Blog: Is the BA Fine in the Departure Lounge?

Date : January 6, 2020

This blog was written in January 2020. Please note that the extensions mentioned in this alert have been extended further to May in the case of BA and June in the case of Marriott

Last week we talked about the UK's first fine under GDPR. You can read our alert on that here https://www.corderycompliance.com/first-uk-gdpr-fine/. We mentioned in that alert that the two big Notices of Intent against BA and Marriott were not fines just yet and that the Information Commissioner's Office (ICO) had extended its time to deal with both of them until 31 March 2020. So what is the current position?

The first thing is to say there are lots of issues involved. This blog will cover some though it's not a comprehensive analysis of the full legal position.

What is this about?

Last year both BA and Marriott told their respective stock exchanges that a Notice of Intent had been issued by the ICO regarding a data breach. In the case of BA the amount of the proposed fine was £183.39m and in Marriott's case £99.2m. It's important to remember that it was the organisations concerned, not the ICO, who initially made this public.

You can read more about the BA case here https://www.corderycompliance.com/uk-dpa-to-fine-ba-for-data-breach/ and the Marriott case here https://www.corderycompliance.com/ico-intention-to-fine-marriot-99-million-for-data-breach/.

Whilst any fine would be for breach of GDPR, technically the fines (called Monetary Penalties) would be levied under UK legislation in this case, the Data Protection Act 2018 (DPA 2018). There's a list of things in s.155 DPA 2018 the ICO needs to take into account when setting the penalty and this includes some things which might require quite a bit of investigation including "*any action taken by the controller or processor to mitigate the damage or distress suffered by data subjects*" and "*the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by the controller or processor* …"

Steps like an analysis of the technical and organisations measures (TOMs) in place at the time of breach and how they might be improved are key in the investigation of any data breach. We've handled approaching 100 data breaches and it's a key step in the process we use. You can find out more about our process and the tools we use when responding to data breaches here https://www.corderycompliance.com/solutions/breach-navigator/. For example with our automated tool Cordery Breach Navigator an organisation will look at remediation and mitigation as part of its analysis and reporting procedure.

What did the ICO say?

The ICO has responded to Freedom of Information requests about the delay in dealing with both cases. On 21 November 2019 it said "*The ICO, as a general position, does not comment on our investigations as this may prejudice our regulatory function. We will usually publish any enforcement action on our website when it is appropriate to do so*." The ICO confirmed in that response that it had received representations from both companies which it was considering "*The Information Commissioner is considering those representations in deciding whether to give a penalty notice, and the amount of the penalty if a penalty notice is given*." We understand that the ICO has more recently confirmed to Mischon de Reya that an extension has been agreed in both cases until 31 March 2020.

What is the reason for the delay?

The ICO has not confirmed the reason for the delay. There are a number of possibilities. They include:

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.

1. In cases like this the ICO is not the only relevant regulator. One of the key aspects of GDPR is co-operation and consistency. The aim is to reach 'consensus' amongst relevant regulators in other EU countries (called Supervisory Authorities in GDPR but more commonly referred to as Data Protection Authorities or DPAs). We've heard rumours that there have been delays at an EU level and it might be that the delay is to accommodate other DPAs' views. GDPR Article 60 has a fairly complicated process for sharing draft decisions in cases like this giving the other DPAs set periods to consider and make submissions.
2. These are also likely to be fairly complex cases. As we've said before cases like this always involve an investigation of the technical and organisational measures (TOMs) an organisation had in place prior to the breach. The Doorstep Dispensaree case also suggests that the ICO will be prepared to take into account mitigation and remediation measures the organisation has put in place after the breach. This could involve a fairly detailed technical analysis of new security measures, steps taken to harden ecommerce and booking systems and a review of new organisational structures and warning systems put in place after the breach.

In short then it's not too surprising that the ICO's investigation is taking some time. Although much of the initial work was done before the Notice of Intent was served it is likely that detailed representations have been made by both companies since.

What about Brexit?

One of the other interesting aspects of this case is that, if things go according to the UK Government's plan, the UK will have left the EU by the end of March. The UK will still have data protection law and DPA 2018 will still be in force but this will add some complexity. For example if a deal is not done with BA and Marriott and they appeal their fines will the UK courts have to interpret GDPR matters alone and without guidance from the European courts? Will that delay any appeal proceedings?

We made a film last year about the data protection position after Brexit. You can watch that film here https://www.corderycompliance.com/hard-brexit-and-data-protection/.

Conclusions

As you'll see some of the issues involved are complex and I've just scratched the surface a little in this blog. The result in both cases is likely to be fascinating and as we said in July if the level of fines isn't reduced appeals seem likely. In fact the chances of an appeal are even more likely now than they were in July with the settlement of Facebook's appeal in October. Given the time this is taking and the fact that extensions seem to have been agreed there's room for speculating that the eventual fines might end up less that the Notices of Intent. All of this underlines one other point – it's always premature to regard a Notice of Intent as a fine. In the UK's only GDPR fine to date, Doorstep Dispensaree was fined £275,000 against an initial Notice of Intent which proposed a fine of £400,000. The UK Treasury should not be planning to spend the full £282m these cases could bring any time soon.

Resources

There is more information about this and other data protection topics in Cordery's GDPR Navigator subscription service. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at www.bit.ly/gdprnav.

You can see the ICO's FOI statement here http://bit.ly/37GoeGU. Details of the response to Mischon de Reya are here http://bit.ly/2twgRD2. Details of the Facebook appeal are here https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/statement-on-an-agreement-reached-between-facebook-and-the-ico/.

For more information please contact Jonathan Armstrong at Cordery in London where his focus is on compliance issues.

Jonathan Armstrong
Cordery

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.

Lexis House
30 Farringdon Street
London EC4A 4HHOffice: +44 (0)20 7075 1784
jonathan.armstrong@corderycompliance.com

News 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.