19 July 2019 No.229

3HR Legal Weekly

Commercial

Massive GDPR fines begin

In the last few weeks, the Information Commissioners Office (ICO), the government's data protection regulator, has indicated that it intends to fine the Marriot hotel group and British Airways £99,200,000 and £183,000,000 respectively for recent data protection breaches.

These fines show the massive increase in power the ICO has under the GDPR, and emphasise how important your continued compliance is. Gone are the days when the ICO only had the power to levy a maximum fine of £500,000. Fines of 20,000,000 Euros or 4% of global turnover (whichever is the larger) are quickly becoming common.

In addition, the FTC has said that it will be giving Facebook a fine of up to $5 billion for privacy violations related to Cambridge Analytica. It is inevitable that the ICO will also be focussing on Facebook and that fines under the GDPR will follow.

Both the Marriot and BA data breaches related to inadequate IT security and systems, so it is important to review and consider whether your current setup is adequate, or needs replacing or reinforcing to ensure your stored data is secure.

The Marriot fine will be particularly difficult for the company to accept, as it related to a faulty customer management system operated by a separate hotel chain, Starwood, which it bought in 2016. The compromised data belonged to 30,000,000 people who had stayed at the Starwood hotels.

The BA fine resulted in a website hack that re-directed passengers from BA's corporate website to a fraudulent site, which collected personal data while pretending to be the official BA site. 500,000 users were impacted.

Other recent fines include £400,000 for illegally sharing data between companies, £40,000 for sending marketing emails to customers without consent, £90,000 for nuisance telephone calls, and £100,000 for sending direct marketing messages without proper consent.

However, even though the BA and Marriot fines are related to IT systems, technology is not the only area that needs your attention. Data protection compliance is an ongoing and ever-changing responsibility. It is helpful that we now have a year of post-GDPR guidance from the ICO and the European Data Protection Board. It will assist when you carry out your annual reviews of what you have been doing and will help update your processes and documents accordingly.

There are many areas that need regular attention. Can you securely dispose of any data to remove the risk of it being breached? Have your privacy notices been updated? Have you fully implemented your GDPR documentation? Are your privacy notices and policy documents being used by staff? Have you made any changes in your processes that may necessitate looking again at how compliant you are? Do you now have processes in place to ensure that you are disposing of older data in accordance with your retention policy?

Have you checked whether you could shorten any of the periods that you set in that retention policy? Are you carrying out any 'high risk' processing which would need documenting? Have you provided training for new and existing staff? Does your data breach reporting system work properly so you would be able to report any breaches to the ICO within the required 72 hours? These are just a few of the points you should think about.

As the stakes are so high, it is important that you take action to avoid the consequences of breaching data protection law. If you require advice in relation to data protection, or an annual review, please contact the commercial department at 3HR Corporate Solicitors.

If you would like to read more about the Marriot and BA fines, please click here: https://www.bbc.co.uk/news/technology-48928163

Richard Hull
Senior Commercial Solicitor
E: richard.hull@3hrcs.com