GDPR Enforcement and Fines Have Arrived

After the introduction of the European Union (EU) General Data Protection Regulation (GDPR) in May 2018, 2019 was expected to be the year of enforcement. It is fair to say that regulatory activity has picked up, but the envisaged "mega fines" have not been widespread. The fact that the GDPR contains extraterritorial provisions means US-based and other non-EU-based organizations should be tracking GDPR enforcement developments as they may be subject to the GDPR due to their customer base and/or employee work locations.

In the summer of 2019, the UK saw the Information Commissioner's Office (ICO) propose two massive fines – £183 million against British Airways and £99 million against Marriott Hotels in relation to security breaches. The ICO had six months from the date of issuing a notice of intent to issue a final monetary penalty – this period was due to expire in January 2020, but the ICO agreed an extension of time until March 31, 2020 with British Airways and Marriott[1]. Unless the ICO scores a huge own goal and misses the new deadline, the final notices are on their way.

In the meantime, the ICO issued a final monetary penalty notice of £275,000 on December 20, 2019 against a north-London based pharmacy, Doorstep Dispensaree, for storing 500,000 medical documents containing sensitive medical data in unlocked containers. The ICO was highly critical of Doorstep Dispensaree, saying it had taken a "cavalier" attitude to the protection of personal data.

This is not the first enforcement action by the ICO under the GDPR, but it is the first GDPR fine. Back in October 2018, the ICO issued an enforcement notice against AggregateIQ under the GDPR, requiring the organization to change its data processing practices. Given that this notice was issued to a Canadian organization under the GDPR's extra territorial scope, it is difficult to assess its effectiveness.

While ICO fines have been rare, other European regulators are more active, with GDPR fines issued across Belgium, Bulgaria, France, Germany, Greece, Hungary, Italy, Lithuania, Netherlands, Norway, Poland, Romania, Spain and Sweden.

[1] https://www.theregister.co.uk/2020/01/13/ico_british_airways_marriott_fines_delayed/

BZCER036_US_02/2020

At present, there is little consistency across regulators with regards to the level of fine issued. The Spanish Data Protection Agency (DPA) has issued relatively low fines against large organizations, for example, the Corporación de Radio y Televisión Española was fined a mere €60,000, and La Liga was fined €250,000 for alleged spying on users via a mobile phone microphones.

hired to help them respond to the attack. The response is further complicated when the MSP itself is also infected with ransomware. Where an attack group knows they have hit an MSP, and also infected downstream clients, they may refuse to negotiate with the end clients and instead only respond to the MSP in order to increase their ransom demands. This tactic can also leave clients with little to no control over their data software recovery.

At the higher end of the scale, the Austrian DPA imposed an administrative fine of €18 million on Österreichische Post AG (ÖPAG) for violations of the GDPR by processing personal data on the political views of affected data subjects. In Germany, the Berlin Commissioner for Data Protection and Freedom of Information issued a fine of around €14.5 million against Deutsche Wohnen SE for violations of the GDPR relating to the unnecessary collection and retention of personal data.

Social media giants and their data protection practices have been the focus of many regulators. In particular, the DPA in Ireland (where many of these companies are domiciled) has been busy investigating Facebook and Twitter, though no enforcement action has yet been taken. However, other European regulators have taken matters into their own hands – the Italian DPA issued a fine of €1m against Facebook over the Cambridge Analytica scandal, and a German DPA has separately issued a fine of €2m against Facebook for underreporting complaints by data subjects. The French DPA, the Commission Nationale de l'Informatique et des Libertés (CNIL), also issued a sizable €50m fine against Google in early 2019 for failing to provide users with transparent and understandable information on its data use policies.

European regulators have also been inconsistent in their approach to dealing with cyber incidents. The UK's ICO, for example, often takes a practical approach to ransomware incidents and has appreciated that, while personal data may be affected, the attack's motive is not usually to obtain personal data or use it to cause harm to data subjects, but tends to be purely financial in nature.

On the other hand, we have seen the Irish Data Protection Commission (DPC) adopt a highly active approach to investigating ransomware, taking a particular interest in the technical side of the attack, asking numerous questions and even seeking disclosure of forensic IT reports.

Inconsistency also exists within regulators. We have seen examples of the ICO receiving a breach notification and closing down its file within a matter of days, and other examples of investigations lasting for over six months before closure. This level of inconsistency makes it difficult to predict how an investigation will play out, and highlights the importance of carrying out and documenting a thorough response to a data privacy incident, just in case it attracts the regulator's attention.

Overall, 2019 was a year in flux. Regulators have been grappling with their newfound powers and have been using them inconsistently across Europe. One can only hope that 2020 brings greater guidance and oversight from both individual regulators and the European Data Protection Board . Until then, the regulatory landscape in Europe remains a patchwork quilt of rules and approaches. All organizations that operate across different jurisdictions would be wise to seek local advice on their data protection practices, particularly if they suffer a data breach or cyber security incident. The penalties for getting it wrong can be severe.

BBR Services – a dedicated team of experts

Beazley is unique among insurers in having a dedicated business unit, Beazley Breach Response (BBR) Services, that focuses exclusively on helping clients manage cyber incidents successfully. This in-house team of experts works closely with cyber policyholders on all aspects of incident investigation and breach response and coordinates the expert services that insureds need to satisfy legal requirements and maintain customer confidence.

In addition to managing data breach response, BBR Services provides a full range of resources to help mitigate risks before an incident occurs. BBR Services develops and maintains Beazley's risk management portal as well as coordinates newsletters and live expert webinars and pre-breach services such as onboarding calls, incident response plan reviews and on-site workshops.

beazley

www.beazley.com/bbr