GT GreenbergTraurig

Alert | White Collar Defense & Special Investigations/ Data, Privacy & Cybersecurity

July 2019

2 Intent-to-Fine Notices in 2 Days by UK Information Commissioner for GDPR Violations; Amounts Total £282 Million

It has been over a year since the General Data Protection Regulation (GDPR) came into force – and it did so with great fanfare. The GDPR had the effect of overhauling how personal data is dealt with across Europe, introducing the 'gold standard' of protection for the rights and freedoms of EU data subjects. At the same time the UK enacted the Data Protection Act 2018 (DPA).

By far the most radical change implemented by the GDPR over the previous regime was giving supervisory authorities the power to impose potentially huge fines for breaches of its provisions.

The level of fine that can be imposed depends on the nature and seriousness of the failure. GDPR Article 83 provides that in the case of a firm or company breaching the obligations imposed on it, such as the basic principles for processing personal data, the maximum fine available to the Information Commissioner's Office (ICO) is €20 million or 4% of the firm or company's total annual worldwide turnover, whichever is higher.

A Sleeping Giant No More

Unsurprisingly, the potential for such huge fines created a media furore not only in the UK but also internationally. It is only this month, however, that the ICO publicly announced its first uses of the significant firepower available to it.

The first case was revealed on 8 July when the ICO announced its intention to fine British Airways (BA) £183.39 million for 'infringements of the GDPR…[relating] to a cyber incident notified to the ICO by BA in September 2018' which led to around 500,000 of its customers' personal data being collected by a fraudulent website.

According to the ICO's statement, the incident involved BA customers being diverted to a fraudulent website where their personal details were harvested by attackers. BA Chairman and CEO Alex Cruz said that BA 'responded quickly to a criminal act to steal customers' data' and that BA found 'no evidence of fraud/fraudulent activity on accounts linked to the theft'. Mr Cruz further stated that the airline was 'surprised and disappointed' in the decision reached by the ICO.

The ICO's statement regarding the proposed fine was accompanied by stern words from Commissioner Elizabeth Denham: '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 following day, the ICO announced its intention to fine Marriott International, Inc. just over £99 million for violations of the GDPR relating to 'a cyber incident which was notified to the ICO by Marriott in November 2018'. Marriott reported the issue to the ICO when it was first discovered in November last year; according to the ICO, it is understood that the 'vulnerability began when the systems of Starwood Hotels group were compromised in 2014'. Marriott subsequently acquired Starwood in 2016.

In a statement issued by Marriott, president and CEO Arne Sorenson said, '[w]e are disappointed with this notice of intent from the ICO, which we will contest. Marriott has been cooperating with the ICO through its investigation into the incident, which involved a criminal attack against the Starwood reservation database'. The statement confirms that Marriott 'intends to respond [to the ICO notice] and vigorously defend its position'.

The Marriott case also highlights the importance of data protection issues in corporate acquisitions. ICO Commissioner Denham said, 'the GDPR makes it clear that organisations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired but also how it is produced'.

Prior to GDPR implementation, the maximum fine available to the ICO was £500,000, and it used these powers to fine companies such as mobile phone retailer Carphone Warehouse (£400,000), telecommunications firm TalkTalk (£400,000) and a social media giant (£500,000).

As significant as these fines may have been at the time, the intended penalties against Marriott and BA represent a new era of data privacy enforcement and cement the GDPR as a real game-changer for data controllers.

The potential for even more severe penalties under the GDPR means that compliance really is, as described by Ms Denham in her foreword to the ICO's 2018/19 annual report, a 'board level issue'.

Unknown Quantities

Whilst ICO statements on both proposed fines confirm that BA and Marriott cooperated with the respective investigations and made improvements to their security, the unenthusiastic reactions of both companies suggest more than a level of bemusement as to how the ICO reached its figures. In accordance with DPA requirements, the ICO has produced and published a Regulatory Action Policy to provide guidance as to how it exercises the investigation and enforcement functions afforded to it, including:

1. Information Notice – a formal request for a controller, processor, or individual to provide the ICO with information within a specified time frame to assist it with investigations (s.142 DPA 2018);

2. Assessment Notice – a notice requiring a controller or processor to allow the ICO to assess whether the controller or processor is compliant with data protection legislation, which can involve document inspection and formal interviews of relevant individuals (s.146 DPA 2018);

3. Enforcement Notice – a notice requiring a person to take or refrain from taking steps specified in the notice, where the commissioner is satisfied that the person has breached a relevant obligation (s.149 DPA 2018); and

4. Penalty Notice – a notice requiring payment of an amount by a person to the commissioner where the commissioner is satisfied that the person has breached a relevant obligation (s.155 DPA 2018).

In respect of penalty notices, the guidance makes clear that in deciding whether to impose a penalty – and if so, the amount of the penalty – the ICO will take into account a number of factors including the nature, gravity, and duration of the failure, any relevant previous failures, and the degree of cooperation with the commissioner.

The guidance further describes a five-step mechanism used by the ICO in exercising its discretion to set the amount of the penalty, subject to the maximum outlined above. The steps are as follows:

1. Removing any financial gain from the breach.

2. Adding in an element to censure the breach based on scale and severity, taking into account the above-referenced factors and the others listed in the DPA 2018.

3. Adding in an element to reflect any aggravating factors.

4. Adding in an amount for deterrent effect to others.

5. Reducing the amount to reflect any mitigating factors.

To date, the ICO has only officially indicated that the fine amounts will be determined at the end of the process. The guidance suggests that the Notices issued to both BA and Marriott should set out the findings of the investigation as well as the rationale for the proposed penalty. Both companies are now able to submit representations to the ICO, and in light of the magnitude of the fines, we expect they will be applying significant resources to this part of the process.

A Public Problem

The ICO's statements make clear that both proposed fines were made public in response to disclosures by BA and Marriott to the London Stock Exchange and the U.S. Securities Exchange Commission, respectively. This is a good example of how enforcement action against a company can impact its obligations under market-specific listing rules, even in circumstances where the enforcement action is incomplete.

In the absence of further publicised fines under the GDPR and until a final decision is reached in both cases, it remains difficult to derive any meaningful analysis of how the ICO and other supervisory authorities will proceed in future situations. Many are eager to know the extent to which the ICO is prepared to reduce the numbers following BA and Marriott's submission of representations.

Whatever the outcome, the ICO has shown that it is prepared to use the full weight of the powers given to it by the GDPR.

Until further cases come to light, the publication of the BA and Marriott fines will serve as a wakeup call to any companies yet to review their systems post-GDPR.

Authors

This GT Alert was prepared by **Anne-Marie Ottaway**, **Barry Vitou, Gareth Hall,** and **Ewen Mitchell**. Questions about this information can be directed to:

- Anne-Marie Ottaway | +44 (0) 203.349.8700 | ottawayam@gtlaw.com
- Barry Vitou | +44 (0) 203.349.8700 | vitoub@gtlaw.com
- Gareth Hall | +44 (0) 203.349.8700 | hallg@gtlaw.com
- Ewen Mitchell | +44 (0) 203.349.8856 | mitchelle@gtlaw.com
- Or your Greenberg Traurig attorney