July 12, 2019

# UK's ICO Announces Significant Fines for GDPR Violations

On July 8 and 9, 2019, the Information Commissioner's Office (ICO) – the data protection authority of the United Kingdom – announced its intention to levy substantial fines against two companies for violations of the EU General Data Protection Regulation (GDPR). These potential fines mark the first major sanctions ordered by regulators under their new powers as granted by GDPR; for more information on GDPR, please see our client memorandum "Implications of the New EU Data Protection Regime and Its Expanded Application for Non-EU Entities."

On July 8, ICO announced its intention to fine British Airways £183.39 million (about $228 million) for GDPR violations relating to a 2018 data breach. Citing "poor security arrangements" at British Airways, ICO's announcement noted that "[p]ersonal data of approximately 500,000 customers were compromised in this incident[,]" including "log in, payment card, and travel booking details as well [as] name and address information."

The announcement from ICO included a statement from Information Commissioner Elizabeth Denham highlighting the importance of a company's obligations as a data controller under GDPR and ICO's focus on enforcing the rights of data subjects:

> "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 very next day, ICO announced another intended fine, notable not only for its amount, but also because it is against an American company. In its July 9 announcement, ICO stated its intention to fine hotel company Marriott International £99.20 million (about $123 million) for violations of GDPR relating to a data breach that impacted "approximately 339 million guest records globally . . ., of which around 30 million related to residents of 31 countries in the European Economic Area (EEA). Seven million related to UK residents."

ICO indicated that while the breach may have begun in 2014 in the systems of the Starwood Hotels group, which Marriott purchased in 2016, Marriott did not discover the breach until 2018. Notably, ICO emphasized potential issues in the due diligence process when Marriott purchased Starwood, stating "ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems."

Further, it included another statement from Information Commissioner Denham on this issue:

> "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 protected."

In both announcements, ICO noted that each company had self-reported the incidents, had cooperated with ICO's investigations, and had, since then, improved its security. Each company will have an opportunity to present to ICO on the proposed fine and "ICO will consider carefully the representations made by the company and the other concerned data protection authorities before it takes its final decision."

ICO's announcements of intended actions raise a number of key points relating to data privacy:

- **Major GDPR fines are a real concern**. Companies that may have become complacent at the relative quiet from data protection authorities in the year since the enactment of GDPR should now be on notice that significant fines for failure to protect personal data are a genuine threat.
- **GDPR will be enforced internationally**. Companies hoping that data protection authorities would limit their enforcement efforts to the EU should now recognize that the GDPR's long arm is a reality.
- **Data privacy is a legal process risk for companies**. Due diligence, e-discovery, investigations, investment funds, and more may all have a component that requires consideration of the impact of data privacy laws. Companies and their counsel should be aware of this and focus efforts accordingly to manage risk relating to data privacy obligations.
- **Directors and officers should take note.** In addition to the potential financial and reputational impact of major regulatory fines, directors and officers should be aware of the potential threat of follow-on shareholder litigation, which could lead to significant exposure and corporate risk.
- **The data privacy landscape continues to evolve, both in the U.S. and abroad.** Fines and liability relating to data privacy are becoming increasingly common and will become more significant over time as new laws take effect and regulators step up enforcement. Companies should stay aware of the evolving data privacy regulatory landscape; of particular note in the U.S. are the California Consumer Privacy Act (CCPA) due to take effect in 2020 and the ongoing discussions around a potential federal data privacy law.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning
+1 212-373-3061
cboehning@paulweiss.com

Jonathan S. Kanter
+1 202-223-7317
jkanter@paulweiss.com

Brad S. Karp
+1 212-373-3316
bkarp@paulweiss.com

Jeannie S. Rhee
+1 202-223-7466
jrhee@paulweiss.com

*E-Discovery Counsel Ross M. Gotler contributed to this Client Memorandum.*