Data Protection Act 1998

Monetary Penalty Notice

Dated:

27 August 2013

Name: ABERDEEN CITY COUNCIL

Address: 2nd Floor, Old Town House, Broad Street, Aberdeen, AB10 1FY

Introduction

---

1. This Monetary Penalty Notice is issued by the Information Commissioner ('the Commissioner') pursuant to section 55A of the Data Protection Act 1998 ('The Act'). A monetary penalty notice is a notice requiring the data controller to pay to the Commissioner a monetary penalty of an amount determined by the Commissioner and specified in the notice.

2. Aberdeen City Council is the data controller, as defined in section 1(1) of the Act, in respect of the processing of personal data carried on by Aberdeen City Council (referred to in this notice as 'the data controller').

3. Following a serious contravention of the data controller's duty, under section 4(4) of the Act, to comply with the seventh data protection

principle, the Commissioner considers, for the reasons set out below, to serve on the data controller notice of a monetary penalty in the sum of £100,000.

Statutory framework

---

4. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, 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 it is the data controller.

5. Under sections 55A and 55B of the Act (introduced by the Criminal Justice and Immigration Act 2008 which came into force on 6 April 2010) the Commissioner may, in certain circumstances, where there has there been a serious contravention of section 4(4) of the Act, serve a monetary penalty notice ('MPN') on a data controller requiring the data controller to pay a monetary penalty of an amount determined by the Commissioner and specified in the notice but not exceeding £500,000.

6. The Commissioner has issued Statutory Guidance under section 55C (1) of the Act about the issuing of monetary penalties which is published on the Commissioner's website. It should be read in conjunction with the Data Protection (Monetary Penalties and Notices)

Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010.

7. This case involves the disclosure of sensitive personal data. Sensitive personal data is defined in section 2 of the Act (in so far as it is applicable to this case) as follows:-

"In this Act "sensitive personal data" means personal data consisting of information as to- [the data subject's]

(e) ...physical or mental health or condition,

(g) the commission or alleged commission by him of any offence..."

Power of Commissioner to impose a monetary penalty

---

8. Section 55A of the Act provides that:

(1) 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 Act] *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.

Background

9. Between 8 and 14 November 2011, a [redacted] employed by the data controller working from home on her home computer inadvertently uploaded four documents which related to her work and contained sensitive personal data on to a website on the internet.

10. The employee who uploaded the data had been home working in her current capacity ([redacted]) since September 2010. However, the member of staff had also worked from home prior to this date as a [redacted].

11. At the time of the incident, there was no relevant home working policy in place for staff to adhere to though this employee and all other staff was allowed to access work material from home.

12. Whilst there was a Tele-working policy which addressed the health and safety aspects of home working, the existence of the policy demonstrated the Council's awareness that home working was necessary though the Council did not consider the impact homeworking might have on data security.

13. The data controller has confirmed that the information which the employee was processing at the time of this incident, including the personal data, was relevant to her role as a [redacted]. Part of this role is to chair [redacted] Reviews. The reviews do not take place at fixed locations which is why the employee is authorised to access the relevant data remotely.

14. Following an investigation into the incident, the data controller believes that the employee had accessed the sensitive documents through either her Council 'Groupwise' email account (which can be accessed through any network) or via a USB stick. The data controller believes that when the employee accessed the files they were auto-saved to her computer's 'My Documents'. The data controller has explained that this happened because the computer had a file transfer program installed

on it and that the employee, without knowledge or intention, activated the program which uploaded the entirety of her My Documents file, including the data which originated from the work email or USB stick, on to the internet. The employee told the data controller that the computer is second hand and that it must have had the auto-upload program installed on it by a previous owner. The program placed the files onto a website. Once the files had been uploaded they became accessible to all internet users by inputting specific search terms into a search engine such as names of attendees at the meeting.

15. On 15 February 2012, a [redacted] informed his manager that he had entered his name and job title into a search engine and on scrolling down the search results noticed that an Aberdeen City Council core group meeting was listed. The employee stated that he had clicked on the link and opened the file and realised it was a group minute dated 16.2.11 relating to a child.

16. The [redacted] who found the information on the internet was mentioned in the minute of the core group meeting in his capacity as the [redacted]. The [redacted] also stated that there were other documents on the same website which appeared to have originated from the data controller's social work service.

17. The [redacted] also pointed out to another member of the multi-agency team, a [redacted] (NHS Grampian [redacted]) that his name was also mentioned in the core group minutes that he had found on the internet. The [redacted] attended the core group meeting.

18. Four hours after becoming aware of this incident, the data controller had removed the source documents from the website. They have also confirmed that no cached versions of the documents are still available.

19. After the incident was reported internally, the data controller reported the breach to the ICO by phone on 17 February 2012.

20. A national newspaper became aware of this incident and published a story on 18 February 2012. The article does not identify any of the data subjects and the data had been removed from any online sources before the story was published. It appears that a source close to the case informed the newspaper of the incident and they subsequently located the data online.

21. The data controller, upon being contacted by the newspaper about this incident, sought assurances that the personal data contained in the documents would not be published.

22. The four documents uploaded on to the website were:-

i) Minute of a core group meeting held in relation to a child.

ii) A LAAC Review minute

iii) A child's plan

iv) A transfer summary

23. All of the above mentioned documents contain highly personal, sensitive and confidential information about the children, their family and their involvement with Social Work Services and other partner organisations such as the NHS.

24. The personal data totals 39 pages and contains names and addresses of service users, details of family members, sensitive personal data relating to alleged criminal offences such as [redacted]. Other sensitive personal data includes [redacted].

