Browne Jacobson

Marriott International: a look behind the ICO's £99m fine and what this means for corporate acquisitions

Last month, the Information Commissioner's Office (ICO) announced notice of its intention to fine (NOI) Marriott International, Inc. £99m for infringements of the GDPR.

05 August 2019

Last month, the Information Commissioner's Office (ICO) announced notice of its intention to fine (NOI) Marriott International, Inc. £99m for infringements of the GDPR. This was the second NOI in as many days, following hot on the heels of the NOI issued to British Airways for an eye-watering £183m.

Marriott notified the ICO of a cyber incident it discovered in November 2018. Personal data, including names, addresses, passport numbers and encrypted payment card numbers contained in approximately 339 million guest records globally, were exposed by the incident. This is a classic data breach and the proposed fine is dwarfed by the BA fine, but what is of particular interest here is that Marriott inherited this breach as a result of a corporate acquisition.

The ICO has stated its belief that the vulnerability began in 2014, when the IT systems of Starwood Hotels and Resorts Worldwide LLC, a subsidiary of Marriott, were compromised. Marriott did not acquire Starwood until 2016, but the ICO did not see this as a mitigating factor. In fact, the ICO specified that Marriott had failed to undertake sufficient due diligence on Starwood at the time of the acquisition, with Information Commissioner Elizabeth Denham stating:

"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."

Marriott will make representations to the ICO in an effort to reduce the fine. The ICO will also take into consideration any representations from its equivalent bodies in the other affected countries of the EEA.

Whatever the final outcome, it is clear that the ICO is unlikely to excuse businesses that have inherited an existing data breach through a corporate acquisition, meaning the importance data protection due diligence (in the form of both legal due diligence and technical IT due diligence) when acquiring businesses cannot be overstated. If your business is buying a company, the scope of the due diligence exercise should be clearly defined at the outset, taking into account the nature of the target business and the likely risks it will face from a data protection perspective. Purchasers need to adopt a robust attitude throughout the due diligence exercise, seeking contractual protection in the acquisition documents following that diligence, and ensuring that all 'post-Completion' resolutions are actioned and completed as soon as possible following completion of the transaction.

Contact

Mark Hickson

Head of Business Development

onlineteaminbox@brownejacobson.com

+44 (0)370 270 6000

Related expertise

Commercial law

Criminal compliance and regulatory

Data protection and privacy

Dispute resolution and litigation