Welcome to ComplianceWeek.com. This site uses cookies. **Read our policy**.

COMPLIANCE WEEK
FOR THE WELL-INFORMED CHIEF COMPLIANCE OFFICER AND AUDIT EXECUTIVE



GDPR enforcement varies widely by country



By Neil Hodge | Fri, Jul 19, 2019 1:38 PM

The introduction of the GDPR has seen a general increase in complaints and breach notifications, though this does not mean that data protection rules have been broken. Simply, growing awareness has resulted in an uptick of reports and a responsibility by regulators to review them and investigate where necessary.

Country-by-country look at GDPR enforcement trends

Austria

Austria operates a system whereby first breaches of the GDPR can basically be sanctioned by a warning—the Austrian DPA only imposes fines from the second breach onwards. So far, the regulator has handed out three fines, all of which involved illegal video surveillance. And the penalties have been relatively lenient, ranging from €300 to €5,280 (U.S. $337-$5,932).

Denmark

Even before May 25, 2018, it was clear that the Danish DPA would not impose large-scale GDPR fines from the beginning, as Danish constitutional law means the regulator cannot issue penalties under the new data rules until the Danish courts have established an adequate level for fines for the various types of breach of the GDPR.

However, the Danish DPA has referred one particular case to the Danish Prosecution Service. Following an inspection visit at a Danish taxi company, the Danish DPA found it had stored personal data (mainly phone numbers) from approximately 9 million taxi rides without a legitimate reason. Consequently, the Danish DPA has suggested a fine of DKK 1.2 million (U.S. $180,000) be imposed.

France

The French Data Protection Authority (CNIL) imposed a €50 million (U.S. $56.3 million) GDPR fine on Google on Jan. 21 for two counts of violating data protection rules. It was found that the internet giant failed to provide adequate transparency information to individual users and failed to provide a valid lawful basis for the processing of user data as the consent it had obtained did not meet the enhanced requirements of the GDPR.

Other large fines the regulator has handed out include Bouygues Telecom (€250,000; U.S. $280,000), Uber (€400,000; U.S. $449,000), Dailymotion (€50,000; U.S. $56,000), and Optical Center (€250,000; U.S. $280,000)—all of which relate to a lack of technical measures securing client data.

Generally, however, the CNIL has not yet imposed fines as vigorously and as widely as many people feared: instead, it has preferred to provide information, guidelines, e-learning training, and various tools about the new regulation on its Website. It has also treated smaller companies with more leniency. Complaints to the CNIL have increased by 32.5 percent compared with 2017.

Germany

In Germany, the DPAs are organized on a state level, which means there are 16 data regulators. In total, German DPAs have issued 75 fines since the GDPR was implemented, totaling just €449,000 (U.S. $504,000)—the largest single fine being €80,000 (U.S. $90,000) to a healthcare organization that exposed sensitive personal data.

Latvia

The Latvian DPA did not impose many penalties during the first year of GDPR application. The biggest publicly announced fine was only €2,000, which is even smaller than the penalties imposed before the GDPR started to apply a year ago. However, there are a couple of reasons for this: firstly, the regulator said that it wanted to consult and help organizations comply, rather than punish them (an approach taken by several other EU data authorities, such as Belgium, Bulgaria, Croatia, Cyprus, and Greece), and secondly, it is overloaded with cases.

Lithuania

The Lithuanian DPA has been quite active. In January it made public a list of planned inspections announcing the names of 75 organizations that will face GDPR compliance inspections this year. After the investigations are completed, the DPA will provide its recommendations regarding the most common compliance failures.

Netherlands

The Dutch Data Protection Authority has not yet imposed GDPR fines as vigorously as many people feared: it started first and foremost by providing information, guidelines, and tools about the GDPR on its website. So far, only one headline fine has been handed out: Uber was fined €600,000 (U.S. $673,000) for failing to comply with the obligation to report data breaches within 72 hours.

Sweden

The Swedish DPA has not yet imposed any fines, but the regulator has provided information about ongoing investigations. Cases of interest include Google's access to user location data by means of its so-called "Location History" and "Web & App Activity," and how payments services provider Klarna uses customers' personal data. A school is also being investigated over its use of facial recognition software to register attendance.

United Kingdom

The two biggest enforcement actions so far stemming from GDPR violations have come from the U.K.'s Information Commissioner's Office, which in the past week fined British Airways £183.4 million (U.S. $230 million) and Marriott £99.2 million (U.S. $124 million) on back-to-back days for data breach-related violations.

No fines yet

Belgium, Ireland, Czech Republic, Denmark, Finland, Italy, Slovakia, Slovenia, Spain, and Sweden

Source: **Ius Laboris**

According to the European Data Protection Board (EDPB), the body that **reviews and provides guidance** about how the GDPR should be applied across the European Union, there have been 281,088 cases logged by the various supervisory authorities in the first year of the GDPR's application. Of these, 144,376 related to consumer complaints and 89,271 related to data breach notifications by data controllers. The Netherlands, Germany, and the United Kingdom have reported the largest number of breaches, respectively; Liechtenstein, Iceland, and Cyprus have reported the lowest.

