Winter Is Here:
The GDPR Shows Its Teeth in a String of Major Fines

Georgia Moorhouse
Natalie Farmer
Natascha Gerlach
Cleary Gottlieb[1]

Just over a year after the EU General Data Protection Regulation (GDPR) took effect across all EU Member States in May 2018, regulators have begun to flex their new muscles by imposing major fines for violations. Where the size of fines under member states' previous data protection legislation was limited[2] the GDPR now allows for fines of up to the higher of €20 million or 4% of a company's global annual turnover for certain violations. As recent headline-grabbing fines for data protection violations show, when it comes to the new enforcement powers at their disposal, regulators appear to have found their footing - and further enforcement should be expected. In May 2019, for example, the European Commission revealed that data protection authorities have received a total of 144,376 complaints for violations of the GDPR, and 89,271 mandatory notifications from companies about data breaches. There are currently 446 ongoing cross-border investigations into violations and in Ireland, the Data Protection Commission has revealed it is investigating Facebook, Instagram and WhatsApp, as well as Apple, LinkedIn and Twitter.

The first significant fine of the new data protection regime was handed down in July 2018 by the Portugese Comissão Nacional de Protecção de Dados against the public sector hospital Centro Hospitalar Barreiro Montijo. The hospital was sanctioned for mismanaging patients' data, by failing to ensure that access to confidential and sensitive information was limited to relevant health-care professionals. Three separate fines with a combined value of € 400,000.00 were imposed for violations of Art. 5(1)(c), 5(1)(f) and Article 32(1)(b) of the GDPR. The fines demonstrate that access controls are essential in connection with personal data processing.

The French Commission Nationale De L'Iinformatique et des Libertes (CNIL) followed in January 2019 with a fine of €50 million against Google. The fine was significant not only because of its size, but because it constituted the first major action taken by a European regulator against a tech giant.

In July of this year, the UK ICO issued notices of intention to impose fines on British Airways and the Marriott hotel chain, the size of which could be considered impressive even by antitrust law standards.. Separate cybersecurity incidents at the two companies saw the personal data of millions of customers misappropriated and the ICO has made it quite clear, where personal data is concerned great care must be taken to keep it secure. The UK ICO has not published its final enforcement notice yet, but while the cybersecurity incidents were the catalyst for investigation, it seems likely that these companies will face fines for various and multiple infringements of the GDPR.

British Airways faces a potential fine of £183.4 million which, if enforced, would be the largest fine to be levied under the GDPR (and in the history of data protection law enforcement in Europe).

British Airways

According to the ICO's press release, the cybersecurity incident in question involved a hack disclosed to the ICO in September 2018 that caused user traffic to the British Airways customer website to be diverted to a fraudulent site. The false site was then able to harvest the personal information of approximately 500,000 British Airways customers. The ICO commented that its investigation revealed "poor security arrangements" in relation to the security of customers' log in, payment card, and travel booking details as well name and address information. It has not been revealed how the ICO determined the size of the fine, though it amounts to approximately 1.5% of British Airways' global passenger turnover in 2018 (£11.6billion), falling short of the maximum fine of 4% of annual turnover which could be levied under the GDPR.

Marriott

The ICO has also published its intent to fine Marriott a £99.2 million for a cybersecurity incident, notified in November 2018. The ICO reported that it had carried out an extensive investigation into the incident, which is thought to have initially occurred when the guest reservation database of the Starwood hotels group was compromised as far back as 2014. Starwood was later acquired by Marriott in 2016, who allegedly did not discover the cybersecurity incident until 2018. A variety of customers' personal data contained in approximately 339 million of the hotel group's global guest records is reported to have been affected. Of these records, around 30 million related to individuals in the European Economic Area and, within that, 7 million records related to individuals in the UK. The ICO commented that its investigation revealed that Marriott "failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems".

The fine ICO intends to issue highlights an area for potential privacy concerns not always on the forefront of privacy compliance - due diligence in the context of mergers and acquisitions. The ICO press release does not go into detail regarding the nature of the type of diligence Marriott should have conducted on the IT systems of its M&A target (Starwood), especially given that Starwood itself did not appear to have had any knowledge of the breach either. The ICO's statement suggests that after the acquisition Marriott did not use reasonable measures to ensure that data stored in its (and Starwood's) systems was secured, but has not provided further detail on what additional measures would have been appropriate or how such measures could have helped identify the data breach earlier. Certainly purchasers and investors will see this as a reminder to use both legal and technical experts to conduct state-of-the-art due diligence on cybersecurity and privacy matters given the potential consequences of failing to do so under GDPR. The ICO has again not detailed the basis upon which it has calculated the size of the proposed fine, but it appears to amount to approximately 0.6% of Marriott's revenues in 2018 (US$20.758 billion).

The sanctions for British Airways and Marriott may well set the tone set for future enforcement of the GDPR in the UK. This was certainly emphasised by UK Information Commissioner, Dame Elizabeth Denham, who commented in connection with the proposed British Airways fine:

> "People's personal data is just that – personal. When an organisation fails to protect it from loss, damage or theft it is more than an inconvenience. That's why the law is clear – when you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights."

The Garante — Rousseau

Though the size of the fine pales in comparison to the massive sanctions set to be handed down by the British regulator, the first GDPR sanction has recently been imposed by Italy's watchdog, the Garante. On 4 April 2019, the Italian data protection agency levied a fine of EUR 50,000 against Rousseau association, which runs the online platforms associated with the 5 Star Movement, a political party currently forming part of the Italian government. The Rousseau platform provides online direct e-voting to Italian citizens for 5 Star. An inspection of the technical and organisational measures of the same revealed continuing security concerns in violation of Art. 32 GDPR. Rousseau had already been under investigation for violation under the pre-GDPR data protection act after a data breach in 2017, which resulted in a requirement to implement a series of improvements to the technical security of the systems, as well as updates to the privacy notices. Two extensions had been given, and while the Italian DPA found that significant improvements had been made, the Garante's investigation raised concerns regarding the anonymization of voter information after votes had been cast, as well as concerns about the possibility of vote-tampering by individuals at Rousseau.

Apart from being the first decision from the Italian DPA, it is also remarkable for having been levied against a processor, Rousseau, without also charging the controller, the 5 Star Movement. While it is not news that the GDPR places processors under direct statutory liability, this direct enforcement action is the first under GDPR.

Moving Forward

Considered together, the fines issued this calendar year (of which the above are just a few examples) indicate that European regulators will not pull their punches when it comes to enforcing the GDPR, and are also willing to show the "teeth" that the GDPR was intended to provide them with. Though Google, British Airways, and Marriott have all appealed their fines, regardless of the outcome, the decisions to date serve as important indicators of the focus of regulators going forward. Further investigations are ongoing and more large fines are to be expected. It remains to be seen what effect the efforts of certain regulators to coordinate a fining matrix will have on harmonising fines across member states.

Endnotes

[1] Georgia Moorhouse is a Trainee Soliciter in Cleary Gottlieb's London office; Natalie Farmer is an Associate in Cleary Gottlieb's London office; Natascha Gerlach is a Senior Attorney in Cleary's Brussels office

[2] Under the previous UK data protection legislation, for instance, the maximum fine that regulators could impose was £500,000. Facebook was fined the maximum amount by the UKs Information Commissioner's Office (ICO) for the Cambridge Analytica scandal, despite the large number of affected data subject (up to 87 million) whose data was improperly shared with third-party developers without their consent.