

**DATA PROTECTION ACT 1998**

**SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER**

**MONETARY PENALTY NOTICE**

To: Heathrow Airport Limited

Of: The Compass Centre, Nelson Road, Hounslow, Middlesex, TW6 2GW

1. The Information Commissioner ("Commissioner") has decided to issue Heathrow Airport Limited ("HAL") with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA"). The penalty is being issued because of a serious contravention of the Seventh Data Protection Principle by HAL.
2. This notice explains the Commissioner's decision.

**Legal framework**

3. The DPA implemented European legislation (Directive 95/46/EC) aimed at the protection of the individual's fundamental right to the protection of personal data. The DPA must be applied so as to give effect to that Directive. Both the DPA and the Directive have since been repealed with effect from 25 May 2018. However, sections 55A, 55B, 55D and 55E of the DPA continue to apply for the purposes of the present case, since the Commissioner considers it appropriate to serve this Notice of Intent in respect of contraventions of section 4(4) of the DPA taking place before 25 May 2018: see Data Protection Act 2018, Schedule 20, Part 7, paragraph 38(1)(c).

4. HAL is a data controller, as defined in section 1(1) of the DPA in respect of the processing of personal data. Section 4(4) of the DPA provides that, subject to section 27(1) of the DPA, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which he is the data controller.

5. The relevant provision of the DPA is the seventh data protection principle which provides, at Part I of Schedule 1 to the DPA, that:

*"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".*

6. Paragraph 9 at Part II of Schedule 1 to the DPA provides that:

*"Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to –*

*(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and*

*(b) the nature of the data to be protected".*

8. Under section 55A (1) of the DPA the Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that –

(a) there has been a serious contravention of section 4(4) of the DPA by the data controller,

(b) the contravention was of a kind likely to cause substantial damage or substantial distress, and

(c) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the data controller –

(a) knew or ought to have known –

(i) that there was a risk that the contravention would occur, and


(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

(b) failed to take reasonable steps to prevent the contravention.

9. The Commissioner has issued statutory guidance under section 55C (1) of the DPA about the issuing of monetary penalties that has been published on the ICO's website. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 prescribe that the amount of any penalty determined by the Commissioner must not exceed £500,000.

**Background to the case**

10. HAL describes itself as “the UK’s premier airport” from which “some 80 airlines fly direct to over 180 destinations worldwide”. According to HAL’s annual report and financial statements for the year ending 31 December 2016 Heathrow is Europe’s busiest airport and the world’s seventh busiest airport. It employs approximately 6,500 staff.
11. On 16 October 2017 a member of the public found a USB memory stick in Kilburn, West London.
12. The individual took the USB memory stick to a local library where they plugged it into a computer and accessed files, which were not encrypted or password protected.
13. The USB stick held 76 folders and over 1000 files originating from HAL. Approximately 1% of the information comprised personal data, including sensitive personal data. In particular, the stick held 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 also 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. The information was visible for approximately three seconds within the video wherein a page of an open ring binder (containing the information) was erroneously captured by the video. The Commissioner has noted HAL’s submission that the personal data in fact comprised less than 1% of the information on the USB stick given the way it was captured and displayed, and as a result would not be readily available or searchable, but she considers that a motivated individual could locate and extract the data in a more permanent form, for example by way of screenshot.

14. Following discovery of the information the individual contacted a national newspaper ("the newspaper") and handed over the USB stick on 21 October 2017.
15. On 26 October 2017, the newspaper informed HAL that it was in possession of the USB stick, which it returned to HAL the following day. The newspaper had already taken and retained a copy of the USB stick without HAL's knowledge or consent, and which it declined to return or destroy despite requests by HAL. 
16. The Commissioner first became aware of the incident on 29 October 2017 via the media, and on 30 October 2017 contacted HAL asking for information about the matter. On that same day HAL had established that personal data was contained on the USB stick (a fact which was previously unknown from media reports) and accordingly agreed to provide the Commissioner with further information to assist her enquiries which it did by way of a follow up call on 2 November 2018, and completion of a breach notification form on 7 November 2017.
17. HAL's own investigation into the matter indicated that the data contained on the USB stick had been compiled by an employee security trainer whom HAL has stated was in a "relatively junior position by grade". The personal data held on the stick was contained within a training video, and whilst relevant to the employee's role, was unauthorised, and the existence of which HAL was unaware.

