

CLIENT ALERT

ICO Announces Intention to Issue More Than \$350 Million in Fines for Data Breaches Under the GDPR

July 11, 2019

AUTHORS

Daniel K. Alvarez | **Elizabeth J. Bower** | **Henrietta de Salis** | **Elizabeth P. Gray**
Jill Guidera Brown

In two statements released this week, the UK Information Commissioner's Office ("ICO") announced its intention to fine both British Airways and Marriott International for infringements of the General Data Protection Regulation ("GDPR") in connection with data breaches reported by those companies in 2018. The proposed fines would be the two largest penalties levied against a company under the GDPR by any regulator in the UK. The ICO's announcement follows the French data protection authority's action earlier this year in which it fined Google €50 million (approximately \$56 million USD) for violations of the GDPR related to transparency and consent. (See our Client Memo on Google's fine, [here](#).) The ICO's announcements, and accompanying fines, highlight the importance of safeguarding and understanding the personal data in a company's possession, whether its own or acquired through corporate transactions.

The ICO will take account of any representations by British Airways and Marriott and other EU Member States' data protection authorities before taking its final decision.

British Airways: A Record-Setting Fine

On July 8, 2019, the ICO announced that it intends to fine British Airways £183,390,000 (approximately \$230 million USD) for violations of the GDPR related to a cybersecurity incident in which malware on the airline's website diverted user traffic to a fraudulent site where attackers were able to harvest customer details. The personal data (including credit card

ICO Announces Intention to Issue More Than \$350 Million in Fines for Data Breaches Under the GDPR

information) of approximately 500,000 customers was compromised in the incident. Following an extensive investigation, the ICO asserted that poor security measures at British Airways enabled the data breach and justified the proposed penalty. While the ICO noted that the airline has made improvements to its security program following the incident, the GDPR requires covered entities to implement appropriate security measures and to notify supervisory authorities and individuals of data breaches if certain thresholds are met. The proposed fine is by far the highest imposed under the GDPR to date, but it could have been higher. The proposed fine is equal to 1.5 percent of the airline's global turnover for financial year 2017. The GDPR permits penalties up to 4 percent of annual revenues.

British Airways, in a statement to investors by its parent company, IAG, has stated that it found no evidence of fraudulent activity on accounts linked to the incident, and that it intends to vigorously defend itself against the proposed fine.

Marriott: Spotlight on Data Security in Due Diligence

The day after its British Airways announcement, the ICO announced its intention to fine Marriott International £99,200,396 (approximately \$124 million USD) in connection with a breach of its Starwood guest reservation database that affected approximately 339 million guests. Marriott discovered and disclosed the incident in November 2018, though the compromise in Starwood's systems likely took place in 2014—before Starwood was acquired by Marriott in 2016. (See our Client Memo on security measures companies can take in the aftermath of the Marriott breach, [here](#).)

In its announcement of the proposed penalty, the ICO highlighted the importance of privacy and data security due diligence in deals to ensure compliance with the GDPR, and asserted that Marriott had failed to undertake “sufficient due diligence” and “should have done more to secure its systems” when it acquired Starwood in 2016. The UK Information Commissioner Elizabeth Denham noted: “The GDPR makes it clear that organizations 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.”

Moving Forward

Unfortunately for most companies, these announcements have raised more questions than they have answered. We will ultimately have to wait and see if the ICO will issue detailed findings and guidance on some of the specific points raised, such as what qualifies as “sufficient due diligence” in corporate acquisitions. An implication of the ICO's statement regarding its investigation of Marriott is that sufficient due diligence would have given Marriott the opportunity to, or require Starwood to, put in place adequate data security measures over customer data. The ICO has noted that Marriott has made improvements to its data security arrangements since the breaches came to light. In the meantime, these announcements reinforce that regulators intend to use their significant authority to impose fines granted by the GDPR, and the Marriott announcement, in particular, highlights that buyers and sellers alike should thoughtfully consider privacy

ICO Announces Intention to Issue More Than \$350 Million in Fines for Data Breaches Under the GDPR

and data security issues when assessing risk as part of the M&A due diligence process. And while the ICO's announcement specifically highlights this need for any deal that might involve EU personal data subject to the GDPR, it remains the case that even deals outside of the GDPR's scope should include careful review of privacy and data security issues as well, as evidenced by the 2016 Yahoo/Verizon deal in which Verizon was able to negotiate \$350 million off of Yahoo's purchase price due to previously undisclosed security breaches.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez

202 303 1125

dalvarez@willkie.com

Elizabeth J. Bower

202 303 1252

ebower@willkie.com

Henrietta de Salis

+44 20 3580 4710

hdesalis@willkie.com

Elizabeth P. Gray

202 303 1207

egray@willkie.com

Jill Guidera Brown

202 303 1217

jgbrown@willkie.com

Copyright © 2019 Willkie Farr & Gallagher LLP.

This alert is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This alert may be considered advertising under applicable state laws.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Palo Alto, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.