The three areas that have been subject to the most consumer complaints are telemarketing, promotional emails, and CCTV/video surveillance.

Yet, according to law firm DLA Piper's "**GDPR Data Breach survey**" released in February, just 91 GDPR fines had been handed out across the European Economic Area within the first eight months of the GDPR coming into force. That figure has now risen—but not by much, say experts. The EDPB's February 2019 report to the European Parliament indicated 11 countries had imposed GDPR fines totaling approximately €56 million (U.S. $63 million)—including the €50 million (U.S. $56.3 million) levied against Google by France's CNIL.

Most EU countries have now issued fines under the GDPR (those that have not are Belgium, Ireland, Czech Republic, Denmark, Finland, Italy, Slovakia, Slovenia, Spain, and Sweden). For the most part, the quantum to date has been in keeping with the old regime, meaning relatively modest penalties. Leaving aside headline cases, up until this February the average fine levied was around €66,000 (U.S. $74,000).

Determining which countries are the toughest enforcers depends on one's viewpoint. Before last week, the United Kingdom hadn't issued a single fine; now it's in pole position with a penalty tally over four times more than the rest of Europe put together. A lot depends on the approach of each supervisory authority. Many have preferred to educate and cooperate, rather than punish, using the GDPR's first year as a grace period to promote compliance (Belgium, Cyprus, and Latvia are some examples).

Some, **like Austria**, have decided to target general, low-level abuses that could apply to a wider range of organizations, rather than aim for big tech firms as a priority. For example, in September 2018, the Austrian supervisory authority, the DSB, fined a sports betting café €5,280 (U.S. $5,900) for installing a CCTV camera that recorded passers-by, in contravention of the GDPR's ban on large-scale monitoring of public spaces.

Some of the more severe penalties to date have focused on technology misuse at one end of the spectrum and general data sloppiness at the other. For example, the national soccer league in Spain, LaLiga, was fined €250,000 (U.S. $280,000) for offering an app which—without their knowledge or consent—accessed the microphones of users' mobile phones for the purpose of detecting whether pubs that were screening soccer matches had actually paid a fee to do so.

Meanwhile, a Portuguese hospital was fined €400,000 (U.S. $449,000) after an investigation revealed the hospital's staff, psychologists, dieticians, and other professionals had unlimited access to patient data through false profiles. A subsequent audit carried out revealed the hospital had 985 registered doctor profiles despite only having 296 doctors.

Germany's 16 data supervisory authorities have been the most proactive enforcers, handing out a total of 75 fines since the GDPR was implemented. The first was in November 2018, when the LfDI Baden-Württemberg fined the social media platform Knuddels €20,000 (U.S. $22,000) for storing passwords in plaintext, following a data breach in which approximately 330,000 users' personal data was compromised. The highest German fine to date was also issued by the Baden-Württemberg authority: €80,000 (U.S. $90,000) to a healthcare organization that exposed sensitive personal data.

Hungary, meanwhile, has handed out the largest fine in respect to proportion of an organization's turnover. The Hungarian National Authority for Data Protection and Freedom of Information (NAIH) issued a HUF 30,000,000 fine (U.S. $103,000) to the organizers of the Sziget multicultural music and arts festival over their security procedures, which involved photocopying IDs of hundreds of thousands of festival-goers

and taking photos at the entry gate. The penalty represented 2.3 percent of the company's net revenue.

While the Netherlands has issued very few fines, it has dealt out one very **sizeable, high-profile one**. Last November, the Dutch Data Protection Authority hit taxi-app firm Uber with a €600,000 (U.S. $673,000) penalty for "violating the Dutch data breach regulation" by failing to inform the regulator within 72 hours of discovery that it had suffered an unauthorized breach that affected 57 million Uber users worldwide (of which 174,000 were Dutch citizens). It also came to light that Uber had paid the attackers $100,000 to destroy the data, which included the names, e-mail addresses, and telephone numbers of customers and drivers they had downloaded.

Karen Holden, founder of London legal practice A City Law Firm, says GDPR regulators have generally set out several conditions that are considered when issuing fines, such as the nature of the infringement (external hack, negligence, or both); what type of data was compromised; what actions were taken following the incident; and how cooperative the company was with regulatory and authoritative entities.

"It is clear that each case is judged on its own merits and is very much dependent on the facts of each case," says Holden. "In the case of Knuddels in Germany, for example, the company was spared a much harsher penalty due to its effective strategy in responding to and dealing with the data breach," she says.

Websites

We are not responsible for the content of external sites

EDPB overview of GDPR implementation

DLA Piper survey