18. It appears from HAL's investigation that the USB stick was lost in transit when the staff member was commuting to or from their place of work.
19. HAL reported the matter to the police on 26 October 2017 having been informed of the incident by the newspaper. Police confirmed that the device at the public library where the USB stick files were viewed had not retained a copy of the files. At the same time, HAL also mobilised its security team to ensure the security and containment of the data, and suspended the staff member involved whilst an internal investigation was completed.
20. In response to the incident, on 31 October 2017, a companywide instruction was issued directing staff to locate any memory sticks in their possession, delete any files contained on the devices and then transfer the data or destroy the device according to advice provided by HAL's IT department.
21. HAL also notified and worked with other relevant regulatory and advisory bodies in relation to the incident, and engaged third party specialists to monitor the internet and the 'dark web' for indicators that the breach had spread further or that documents were being traded online. So far as the Commissioner understands there has been no indication that the information has been further disseminated or accessed by anyone other than the member of the public and the newspaper.
22. At the time of the incident the use of removable media to transport data was widespread across HAL, however HAL had limited measures in place to maintain oversight of data being removed from its systems. Indeed, HAL's own investigation report stated that "subsequent review

has identified that there are no technical barriers to employees uploading sensitive data to removable devices and colleagues across many areas of the airport are using a combination of personal and Heathrow issued data sticks in order to port files between locations and devices". It further stated that it "cannot state exactly what, if any, personal data has been recorded onto personal flash drives in the past".

23. At the time of the incident HAL had in place policies including an 'Information Security Policy' and 'Acceptable Use Policy'. The latter, implemented on 30 May 2017, provided specific guidance regarding the use of removable media. It stated: "Data stored on removable media is solely the responsibility of the person who creates or maintains it. Removable media is inherently insecure and vulnerable to malware infection, as such its use should be minimised wherever possible. If removable media is used users are responsible for safeguarding such equipment and must take all responsible precautions to prevent theft, loss, damage or other hazards to such items consistent with the sensitivity of the stored data (confidential data should always be encrypted, never be left unattended where other individuals may have access to it) when at rest, in transit or at remote location."
24. HAL had previously made guidance available to staff between 2013 and 2016 via its intranet regarding the risks associated with sensitive information and the use of removable media such as: "The loss or theft of sensitive information on removable media can have severe financial penalties and lead to significant reputational damage – imagine the headlines" and included such rules as: "Protect sensitive files with passwords", "Don't copy if you don't have to. Put sensitive files on removable media only when necessary" and "Keep removable media secure. Never leave them unattended in offices, public places, or in vehicles". HAL submitted to the Commissioner that at the time of the

incident this guidance had been temporarily held on an older internal website, but still accessible by staff. However she considers existence of guidance on an outdated intranet site was insufficient to ensure its existence was brought to the attention of its staff.

25. In October 2016 HAL made available a message via its intranet site which stated: "Think twice before saving files onto USB sticks or other media that can be lost or stolen".
26. Prior to the incident employees also had access to its 'Stay Safe Online' guidance via HAL's current internal website which has replaced the guidance detailed in paragraph 24 above. This guidance includes statements such as: "Only use encrypted removable devices (e.g. USB's) approved by Heathrow and only use them if there's no alternative".
27. At the time of the incident HAL had limited data protection training in place. There were no specified documented processes for determining which staff should receive training or for monitoring uptake; HAL informed the Commissioner that its data protection manager made 'thought based determinations' as to which groups of employees had the greatest exposure to personal data and a strategy for training devised accordingly. HAL estimated that only 2% of its 6,500 employees had received data protection training, being those deemed to be at greatest risk of exposure to personal data. It also confirmed that such training was not in place for security trainers, including the staff member involved in this incident.
28. The Commissioner has made the above findings of fact on the balance of probabilities.



