ICO announces intention to fine Marriott hotel group over £99 million for data breach

Date : July 9, 2019

Introduction

Hot on the heels of its announcement of its intention to fine the airline B.A. £183.39 million for a data breach (which Cordery reported on here: http://www.corderycompliance.com/uk-dpa-to-fine-ba-for-data-breach/) the ICO has also issued a notice of its intention to fine the hotel group Marriott International ("Marriott") £99,200,396 for a data security breach.

It is important to stress that this is an intention to fine, i.e. it is not yet a fine. Both Marriott and other EU Data Protection Authorities (DPAs) can now make comments (this is a case that falls under the GDPR "one-stop-shop" system) before any final decision is taken by the ICO.

What's it all about?

This matter concerns a cyber-security incident where various personal data contained in some 339 million guest records globally were exposed – around 30 million related to residents of 31 countries in the European Economic Area including 7 million relating to UK residents.

According to the ICO, the "vulnerability" seems to have occurred when the systems of the Starwood hotels group ("Starwood") were compromised in 2014. Marriott later acquired Starwood in 2016 but the exposure of customer information was not discovered until 2018. Marriott notified the ICO of the incident in November 2018.

What are the regulator's findings?

The ICO's investigation has concluded that Marriott failed to undertake sufficient due diligence when it purchased Starwood and it should also have done more to secure its systems. In a statement signaling that the ICO won't flinch from taking strong action where necessary, the Information Commissioner Elizabeth Denham said: "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".

The ICO had made it clear that Marriott has co-operated with the ICO investigation and has made improvements to its security arrangements. In terms of next steps Marriott now has the opportunity to make representations to the ICO as to the proposed findings and sanction – it is understood that Marriott will contest the ICO's intended fine and defend itself accordingly.

The ICO's announcement can be found here: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

Are there any other possible consequences?

Statements from lawyers contemplating bringing a class-action case against Marriott can be expected. We've previously written about this particular issue here http://www.corderycompliance.com/data-protection-breaches-and-compensation-litigation-issues-for-consideration/.

Have there been other GDPR fines, including for security breaches?

Yes. For example, Portugal had one of the first GDPR cases involving a fine of €400,000 for Centro Hospitalar

Barrerio Montigo for breaching the security provisions of GDPR (amongst other violations). The Google case in France, which was mostly for breaches of the requirements of the transparency principle, currently remains the largest public GDPR fine (for more on this see here http://www.corderycompliance.com/french-data-protection-authority-fines-google-e50m-for-violations/).

What are the takeaways?

Organisations clearly need to undertake thorough due diligence when making a corporate acquisition. For example, during the due diligence process, a buyer will need to investigate the target business' data protection compliance including its security systems and when negotiating a share purchase agreement or asset purchase agreement including post-migration of personal data.

Organisations clearly also need to make sure that they do all that they can to stop data breaches, including making sure they can react to data breaches quickly when they happen - therefore they must have a first-rate strategy and proper tools in place for responding quickly when these incidents do happen.

Cordery's Breach Navigator can help organisations respond to a breach and assess its consequences. There are more details here https://www.corderycompliance.com/solutions/breach-navigator/.

For more information on GDPR see details of Cordery GDPR Navigator here www.bit.ly/gdprnav.

For more of our reporting about data protection issues, including breaches see here http://www.corderycompliance.com/category/data-protection-privacy/ and here http://www.corderycompliance.com/category/cyber-security/.

For more information please contact André Bywater who is a lawyer with Cordery in London where his focus is on compliance issues..