July 2019

GORNITZKY
80 Years of Excellence

Unprecedented Fines Under the GDPR and the Importance of Conducting Proper Data Protection Due Diligence in M&A

In less than 24 hours, the British Information Commissioner's Office ("ICO") announced its intention to impose fines totaling in more than $350 million on two companies for alleged breaches of the EU General Data Protection Regulation ("GDPR").
The ICO's statements stress the importance of conducting proper due diligence into cyber-security and privacy matters prior to acquiring a business.

In the first statement, published on July 8, 2019, the ICO announced its intent to impose a fine of approximately $230 million on British Airways regarding a cyber incident reported to the ICO by British Airways in September 2018. According to the ICO's statement, the incident involved user traffic to the British Airways website being diverted to a fraudulent site. Through the false site, customer details were harvested by the attackers and personal data of approximately 500,000 customers were compromised. According to the ICO, its investigation had found that consequent to the incident, a variety of personal information was compromised due to what the ICO considers "poor security arrangements at the company".

In its second statement published the following day, the ICO announced its intent to impose a fine of approximately $123 million on Marriott International Inc., for a cyber incident that allegedly led to the exposure of 339 million guest records (30 million of which related to EU residents). According to the ICO's statement, the vulnerability apparently originated in the systems of the Starwood hotel group, acquired by Marriott in 2016. Marriott discovered the exposure in 2018 and reported it to the ICO. In its investigations, the ICO found that Marriott failed to undertake sufficient due diligence when it acquired Starwood and should have done more to secure its systems.

In the Marriott statement, the ICO noted that as part of the accountability obligations under the GDPR, organizations must carry out proper due diligence when making a corporate acquisition. In addition, organizations must establish accountability measures

to assess not only what personal data has been acquired, but also how such personal data is protected.

The ICO's recent statements stress the importance of conducting proper due diligence into cyber-security and privacy matters in M&A transactions, especially where the acquisition or merger involves a company that processes a significant amount of personal data. These statements further emphasize the importance of corporate accountability with respect to cyber-security and the potential liability that arises when failing to demonstrate adequate accountability. In addition, they stress the need for the acquiring company to include appropriate indemnification arrangements in the purchase agreement and to ensure sufficient insurance coverage for data protection matters.

It appears that as the GDPR enters its second year of enforcement, European data protection authorities are shifting gears in enforcement and fines and one can expect additional significant fines in the near future.

For further information please contact:

Assaf Harel, Partner
assafh@gornitzky.com