29. The Commissioner has considered whether those facts constitute a contravention of the DPA by HAL and, if so, whether the conditions of section 55A DPA are satisfied.

**The contravention**

30. The Commissioner finds that HAL contravened the following provisions of the DPA:
31. HAL failed to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data in contravention of the Seventh Data Protection Principle at Part I of Schedule 1 to the DPA.
32. HAL also failed to comply with the requirements set out in paragraph 9 at Part II of Schedule 1 to the DPA.
33. The Commissioner finds that the contravention was as follows:

HAL did not take steps to ensure that personal data on its network was secured to a suitable standard due to gaps in the technical and organisational measures in place at the time of the incident, in particular:

- HAL failed to have in place any or any adequate technical controls to prevent downloading of personal data onto unencrypted removable media. HAL submitted that standard access controls were in place to prevent unauthorised access to data, however the Commissioner notes (and which is accepted by HAL) that it had no specific control to

disable the ability to download data onto unauthorised or unencrypted media. The Commissioners position is that it would be reasonable to expect an organisation such as HAL to implement such controls, given that it was aware that the use of both HAL issued and personal removable media was widespread across the organisation (see paragraph 22);

- HAL failed to have in place adequate organisational measures to prevent staff using personal devices to remove personal data from HAL systems;
- HAL had no control as to whether devices used were secured to an appropriate standard and had no record or control over the number of devices used containing personal data;
- HAL failed to encrypt or password protect the data contained on the USB stick;
- HAL failed to provide staff with any, or any sufficient training in relation to data protection and information security;
- HAL failed to monitor and ensure compliance with existing policies and guidance in relation to the use of removable media. HAL had relevant policies and guidance in place however these were not adhered to; it is particularly noteworthy that HAL was aware that there was widespread use by staff of personal removable media (see paragraph 22) in contravention of its own policies and guidance (see particularly Paragraph 26);

This was an ongoing contravention until HAL took remedial measures to contain the data (see paras 15 & 20 above).

- 34. The Commissioner is satisfied that HAL was responsible for this contravention.
- 35. The Commissioner has gone on to consider whether the conditions under section 55A DPA were met.

**Seriousness of the contravention**

- 36. The Commissioner is satisfied that the contravention identified above was serious.
- 37. This is because the USB stick contained personal and sensitive personal data, including passport details, nationality and trade union membership which was not secured to a suitable standard due to systemic gaps in the technical and organisational measures in place at the time of the incident. In the circumstances, the Commissioner considers that the contravention was serious having regard to the nature of the personal data involved. Given that HAL is Europe's busiest airport, where high level security should be inherent, loss or unauthorised disclosure of personal data of staff could have presented a greater risk if found by individuals who had not handled the data responsibly.
- 38. Furthermore, the Commissioner considers that the contravention was serious as insufficient measures were in place to control the use of removable media to transfer personal data held on its systems, despite apparent widespread use of such devices across the organisation (including personal devices in contravention its own policy and guidance (see paragraph 26)).

39. The Commissioner is therefore satisfied that condition (a) from section 55A (1) DPA is met.

**Contraventions of a kind likely to cause substantial damage or substantial distress**

40. The relevant features of the kind of contravention are loss of an unencrypted USB stick containing personal data during transit due to inappropriate technical and organisational measures taken by the data controller. The data comprised personal details of 10 individuals involved in a particular greeting party and between 12 and 50 aviation security staff. Some of the data, pertaining to trade union membership for two individuals, was sensitive personal data.
41. The Commissioner considers that the contravention identified above had the following potential consequences:
42. The contravention would cause distress to the data subjects whose personal and sensitive personal data has been disclosed to a recipient who has no right to see that information.
43. Further, the data subjects would be distressed by concerns that their data has been further disseminated, even if those concerns do not actually materialise. Whilst the member of the public who found the USB stick and the newspaper have given assurances that they have not further disseminated the information, an encrypted copy of the personal data remains secured by a third party under an access control agreement, and so individuals may (rightly or wrongly) perceive that there is potential for the data to be accessed by the newspaper and/or HAL and disseminated in the future.

