEW STEPS

In the past week, European data protection authorities have found substantial European Union General Data Protection Regulation (“GDPR”) violations and issued corresponding fines against high-profile companies. These decisions are informative for companies doing business in Europe as they indicate clear future enforcement priorities by European regulators.

On December 10, 2020, the French Data Protection Authority (“CNIL”) issued fines against Google (€100M; \$120M) and Amazon (€35M; ~\$43M) for improper use of cookies on their websites. Specifically, the CNIL found that the tech giants automatically dropped tracking cookies when users visited their French (.fr) websites. Under the GDPR, these tracking cookies cannot be used without prior consent by the user. Since at least October 2019, European law has been clear that websites must obtain prior consent before utilizing any non-essential cookies.

These fines follow a similar CNIL fine against Google for \$57M for failing to adhere to the GDPR’s transparency obligations.

Meanwhile, on December 15, 2020, Ireland’s Data Protection Commission (“DPC”) slapped Twitter with a fine of €450,000 (~\$547,000) for failing to properly declare and document a data breach. The DPC is Europe’s leading privacy enforcement agency for many large tech companies, including Facebook, WhatsApp, Google, Apple, and LinkedIn, among others. The DPC fine marked the first cross-border GDPR fine issued by the Irish watchdog. Though many have expressed concerns that the DPC has been slow in reacting to privacy violations by non-EU companies, this cross-border decision is somewhat of a landmark decision for the DPC. In addition to the Twitter case, the DPC has a backlog of over 20 cases against large tech firms, many of which are U.S.-based entities.

In 2020, both the CNIL and the DPC have recently issued guidance on cookie usage and the notice, consent, and transparency requirements of the GDPR. The Amazon and Google fines, together with the CNIL and DPC guiding opinions, provide insight into their enforcement priorities. The guiding opinions make it clear that the CNIL and the DPC are specifically targeting companies that are improperly utilizing non-essential cookies; furthermore, the extent of the fines indicate that the regulatory agencies view these matters as particularly

egregious violations.

Moreover, the DPC's long-awaited first cross-border decision may be seen as a warning that non-EU companies may no longer find safe harbor in Ireland's lethargic enforcement efforts. Should these decisions act as a harbinger of future enforcement efforts, non-EU-based companies will need to quickly ensure compliance with GDPR regulations concerning non-essential cookies. As these decisions indicate, improper cookie usage could be costly for any company doing business in Europe.

If you or your company have questions or concerns about your cookie usage or compliance with international data privacy laws, please contact us.