March 2024

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

British Data Protection Authority Flexes GDPR Enforcement Muscles

No longer is the bark of sanctions for lax data protection practices worse than its bite. The Information Commissioner's Office (ICO)—the United Kingdom's Data Protection Authority—has announced its intention to impose two fines totaling more than £282 million (approximately $354 million) against British Airways and Marriott International for breaching their requirements under the General Data Protection Regulation (GDPR) to safeguard personal data. The ICO had not previously issued a fine larger than £500,000.

It could have been worse. The GDPR allows fines of up to 4% of annual global revenue or €20 million, whichever is greater. Marriott's £99.2 million ($123 million) fine amounts to 2.5% of the hotel chain's global revenue, and the £183 million ($240 million) fine against British Airways represents 1.5% of the company's global revenue.

What is the GDPR and to whom does it apply?

The GDPR is the European Union's comprehensive data privacy and protection regulation, which became enforceable on May 25, 2018. Europe's privacy rules have global reach, imposing a number of obligations concerning the processing and protection of consumers' personal data on organizations located in the European Economic Area (EEA), as well as those which offer goods or services to, or monitor the behavior of, individuals located in the EEA. Chief among these obligations are the requirement that the data controller possess a legal basis to process personal data, and that collected data be safeguarded from misuse and theft.

SUBSCRIBE

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Kate Paine
Attorney
813.202.7151
kpaine@shb.com

Why is the ICO fining British Airways and Marriott?

The fines against both companies arise out of significant data breaches. British Airways suffered a data breach when its website was infected with malware that skimmed transaction details from approximately 500,000 purchasers during a three-week period in 2018. In deciding to issue the record-breaking fine, the ICO found that the large British company had failed to adequately safeguard its website and, as a result, breached its obligation under the GDPR to protect the personal data with which it had been entrusted. In an interview with the *Wall Street Journal*, Information Commissioner Elizabeth Denham cited a "lack of cybersecurity hygiene," including the company's failure to comply with Payment Card Industry (PCI) standards—specifically, the fact that the cards' CVV codes were not encrypted. In the wake of the announcement, shares in IAG, British Airways' parent company, fell by more than 1%.

The amount of the fine against British Airways is particularly noteworthy, considering no evidence of misuse of the compromised personal data has yet been linked to the breach. That said, the fact that the ICO issued a fine of 1.5% of the company's global revenue when it could have been 4% likely reflects the company's cooperation with the investigation and subsequent improvements to its data-security measures.

The fine against Marriott stems from a 2014 breach that did not actually involve Marriott's data, but rather Starwood's, which Marriott acquired in 2016. Through malware used at point-of-sale cash registers, hackers were able to gain access to 339 million Starwood guest records, including those of 30 million people in the EEA. The ICO specifically faulted Marriott for not discovering the breach while conducting due diligence during the acquisition, nor for an additional two years thereafter. Like British Airways, Marriott cooperated in the ICO's investigation.

The ICO's ruling will not be complete until the data protection authorities of the other EEA countries whose residents were affected by the breach have an opportunity to provide input. Marriott and British Airways also have the right to respond to the ICO and, according to public statements, each company intends to do so. Any fines formally imposed can then be appealed before the appropriate judicial body.

What are the takeaways for companies who handle personal data?

Previously, the largest fine imposed for a GDPR violation was the €57 million levied against Google earlier this year by CNIL, France's Data Protection Authority. (For reference, based on its

Al Saikali
Chair, Privacy and Data Security Practice
305.358.5171
asaikali@shb.com

annual global turnover, Google could have been fined nearly €4 billion.) Unlike the fines against British Airways and Marriott arising out of data breaches, Google was fined over its lack of transparency about how it was collecting and sharing user data. Whether this indicates that data protection authorities intend to impose larger fines for security breaches than for breaches involving data processing remains to be seen.

Regardless, the ICO's imposition of huge back-to-back fines, in conjunction with the potential for negative publicity and loss of consumer trust, should serve as a reminder (or at least a wake-up call) that compliance with the GDPR must be a priority for companies who handle personal data—including American companies that offer goods or services to individuals in Europe or monitor their behavior. As Denham has made clear: "[W]hen 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."

Organizations that process personal data should treat it like any other asset. This means regularly reassessing the security measures in place to safeguard the data-collection process and the data itself. In the case of a corporate acquisition, the acquiring company should—at a minimum—determine what data the company to be acquired possesses and whether that data may have been previously exposed to a security breach.