44. If this information has been misused by those who had access to it, or if it was in fact disclosed to untrustworthy third parties, then the contravention would cause further distress and also substantial damage to the data subjects such as exposure to the risk of identity fraud. Indeed, HAL advised the Commissioner during the course of her investigation: "the information relating to the 10 people in the [...] greeting party is sufficiently detailed to facilitate identity fraud". Whilst HAL submitted that from searches conducted on the 'dark web' there is no evidence that the information has been further disseminated or misused, the Commissioner is concerned with this kind of contravention, and even if potential consequences did not actually materialise, she maintains that this kind of contravention is likely to have the consequences identified.
45. The Commissioner considers that the damage and/or distress described above was likely to arise as a consequence of the kind of contravention. In other words, the Commissioner's view is that there was a significant and weighty chance that a contravention of the kind described would have such consequences.
46. The Commissioner also considers that such damage and/or distress was likely to be substantial, having regard to the nature of the personal data involved. In the circumstances, the likely damage or distress was certainly more than trivial.
47. The Commissioner is therefore satisfied that condition (b) from section 55A (1) DPA is met.

**Deliberate or negligent contraventions**

48. The Commissioner has considered whether the contraventions identified above were deliberate. In the Commissioner's view, this means that HAL's actions which constituted those contraventions were deliberate actions (even if HAL did not actually intend thereby to contravene the DPA).
49. The Commissioner considers that in this case HAL did not deliberately contravene the DPA in that sense.
50. The Commissioner has gone on to consider whether the contraventions identified above were negligent. First, she has considered whether HAL ought reasonably to have known that there was a risk that these contraventions would occur. She is satisfied that this condition is met, given that HAL was routinely used to handling large volumes of confidential and highly sensitive personal data, including records of its 6,500 staff and passenger information. Therefore, HAL should have been aware that such information must be kept secure and handled appropriately.
51. Whilst HAL submitted that it was unaware of the existence of the training video held on the memory stick, and that this was an isolated incident on the part of a relatively junior 'rogue' member of staff, HAL was aware of the widespread use of removable media across the organisation. Accordingly HAL should have known that such devices would be vulnerable to security breaches in the absence of appropriate security measures and in particular technical measures to prevent staff from removing personal data from its systems unless authorised.
52. HAL's awareness that USB memory sticks were being used is confirmed by the provision of existing guidance about the risks associated with

sensitive information and the use of removable media. Therefore HAL ought to have known of the risks of a contravention of this type occurring and implemented organisational measures to ensure compliance with policies together with technical controls over the downloading of information from its systems.

53. In respect of training, at the time of the incident HAL knew that training was required to be provided to staff given that its Information Security Policy stated that "all staff, and suppliers working on HAL site, shall have regular and appropriate information security awareness, training and guidance". Whilst HAL submitted that those trained were staff identified as having greatest exposure to personal data, it should also have known that training completion rates of approximately 2% (equating to approximately 130 staff out of 6,500) should be significantly higher to ensure staff were aware of data protection requirements. ICO guidance in existence at the time highlights the importance of training to staff. It is therefore considered that HAL should have known that without appropriate training measures staff would not have been aware of data protection requirements and obligations in respect of handling personal data.
54. The ICO has had longstanding guidance available prior to the incident in the form of "A practical guide to IT security" and "Bring Your Own Device (BYOD)" which included technical security considerations around the use of removable media. It is considered that HAL had ample opportunity to be aware of such guidance and to take steps to act upon the advice they contained.
55. Prior to the incident the ICO had also published details of regulatory action against other data controllers in respect of similar incidents involving the loss of unencrypted USB memory sticks (2012 - Greater Manchester Police & 2013 - North East Lincolnshire Council). HAL had

opportunity to be aware of these cases and the risks identified by the use of such devices.

