Client Alert: Irish Data Protection Commission Issues Annual Report On GDPR Enforcement

Related Attorneys

Marcel C. Duhamel

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 2.25.2020

In February, the Irish Data Protection Commission (DPC) issued its annual report covering the first full year of GDPR enforcement. The Irish DPC's activities are of particular interest to US-based companies. Many large technology companies, such as Microsoft, Intel, IBM, Facebook, Google, and Apple, have operations in Ireland, and the Irish DPC's enforcement efforts with respect to those companies may well serve as a guide to the data protection authorities in other EU member states. US-based companies to which GDPR is applicable should view the Irish DPC's enforcement activities, even if their operations are in other member states, as likely informative of future enforcement in other EU countries.

Summary of Complaints

In the past year, the DPC received 6,904 complaints regarding GDPR. These complaints were submitted by individuals relating to the processing of their personal data, an entity complaining on behalf of an individual, or an advocacy group. Many of these complaints dealt with Access Requests, which constituted 29% of the total GDPR complaints. eMarketing Complaints made up 5% of the complaints, and the DPC prosecuted four Irish entities regarding electronic marketing without consent. Three of the four companies were required to donate money (in a range from €600 to €2,000) in lieu of a conviction and fine. The final entity, Vodafone Ireland, had been previously prosecuted; thus, it was convicted and fined €4,500.

The Irish DPC also received 457 complaints through the One-Stop-Shop (OSS) mechanism concerning cross-border data transfers, an issue which continues to present significant compliance issues for many companies. Under GDPR, multinational companies with establishments in several EU member states are subject to regulation primarily from the Data Protection Authority in the member state where the company has its main establishment. The OSS mechanism is intended to permit companies to obtain guidance and supervision from a single regulator, rather than needing to consult multiple regulators in each EU nation in which they do business. The Irish DPC is

the lead supervisory authority for many large technology and social media companies with locations in Ireland.

The Irish DPC reports that among the most significant sources of complaints are: (1) disputes between employees and their employers, often involving a dispute concerning access to personal data; (2) disputes between telecommunications companies and banks with their customers, often regarding account administration; and (3) complaints against internet platforms, and in particular disputes about individual's rights to data erasure when they close their accounts. The regulator also reports that it has "pursued rigorously" enforcement for direct marketing offenses.

Binding Corporate Rules Review

Binding Corporate Rules (BCRs) provide one mechanism permitting a company in the EU to transfer data to an affiliate outside of the EU. This is of particular importance to US-based companies with affiliates in the EU who wish to exchange persona data of EU data subjects. The issue arises, for example, when the US-based affiliate seeks access to the EU affiliate's employee data. Transfers of personal data from the EU to the US are generally prohibited unless the transferor and transferee take specific steps. Those steps can include obtaining Privacy Shield certification for the US-affiliate, or adopting BCRs that will apply to both affiliates. BCRs must be approved by the relevant Data Protection Authority.

The DPC reports that it has acted as lead reviewer for nineteen BCR applications from twelve different companies that have designated Ireland as their lead authority. A lead authority is chosen based on a myriad of criteria that includes the location of the company's European headquarters and the location where most decisions regarding data transfers are made. Because many technology companies are located within Ireland, the Ireland DPC is named as lead reviewer on many BCR applications.

The DPC forecasts that it will be named as lead authority of more companies as Brexit proceeds. The DPC believes that many companies that currently name the UK as lead authority will transition to Ireland as a result of the UK's departure from the EU.

Overview of Data Breach Complaints

The Irish DPC received over 6,000 data-breach notifications under the GDPR. From 2018 to 2019, the DPC saw an increase of 71% of valid breach notifications. The Report reflects several trends seen in the breaches: late notifications, difficulty in assessing the risk posed by the breach, failure to communicate the breach to individuals, repeated breaches at the same company and of a similar nature, and inadequate reporting regarding efforts to mitigate the breach.

Overview of Compliance Inquiries

As of December 31, 2019, the Irish DPC had 70 compliance investigations open. Many of these involved large internet platforms and focused on whether the targets had lawful bases for processing (including with respect to targeted advertising), whether the targets had satisfied their transparency obligations, and whether the targets had satisfied an obligation to honor a data subject's right to access.

Key Take-Aways

GDPR enforcement remains in its infancy. Just as companies continue to develop strategies to comply with GDPR, EU regulators are continuing to develop their approaches to the interpretation of the regulation and to their approaches to enforcement. US-based companies with exposure to GDPR should monitor these developments and adjust their compliance programs as the regulators' enforcement programs mature. It may be tempting for such businesses to assume that enforcement against the largest internet and tech companies has little relevance to them, but this is a mistake. One should expect instead that the principles established in these early enforcement efforts will be applied later to all companies, including those in the US to whom GDPR applies.