

**DATA PROTECTION ACT 1998**

**SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER**

**MONETARY PENALTY NOTICE**

To: Nottinghamshire County Council

Of: County Hall, West Bridgford, Nottingham NG2 7QP

1. The Information Commissioner ("the Commissioner") has decided to issue Nottinghamshire County Council ("the Council") 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 the Council.
2. This notice explains the Commissioner's decision.

**Legal framework**

3. The Council 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. In July 2011, the Council's digital team launched its 'Home Care Allocation System' ('HCAS'). Third party home care providers could access HCAS to confirm that they had capacity to support a particular service user.
- 10. The home care providers were each sent a link to HCAS via email. There were no access controls on HCAS, such as the use of a username

or password.

11. On 14 June 2016, a member of the public informed the Council that HCAS could also be accessed via an internet search engine. They were concerned that - *"Should someone who would wish to prey on a vulnerable person, e.g. A thief, obtain these details it would not be very difficult for them to attend one of the streets listed, find where the carers attend and subsequently consider attempting a burglary or similar knowing the service user is very likely to be vulnerable or elderly. Your website even states whether the service user has been in hospital. I think it would be very easy for someone to pose as a district Nurse etc. and con someone to let them in with this information."*
12. At that time, HCAS contained a directory of 81 service users including their gender, addresses (to the extent required by each home care provider) and post codes, personal care needs and care package requirements such as the number of home visits per day and whether the service user was currently in hospital.
13. Although the service user's names were not included, a determined person would be able to identify a service user.
14. The Commissioner has made the above findings of fact on the balance of probabilities.
15. The Commissioner has considered whether those facts constitute a contravention of the DPA by the Council and, if so, whether the conditions of section 55A DPA are satisfied.

### **The contravention**

16. The Commissioner finds that the Council contravened the following provisions of the DPA:
17. The Council 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.
18. The Commissioner finds that the contravention was as follows. The Council 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 on HCAS were safeguarded against unauthorised or unlawful access.
19. In particular, HCAS did not have in place an authentication process that identified a user before allowing them to access the system, such as a username or password.
20. This was an ongoing contravention from July 2011 until the Council took remedial action on 14 June 2016.
21. The Commissioner is satisfied that the Council was responsible for this contravention.
22. The Commissioner has gone on to consider whether the conditions under section 55A DPA were met.

**Seriousness of the contravention**

23. 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 on HCAS and the potential consequences. In those circumstances, the Council's failure to take adequate steps to safeguard against unauthorised or unlawful access was serious.

24. 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**

25. The relevant features of the kind of contravention are:
26. On 14 June 2016, HCAS held personal data relating to 81 service users. During the period of contravention, the personal data of up to 3,000 service users would have been held on HCAS. It was possible to infer from the personal data that the service users were elderly and vulnerable. HCAS therefore required adequate security measures to protect the personal data.
27. This is all the more so as regards the elderly and vulnerable service users who expected that the information would be held securely. This heightens the need for robust technical measures to safeguard against unauthorised or unlawful access. For no good reason, the Council appears to have overlooked the need to ensure that it had robust measures in place despite having the financial and staffing resources available.
28. The Commissioner therefore considers that the contravention was of a kind likely to cause distress to the service users if they knew that their personal data had been accessed by unauthorised individuals over a

five year period.

29. The Commissioner also considers that such distress was likely to be substantial, having regard to the number of service users and the nature of the data that was held on HCAS. For example, an elderly and vulnerable service user may worry that a thief or burglar would use the information to prey on her whilst at home or in hospital.
30. Further, the service users would be distressed by justifiable concerns that their information has been further disseminated even if those concerns do not actually materialise.
31. 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 service users, and damage such as theft or burglary.
32. The Commissioner is therefore satisfied that condition (b) from section 55A (1) DPA is met.

### **Deliberate or foreseeable contravention**

33. The Commissioner has considered whether the contravention identified above was deliberate. In the Commissioner's view, this means that the Council's actions which constituted those contraventions were deliberate actions (even if the Council did not actually intend thereby to contravene the DPA).
34. The Commissioner considers that in this case the Council 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.

35. The Commissioner has gone on to consider whether the Council 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 the Council routinely handles information relating to elderly and vulnerable adults. The Council ought to have been aware of the personal data that was held on HCAS.
36. In the circumstances, the Council 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 on HCAS was appropriately protected.
37. Second, the Commissioner has considered whether the Council knew or ought reasonably to have known that there was a risk the contravention would be of a kind likely to cause substantial damage and distress.
38. She is satisfied that this condition is met, given that the Council ought to have been aware of the personal data that was held on HCAS. The Council ought to have known that it would cause substantial distress to the service users if the information was accessed by unauthorised third parties.
39. The Council should also have known that if the data has in fact been accessed by hostile third parties then it could cause further distress to the service users, and damage.
40. Therefore, it should have been obvious to the Council that such a contravention would be of a kind likely to cause substantial damage



and distress to the service users.

41. Third, the Commissioner has considered whether the Council 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 building HCAS with appropriate access controls at the outset and carrying out security testing on the system. The Council did not take those steps. The Commissioner considers there to be no good reason for that failure.
42. The Commissioner is therefore satisfied that condition (c) from section 55A (1) DPA is met.
43. For the above reasons, the Commissioner considers there to have been a serious contravention of the seventh data protection principle on the part of the Council with respect to the personal data that was held on HCAS. The contravention was of a kind likely to cause substantial damage and distress. The Council 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**

44. 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 the Council's deficiencies and the impact such deficiencies were

likely to have on the affected individuals in this case.

45. 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.
46. The Commissioner has taken into account the following **mitigating features** of this case:
- HCAS was taken offline on 14 June 2016.
  - The Council reported this incident to the Commissioner and was co-operative during her investigation.
  - A monetary penalty may have a significant impact on the Council's reputation, and to an extent, its resources.
47. 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**

48. The Commissioner has not received any submissions from the Council in response to her Notice of Intent.
49. The Commissioner has now decided that she can and should issue a monetary penalty in this case, for the reasons explained above.
50. 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.


51. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **27 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.
52. If the Commissioner receives full payment of the monetary penalty by **26 September 2017** the Commissioner will reduce the monetary penalty by 20% to **£56,000 (Fifty 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.
53. 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.
54. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.
55. Information about appeals is set out in Annex 1.
56. 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.

57. 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 24<sup>th</sup> 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)).