Expert Analysis

The Evolution Of GDPR Enforcement Across The EU

By ***James Simpson***

James Simpson

Law360 (November 13, 2019, 3:28 PM EST) -- The last few months have seen the reporting of some very significant fines against well-known businesses for breaching the General Data Protection Regulation.

The first big one was issued by the National Data Protection Commission in France when it fined Google Inc. €50 million. This was followed in the U.K. when the Information Commissioner's Office issued notices of intent or fines against British Airways PLC for €205 million and Marriott International Inc. for €110 million. And in Bulgaria, the Commission for Personal Data Protection fined its National Revenue Agency €2.6 million.

It is anticipated these will be followed by decisions of the German regulator, which is contemplating another multimillion fine against a presently unnamed company, with other similar cases pending in the U.K. and Ireland.

Clearly, the regulators across Europe are beginning to flex their enforcement muscles with the supervisory authorities of 13 different European Union countries appearing in the top 20 list of fines being issued.

That top 20 list also provides some insight into the types of breaches currently in the crosshairs of the regulators — about 60% relate to unauthorized access to personal data either through cyberattacks or poor security procedures. Indeed, all but one of the top 5 involve the loss of data.

The Google case is the only one in that top 5 that relates to breach for other reasons. And while data security does feature highly, for the remainder of cases, the breaches generally relate to organizations not being transparent or operating poor consent, data retention and minimization procedures.

For example, the Spanish Data Protection Authority, the AEPD, fined La Liga, the Spanish Professional Football league, €250,000 for marketing an app that failed to adequately inform its users that the microphone in the user's mobile telephone would be periodically engaged to eavesdrop on the watching of televised football games. The app also failed to get lawful consent for this use.

Inevitably, as the size of the fine relates to a percentage of turnover, large household-name companies or public sector organizations typically appear in that top 20 list. That said, while these blockbuster cases catch the headlines, the level of fines drops considerably outside the top 20 with most fines being less than €100,000.

The European Data Protection Board, which has taken over the pan-European responsibility for data protection regulation and compliance from the Working Party 29, has also provided some useful information. It issued its first annual report in May this year, titled "1 year GDPR – taking stock."

It reports that the number of procedures (cases) rose exponentially from June 2018 to a new high in April 2019. A total of 281,088 cases were reported with action taken in less than 40% of them. Almost 50% of the reported cases were derived from complaints made by data subjects with data breach reporting amounting for about 30% of the remainder.

What are the key themes and trends that can be gathered from this, more than one year on from the introduction of the GDPR?

Well, first, greater public awareness of data protection rights and the new requirement for organizations to report data breaches has understandably increased the number of active cases and the consequent level of enforcement action. This fear of complaints and fines has also inevitably driven better compliance including improved cooperation between organizations and regulators. The EDPB reports that all the cooperation procedures, including cross-border, are robust and working efficiently.

Data protection practitioners also know that, with greater awareness and reporting, litigation risk

More Expert Analysis

Useful Tools & Links
Add to Briefcase
Save to PDF & Print
Rights/Reprints
Editorial Contacts

Related Sections
Corporate Crime & Compliance UK
Financial Services UK
Insurance UK

Companies
British Airways PLC
Google Inc.
Liga Nacional de Futbol Profesional
Marriott International Inc.

Government Agencies
European Union
Information Commissioner's Office

Top 10 trending in Financial Services UK

1 Trio Convicted In Metro Bank Money Laundering Trial
2 Banker Faces Trial For Aiding €100M Dutch Shipping Fraud
3 Exec In LC&F Scandal Looks To Block Access To Private Docs
4 Clearinghouses Call For Longer Buffer After Brexit
5 Fraud Chief Pushes Coordination To Tackle Spiraling Crime
6 What Headlines Missed About 'Cartel' Traders' Trial 1 Year Ago
7 Asset Manager, Investors Settle Share Dispute On Eve Of Trial
8 HSBC Hong Kong Seeks Exit From 'Retread' Of Ponzi Suit
9 Defecting Brokers Won't Be Kept Out Of Poaching Trial

is also growing very quickly. Claims firms have been quick to move into this area and are starting to market aggressively, supporting data subjects in bringing individual claims or class actions against defaulting and vulnerable organizations.

Some practices are even helping data subjects by automating subject access requests to offer quick and efficient means of serving and forcing organizations to provide documents and access to personal data. This has resulted in a greater administrative burden on organizations and seen a growth in the size and activities of in-house data protection teams.

It has also shown the importance of good insurance. Being a new area of risk, the insurance market is still developing policy terms and methods of calculating risk and premiums. It remains that fines are largely uninsurable but the on-costs of having to deal with investigations, remedial action, the administration and management of complaints and claims from data subjects flowing from a fine are all very burdensome — organizations are learning fast that insurance can help with the cost pain!

In terms of enforcement action itself, this is very obviously increasing and it seems that the supervisory authorities in each member state are broadly acting in a consistent manner. Data breach remains the most significant area for enforcement but, as with the Google case, the supervisory authorities are also focusing on the core principles. The Information Commissioner's Office in the U.K. has flagged that it intends to focus on accountability in the second year of the GDPR.

One area of difference is that member states often have different rules relating to consent and opt-ins in the context of marketing. Some have more stringent rules under existing e-privacy regulations, often disapplying soft opt-ins and instead requiring double opt-ins.

The e-privacy regulations were meant to be brought in line at the same time as the GDPR to provide consistency, but the new legislation was postponed and appears to be static for the foreseeable future. Consequently, this continues to be an area of inconsistency across the EU both in terms of legislation and enforcement, and businesses operating across borders need to alive to the differing landscape.

Otherwise, the issued cases and judgments suggest that the adoption of the GDPR is broadly consistent across the EU — there are some regional variations and derogations but the main principles underpinning the GDPR are being applied consistently. While the fines issued by the ICO in the U.K. are the highest, they reflect the size of the defaulting businesses and the seriousness of the breach. Fines for comparative cases appear to be dealt with consistently across the European Union.

It is anticipated that enforcement by way of fines will steadily increase with the greater awareness, even if breach reporting falls, particularly as supervisory authorities have started moving away from a light-touch approach in the initial bedding-in period for the new rules. The supervisory authorities are also actively turning their attention to other areas of compliance.

For example, the U.K.'s ICO is actively addressing businesses that have failed to pay their data protection fee — failing on such a basic requirement is an easy win for it. In its report, the Experiential Designers and Producers Association is recommending more active intervention and investigations which could result in supervisory authorities, particularly in the larger EU member states, acting more aggressively.

In tandem, supervisory authorities will continue to provide help and guidance and there is likely to be an expansion of sector-specific codes of practice and data protection certification. The EDPB has responsibility for collating all EU certification schemes. It is proposed that the EDPB will also implement a European data protection seal where criteria are approved by the EDPB for use across the EU.

Final versions of guidelines for codes of conduct, certification criteria and accreditation of certification bodies were adopted at the plenary session on June 4. The ICO anticipates that UKAS will soon be able to accredit certification bodies who will be able to implement the ICO-approved schemes in line with the EDPB guidelines. Although it will not happen in the immediate short term, it is likely that defaulting organizations will be judged against the standard adopted and issued by these newly created certification bodies.

In the meantime, organizations should sign up to the regular updates from the relevant supervisory authorities. They are informative and provide a good steer on the evolution of GDPR and its enforcement.

10 Post-Scandal Libor Rigging Suit Can Proceed, Investors Say

James Simpson is a partner at Blaser Mills LLP, a member of IR Global.

0 Comments