56. Second, the Commissioner has considered whether HAL knew or ought reasonably to have known that those contraventions would be of a kind likely to cause substantial damage or substantial distress. She is satisfied that this condition is met, given that HAL, as an employer of approximately 6,500 staff and the handler of a significant volume of passengers was aware of the nature of the personal data it handled. Therefore, it should have been obvious to HAL that such a contravention would be of a kind likely to cause substantial damage or substantial distress to the affected individuals. HAL has acknowledged post incident that some of the data on the USB stick could have facilitated identity fraud.
57. Third, the Commissioner has considered whether HAL failed to take reasonable steps to prevent the contravention. Again, she is satisfied that this condition is met. Reasonable steps in these circumstances would have included:
- Encryption of personal data on removable media devices;
  - Organisational measures to control the number of removable media devices issued;
  - Implementation of technical controls to ensure that personal data could not be downloaded onto removable media without authority;
  - Monitoring compliance with formal policies, guidance and procedures regarding information security and the use of removable media; and
  - Provision of adequate data protection training and monitoring to staff.



58. HAL failed to take any of those steps.
59. The Commissioner is therefore satisfied that condition (c) from section 55A (1) DPA is met.

**The amount of the penalty the Commissioner proposes to impose**

60. The Commissioner has taken into account the following **aggravating features** of this case:
- The contravention does not appear to be contained to one service area, suggesting long term and sustained risk to personal data across the organisation;
  - Data protection should have been high on HAL's agenda, given the industry and personal data involved;
  - Only 2% of staff (notwithstanding that these were those identified by HAL as having greatest exposure to personal data) had received training on data protection and information security - the lowest the Commissioner has seen in her experience; and
  - Whilst measures in respect of containment of the incident were actioned promptly, remedial measures in respect of systemic failings across HAL are not as compliant as the ICO would have expected.
61. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the DPA and this is an opportunity to reinforce the need for data controllers to ensure that appropriate and effective security measures are applied to personal data.

## **Conclusion**

62. Taking into account all of the above, the Commissioner has decided that the penalty is **£120,000 (one hundred and twenty thousand pounds)**.
63. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **6 November 2018** at the latest. The monetary penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.
64. If the Commissioner receives full payment of the monetary penalty by **5 November 2018** the Commissioner will reduce the monetary penalty by 20% to **£96,000 (ninety six thousand pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.
65. There is a right of appeal to the First-tier Tribunal (Information Rights) against:
- a) the imposition of the monetary penalty; and/or
  - b) the amount of the penalty specified in the monetary penalty notice.
66. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.
67. Information about appeals is set out in Annex 1.

68. The Commissioner will not take action to enforce a monetary penalty unless:
- the period specified within the notice within which a monetary penalty must be paid has expired and all or any of the monetary penalty has not been paid;
  - all relevant appeals against the monetary penalty notice and any variation of it have either been decided or withdrawn; and
  - the period for appealing against the monetary penalty and any variation of it has expired.
69. In England, Wales and Northern Ireland, the monetary penalty is recoverable by Order of the County Court or the High Court. In Scotland, the monetary penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

Dated the 3rd day of October 2018

Signed

Stephen Eckersley  
Director of Investigations  
Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

## **ANNEX 1**

### **SECTION 55 A-E OF THE DATA PROTECTION ACT 1998**

#### **RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER**

1. Section 48 of the Data Protection Act 1998 gives any person upon whom a monetary penalty notice or variation notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:-

- a) that the notice against which the appeal is brought is not in accordance with the law; or
- b) to the extent that the notice involved an exercise of discretion by the Commissioner, that she ought to have exercised her discretion differently,

the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

GRC & GRP Tribunals  
PO Box 9300  
Arnhem House  
31 Waterloo Way  
Leicester  
LE1 8DJ

- a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.
  - b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.
4. The notice of appeal should state:-

- a) your name and address/name and address of your representative (if any);
  - b) an address where documents may be sent or delivered to you;
  - c) the name and address of the Information Commissioner;
  - d) details of the decision to which the proceedings relate;
  - e) the result that you are seeking;
  - f) the grounds on which you rely;
  - g) you must provide with the notice of appeal a copy of the monetary penalty notice or variation notice;
  - h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.
5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.
6. The statutory provisions concerning appeals to the First-tier Tribunal (Information Rights) are contained in sections 48 and 49 of, and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).