Client Alert: BA & Marriott Data Breaches ICO Fines Finalisation Now Expected August-September 2020

Date : May 14, 2020

Introduction

In the summer of 2019 the UK's data protection regulator the ICO announced its intention to fine the airline British Airways (BA) £183.39 million (around $225 million) and the hotel group Marriott International (Marriott) £99.2 million (around $122 million) for respective data breaches. Although this process was expected to have been completed a few months after this announcement, it became more drawn out. Although no official statement has been made by the ICO, it is now understood that there have been more delays. We now expect the fines to be finalised in August-September 2020. We looked at earlier announcements in connection with delays in both of these cases in our alert in January here http://bit.ly/bagdpr3.

What's this all about?

The BA matter relates to an incident that it notified to the ICO which involved in part website traffic being diverted to a fraudulent site. The rogue site harvested customer's details and personal data of approximately 500,000 customers were compromised, which is believed to have begun in June 2018. The ICO's investigation found that a variety of information was compromised by poor security arrangements at the company including log in, payment card and travel booking details as well as name and address. You can read more about that case here https://www.corderycompliance.com/uk-dpa-to-fine-ba-for-data-breach/

The Marriott matter relates to an incident that it notified to the ICO where personal data contained in some 339 million guest records globally had been exposed. The issue seems to have occurred when the systems of the Starwood hotels group were compromised in 2014. Marriott acquired Starwood in 2016 but the exposure of customer information was not discovered until 2018. The ICO's investigation concluded that Marriott failed to undertake sufficient due diligence when it purchased Starwood and it should also have done more to secure its systems. There is more on the Marriott case here https://www.corderycompliance.com/ico-intention-to-fine-marriot-99-million-for-data-breach/.

What's next?

Both BA and Marriott then had the opportunity to make representations to the ICO as to the proposed findings and sanction. The ICO confirmed later that it had received representations from both companies which it was considering in deciding what to do about any possible penalties, and an extension until the end of March 2020 was granted. This process then seems to have been extended to May-June 2020. It is now understood that, mainly because of the Covid-19 pandemic, the ICO, BA and Marriott had all mutually agreed to extend the deadline for finalising the amount of the fines both companies will have to pay. Our understanding is that whilst still emphasising the seriousness of the breaches, the ICO will apply a lenient approach to the amount of the fines due to the financial impact of Covid-19.

What are the takeaways?

As we've said before, the pandemic will have an impact on GDPR enforcement. Our thoughts on the ICO's guidance for enforcement in the pandemic are here https://bit.ly/icocovid.

Pandemic aside, the time being taken to resolve these two cases is raising more questions than answers. Although the impact of Covid-19 may explain some of the current continued delay, quite why what may end up being over a year to resolve these matters since the ICO announced its intentions to fine may leave some wondering whether GDPR enforcement is going as quickly as it should. In addition, what was also expected to be a showcase for the first significant fines under GDPR in the UK may now be a let-down. Might it even give the organisations concerned a market advantage that they wouldn't ordinarily have? And as we said in January, Brexit now adds additional

complications (see here http://bit.ly/bagdpr3). Even if the fines end up being lower however, neither organisation is likely to escape unscathed – as we've mentioned before, litigation has been threatened on behalf of victims and the reputational damage is likely still to stick whatever the eventual regulatory result.

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- Detailed guidance on the security aspects of GDPR in paper and on film;
- A template data breach log;
- A template data breach plan; and,
- A template data breach reporting form.

For information about our Breach Navigator tool please see here: https://www.corderycompliance.com/solutions/breach-navigator/

We report about data protection issues here: http://www.corderycompliance.com/category/data-protection-privacy/. For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/ and our Data Protection Glossary which can be found here: http://www.corderycompliance.com/?s=glossary.

For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com

Image courtesy of BA news