ICO Fines Heathrow For Lost Memory Stick

Date : October 15, 2018

What is this about?

The UK's data protection regulator, the Information Commissioner's Office (ICO) has fined Heathrow Airport £120,000 for a data security breach committed through the loss of a memory stick which contained sensitive personal data about staff.

What is the background to the case?

In October 2017 a member of the public found a USB memory stick in Kilburn, West London, and then put it in a local library's computer where they accessed the stick's files, which were neither encrypted nor password protected. The individual then provided the stick to a national newspaper.

The stick had on it 76 folders with over 1,000 files originating from Heathrow airport. Only 1% of the information comprised sensitive personal data but this included a training video containing names, dates of birth, vehicle registrations, nationality, passport numbers and expiry, roles and mobile numbers of 10 individuals involved in a particular greeting party, and the details of between 12 and 50 (exact number unconfirmed) Heathrow aviation security personnel including names, job titles and identification of two individuals who were trade union members or chairs.

What did the ICO decide?

Having heard about the matter via the media, the ICO began an investigation.

Although the amount of sensitive personal data comprised less than 1% of the information on the stick because of the way the information was captured and displayed, and so would not be readily available or searchable, the ICO concluded that a motivated individual could nevertheless locate and extract the data in a more permanent form such as a screenshot.

Heathrow had in place policies that provided guidance about the use of removable media including one statement that stated "Only use encrypted removable devices (e.g. USBs) approved by Heathrow and only use them if there's no alternative."

Heathrow had limited data protection training in place and estimated that only 2% of its 6,500 staff had received data protection training, being those deemed to be at greatest risk of exposure to personal data – this despite Heathrow's Information Security Policy stating that "All staff, and suppliers working on [Heathrow] site, shall have regular and appropriate information security awareness, training and guidance". Further, such training was not in place for security trainers, including the staff member who had lost the stick (in transit whilst commuting to or from work). In addition, there were no digital safeguards in place aimed at preventing the use of unauthorised media.

The ICO therefore concluded that Heathrow had failed to undertake appropriate technical and organisational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data in serious contravention of the then existing UK data protection rules. The ICO also determined that Heathrow had failed to take a number of reasonable steps to prevent contravention of the rules including: encryption of personal data on removable devices; monitoring compliance with policies, guidance and procedures concerning information security and the use of removable media; and, the provision of adequate data protection training to staff – the 2% staff trained figure was considered an aggravating feature and described by the ICO as "the lowest the Commissioner has seen in her experience".

What are the takeaways?

The main takeaway is that businesses should question whether they should be allowing staff to use such

removable storage media, which are easily lost and therefore expose a business to high risk – internal policies should therefore be reviewed. A second takeaway is that businesses should review their training with a view to ensuring that all staff are thoroughly trained on keeping data secure (keeping copies of the training records) and that compliance policies etc. must be monitored.

As mentioned above, this case was decided under the previous UK data protection legislative regime but it is likely that the same result would be arrived at under the new data protection regime (EU General Data Protection Regulation [GDPR] & the UK Data Protection Act 2018) and would constitute a breach of the integrity and confidentiality principle (Article 5(1)(f) of GDPR). Further, under the new regime fines can be imposed of up to 4% of global turnover or Euro 20 million, whichever is greater – had this matter been decided under the new regime the fine could therefore have been a lot higher.

The ICO's decision can be found here: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/heathrow-airport-limited-fined-120-000-for-serious-failings-in-its-data-protection-practices/

Cordery's Data Breach Academy can be an effective way of helping manage a data protection breach. There are details here: http://www.corderycompliance.com/cordery-data-breach-academy-2-2/. To find out more about the work we do in connection with data breaches and our four point plan, visit our website here: http://www.corderycompliance.com/dealing-with-a-breach/.

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/.

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 more on Navigator please see here: http://www.corderycompliance.com/solutions/cordery-gdpr-navigator/.

For more information please contact André Bywater or Jonathan Armstrong who are commercial 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