

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: London Borough of Islington

Of: Town Hall, Upper Street, London N1 2UD

1. The Information Commissioner ("the Commissioner") has decided to issue the London Borough of Islington ("Islington") 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 Islington.
2. This notice explains the Commissioner's decision.

Legal framework

3. Islington 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.
4. 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”.

5. 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”.

6. 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.

7. 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.
8. The DPA implements European legislation (Directive 95/46/EC) aimed at the protection of the individual's fundamental right to the protection of personal data. The Commissioner approaches the data protection principles so as to give effect to the Directive.

Background to the case

9. Islington's parking inspectors issue tickets for parking contraventions on the public highway or for traffic offences.
10. In 2012, Islington's internal application team developed 'TicketViewer' on behalf of Islington Parking Services ("the application"). It was hosted separately to Islington's other systems.

11. A user ("user") could log onto the application by entering the vehicle registration number ("VRN") and a parking ticket number to see a CCTV image or video of their alleged contravention or offence.
12. If a user still wanted to appeal a parking ticket, they could send supporting evidence to Islington Parking Services by email or post.
13. This included their name and address together with details of any mitigating circumstances such as health issues, disabilities and financial details.
14. Islington also received sensitive information about users from the 'Traffic Enforcement Centre' in relation to its recovery of unpaid fines in the County Court.
15. The back office processing centre scanned all of this information (including the parking ticket and the CCTV image or video that showed the VRN) onto the user's ticket attachment folder.
16. Between 2012 and 25 October 2015, Islington issued in the region of 825,000 parking tickets and received 270,000 appeals from its users.
17. On 25 October 2015, Islington was informed by a user that the ticket attachment folders could be accessed by manipulating the URL in the user's browser.
18. At that time, the ticket attachment folders contained personal data relating to approximately 89,000 users, including sensitive personal data and financial details.

19. On 16 and 25 October 2015, external testing discovered that a total of 119 documents had been accessed a total of 235 times from 36 unique IP addresses affecting 71 users.
20. The Commissioner has made the above findings of fact on the balance of probabilities.
21. The Commissioner has considered whether those facts constitute a contravention of the DPA by Islington and, if so, whether the conditions of section 55A DPA are satisfied.

The contravention

22. The Commissioner finds that Islington contravened the following provisions of the DPA:
23. Islington failed to take appropriate technical measures against the unauthorised and unlawful processing of personal data in contravention of the seventh data protection principle at Part I of Schedule 1 to the DPA.
24. The Commissioner finds that the contravention was as follows. Islington did not have in place appropriate technical measures for ensuring so far as possible that such an incident would not occur, i.e. for ensuring that the personal data held in the ticket attachment folders were safeguarded against unauthorised or unlawful access.
25. In particular:
 - (a) The 'Folder Browsing' functionality within the web server was misconfigured; and

(b) The application had design faults.

26. The Commissioner is satisfied that Islington was responsible for this contravention.
27. The Commissioner has gone on to consider whether the conditions under section 55A DPA were met.

Seriousness of the contravention

28. The Commissioner is satisfied that the contravention identified above was serious due to the number of data subjects, the nature of the personal data that was held in some of the ticket attachment folders and the potential consequences. In those circumstances, Islington's failure to take adequate steps to safeguard against unauthorised or unlawful access was serious.
29. The Commissioner is therefore satisfied that condition (a) from section 55A (1) DPA is met.

Contravention of a kind likely to cause substantial damage and substantial distress

30. The relevant features of the kind of contravention are:
31. On 25 October 2015, the ticket attachment folders held personal data relating to approximately 89,000 users, including sensitive personal data and financial details. The application therefore required adequate security measures to protect the personal data.

32. This is all the more so when sensitive personal data and financial details are concerned – in particular, as regards the users who expected that it would be held securely. This heightens the need for robust technical measures to safeguard against unauthorised or unlawful access. For no good reason, Islington appears to have overlooked the need to ensure that it had robust measures in place despite having the financial and staffing resources available.
33. The Commissioner therefore considers that the contravention was of a kind likely to cause distress to the users if they knew that their personal data had been accessed by unauthorised individuals.
34. The Commissioner also considers that such distress was likely to be substantial, having regard to the number of users and the nature of the data that was held in the ticket attachment folders.
35. Further, the users would be distressed by justifiable concerns that their information has been further disseminated even if those concerns do not actually materialise.
36. If this information has been misused by those who had access to it, or if it was in fact disclosed to hostile third parties, then the contravention would cause further distress to the users and damage, such as exposing them to possible fraud.
37. The Commissioner is therefore satisfied that condition (b) from section 55A (1) DPA is met.

