UK Data Protection Regulator Announces Intention to Fine BA after Data Breach

Date : July 8, 2019

Introduction

The UK Data Protection Regulator has announced her intention to fine BA (also known as British Airways) after its data breach. She intends to fine the airline £183.39m. It is important to note that this is an intention to fine – not yet a fine – both BA and other EU Data Protection Authorities (DPAs) can now make comments.

You can find out more about GDPR in our FAQs here www.bit.ly/gdprfaq

What is this about?

The proposed fine relates to a cyber incident notified to the ICO by British Airways in September 2018. This involved in part website traffic being diverted to a fraudulent site. The rogue site harvested customer's details. Personal data of approximately 500,000 customers were compromised in this incident, 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 information.

What did BA do?

BA reported the incident to the ICO in compliance with its obligations under GDPR. It made improvements to its security arrangements and it altered its website.

Is this the first GDPR fine for a security breach?

No. If the fine follows it will be the largest so far under GDPR but not the first. In The Netherlands, as at January 2019, the Dutch DPA had taken action against 298 organisations who had reported a data breach and one of the most widely reported cases from Portugal was 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 Portuguese DPA's findings included the fact that there were 985 users of the hospital's IT systems associated with the profile 'doctor' for a hospital that employed only 296 doctors.

The Google case in France, which was mostly for breaches of the requirements of the transparency principle, remains the largest public GDPR fine. There are more details of the Google case here http://www.corderycompliance.com/french-data-protection-authority-fines-google-e50m-for-violations/ .

What happens next?

The ICO will now hear representations from BA. In this case the ICO is also acting as the lead authority across the EU for other DPAs. As a result she will now consult with other DPAs in addition.

BA has said this morning that the fine is equivalent to 1.5% of BA's worldwide turnover for 2017. BA is likely to make representations to the ICO (or even to appeal once the fine is levied) on that basis if it feels that the ICO has over-estimated the breach. BA said this morning that there was no evidence that any of the data compromised had been misused (although this has been disputed by some since BA's announcement). There are a number of options open to BA if the ICO levy the fine and BA chooses to contest it. In some respects the GDPR fining mechanism is based on the EU's competition law regime. In many cases successful challenges have been brought to the courts in Europe against regulatory fines and the indications are that appeals against GDPR fines might follow the same path.

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.

As well as regulatory activity we can certainly expect to see statements from lawyers contemplating a class action against BA. We've talked a bit about that here http://www.corderycompliance.com/data-protection-breaches-and-compensation-litigation-issues-for-consideration/. We understand that a hearing is scheduled for 4th October in the High Court in London to set out the next steps in that litigation. According to lawyers involved in that action 5,500 potential claimants have so far committed to that case with more having contacted the firm since today's announcement.

Conclusion

Organisations need to make sure that they do all that they can to stop data breaches. They also need to make sure they can react to data breaches quickly when they happen. If a fine is levied at these levels it will be an important sign to organisations that the ICO is serious about security. This was an incident where criminals focused on BA's website. The ICO has decided however that organisations must do all that they can to protect their systems - including their websites. Any organisation can be the target for this type of attack. 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 information please contact Jonathan Armstrong or André Bywater who are commercial lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com

André Bywater

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.

Image courtesy of BA

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.