Deliberate or foreseeable contravention

38. The Commissioner has considered whether the contravention identified above was deliberate. In the Commissioner's view, this means that Islington's actions which constituted those contraventions were deliberate actions (even if Islington did not actually intend thereby to contravene the DPA).
39. The Commissioner considers that in this case Islington did not deliberately contravene the DPA in that sense. She considers that the inadequacies outlined above were matters of serious oversight rather than deliberate intent to ignore or bypass the provisions of the DPA.
40. The Commissioner has gone on to consider whether Islington knew or ought reasonably to have known that there was a risk that this contravention would occur. She is satisfied that this condition is met, given that Islington should have been aware of the application and the data that was held in the ticket attachment folders.
41. In the circumstances, Islington ought reasonably to have known that there was a risk that that unauthorised or unlawful access would occur unless it ensured that the personal data held in the ticket attachment folders was appropriately protected.
42. Second, the Commissioner has considered whether Islington knew or ought reasonably to have known that there was a risk the contravention would be of a kind likely to cause substantial damage or substantial distress.
43. She is satisfied that this condition is met, given that Islington should have been aware of the data that was held in the ticket attachment

folders. Islington ought to have known that it would cause substantial distress to the users if the information was accessed by unauthorised third parties.

44. Islington should also have known that if the data has in fact been accessed by hostile third parties then it would cause further damage and distress to the users.
45. Therefore, it should have been obvious to Islington that such a contravention would be of a kind likely to cause substantial damage and distress to the users.
46. Third, the Commissioner has considered whether Islington 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 oversight and testing of the application by Islington's IT security team prior to going live, and regular testing subsequently. Islington did not take those steps. The Commissioner considers there to be no good reason for that failure.
47. The Commissioner is therefore satisfied that condition (c) from section 55A (1) DPA is met.
48. For the above reasons, the Commissioner considers there to have been a serious contravention of the seventh data protection principle on the part of Islington with respect to the personal data that was held in the ticket attachment folders. The contravention was of a kind likely to cause substantial damage and distress. Islington knew or ought to have envisaged those risks and it did not take reasonable steps to prevent the contravention. The conditions for issuing a monetary penalty are met in this case.

The Commissioner's decision to impose a monetary penalty

49. The Commissioner has concluded that the conditions for issuing a monetary penalty are in place. She has considered whether it is appropriate for her to exercise her discretion in favour of issuing a monetary penalty in this case. Her conclusion is that it is appropriate to do so in all the circumstances. The contravention is serious in terms of both Islington's deficiencies and the impact such deficiencies were likely to have on the affected individuals in this case.
50. The issuing of a monetary penalty in this case would be fair and just. It would accord with the Commissioner's statutory guidance and regulatory objectives. It would act as an encouragement to ensure that such deficiencies are not repeated elsewhere.
51. The Commissioner has taken into account the following **mitigating features** of this case:
- Islington referred this incident to the Commissioner, immediately took the application offline and was co-operative during the Commissioner's investigation.
 - The affected individuals were notified by Islington.
 - The Commissioner is not aware of the affected individuals actually suffering any damage or distress in this case.
 - A monetary penalty may have a significant impact on Islington's reputation, and to an extent, its resources.
 - This incident has been publicised on social media and in the local press.
52. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the DPA and this is an

opportunity to remind data controllers to ensure that appropriate and effective security measures are applied to personal data.

Conclusion and amount of penalty

53. The Commissioner confirms that she has taken account of Islington's submissions in response to her Notice of Intent.
54. Notwithstanding those submissions, the Commissioner has decided that she can and should issue a monetary penalty in this case, for the reasons explained above.
55. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of **£70,000 (Seventy thousand pounds)** is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.
56. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **7 September 2017** 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.
57. If the Commissioner receives full payment of the monetary penalty by **6 September 2017** the Commissioner will reduce the monetary penalty by 20% to **£57,000 (Fifty seven thousand pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.
58. 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.

59. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.

60. Information about appeals is set out in Annex 1.


61. 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.

62. 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 7th day of August 2017

Signed


Stephen Eckersley
Head of Enforcement
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)).