25. Some of the data is in relation to a [redacted]. There is a section of text which contains a detailed account of key events in a data subject's life.

26. Due to redactions, applied by the data controller for the purpose of the Commissioner's investigation, it is difficult to ascertain exactly how many data subjects' addresses have been disclosed by the report, but it is clear however that names, addresses and dates of birth are included in some of the reports which were disclosed.

27. The data protection policy in place at the time of this incident was impractical and ambiguous. It demonstrates the data controller's awareness of the importance of data security but the actions of the Council did not reflect this recognition. The data controller relied on staff adherence with the data protection policy without providing the technical infrastructure to make this achievable.

28. The data controller's Social Care and Wellbeing department had issued 76 encrypted USB sticks between 5 May 2010 and 31 January 2012. A recall program on non-encrypted USB sticks was initiated following this incident. No sticks were returned as a result of this program. This either indicates that few staff used non-encrypted USB sticks or that staff have not returned them and continue to use them to date.

29. Prior to this incident, there were no controls in place to stop staff from using non-council issued USB sticks. In light of the apparent flexibility of the working arrangements and the lack of technical limitations, the

data controller cannot conclude that because no USB sticks were returned, nobody was using them.

Grounds on which the Commissioner proposes to serve a monetary penalty notice

---

30. In deciding to issue this Monetary Penalty Notice, the Commissioner has considered the facts of the case and the deliberations of those within his office who have recommended this course of action. In particular, he has considered whether the criteria for the imposition of a monetary penalty have been met; whether, given the particular circumstances of this case and the underlying objective in imposing a monetary penalty, the imposition of such a penalty is justified and whether the amount of the proposed penalty is proportionate.

Serious contravention of section 4(4) of the DPA

31. The Commissioner is satisfied that there has been a serious contravention of section 4(4) of the Act in that there has been a breach of the data controller's duty to comply with the Seventh Data Protection Principle.

32. The Seventh Data Protection Principle provides, at Part I of Schedule 1 to the Act, 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".*

33. Paragraph 9 at Part II of Schedule 1 to the Act further 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"*

34. In particular, in this case, the data controller has failed to take sufficient appropriate technical and organisational measures against unauthorised processing of personal data so as to effectively prevent

such unauthorised processing occurring. Such measures may include taking timely steps to introduce the use of a secure home working policy, providing its employees with the necessary equipment to make home a secure place to work, providing its employees with appropriate and adequate training, the outcomes of which are suitably monitored, sufficient management training and management checks on the efficacy of the home working policy, once introduced, and taking subsequent steps to ensure that the policy was sufficiently adhered to.

35. The Commissioner considers that the contravention in this case is serious for the following reasons:-

i) Sensitive personal data has been placed online and made available on a global scale.

ii) There were not sufficient technical or organisational measures in place to prevent it occurring contravening the seventh data protection principle.

The contravention is of a kind likely to cause substantial distress

36. The Commissioner is further satisfied that the contravention in this particular case is of a kind likely to cause substantial damage and substantial distress for the following reasons:-

i) Confidential personal data was disclosed to unauthorised third parties (via the internet) due to the inappropriate technical and organisational measures taken by the data controller.

ii) The data in this case is particularly sensitive as the data, spread over four documents, identifies vulnerable members of the public. It constitutes an appraisal of the lives of several families and individuals based on current and past events.

iii) The data subjects would suffer from substantial distress knowing that their confidential personal data has been disclosed to third parties (via the internet) and that there is the possibility that their data may have been further disseminated and possibly misused. That is so, even if those concerns do not actually materialise in practice.

iv) The affected individuals had entrusted their detailed information to the data controller, on the basis that it would be dealt with in confidence.

The data controller ought to have known that there was a risk that the contravention would occur, that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to reasonable steps to prevent the contravention

37. The Commissioner is satisfied that section 55A (3) of the Act applies in that the data controller ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial distress, but it failed to take reasonable steps to prevent the contravention for the following reasons:-

i) The data controller had an acceptable use policy called 'home working' which identifies the requirement to ensure sensitive information has the required safeguards applied to it. The data controller therefore knew there were inherent risks attached to working with sensitive personal data when off site.

ii) Despite this policy, the data controller did not supply the necessary technical measures required to safeguard personal data from the employee's home.

iii) As the data controller's staff work with sensitive personal data of this nature on a daily basis, the data controller should know of

the associated risks and that it is likely to cause substantial damage or distress if mishandled.

iv) The employee was authorised by management to work from home. Despite this, the necessary equipment to make home a secure place to work from was not provided. There were no steps taken which could have prevented this incident.

38. In the circumstances, the data controller knew, or ought to have known that there was a risk that these contraventions would occur, and would continue to occur, unless reasonable steps were taken to prevent the contravention such as those suggested in paragraph 31 above.

39. Further it should have been obvious to the data controller that such a contravention would be of a kind likely to cause substantial distress to the data subjects due to the nature of the data involved.

Aggravating features the Commissioner has taken into account in determining the amount of a monetary penalty

Effect of the contravention

40. The data which was made publicly available on the internet related to vulnerable people held in confidence. The Council's failure to maintain a

confidential service exposed these individuals to unnecessary risk, both perceived and tangible.

Behavioural issues

41. The home working policy implemented since this incident occurred still enables all staff to access their emails from any internet connection. Policy dictates that staff cannot download documents from email but this relies on staff adhering to that policy. Unrestricted access to staff email is a potential cause of this incident and despite this, the Council's remedial measures fall short of eliminating the risk of a similar incident occurring in the future.

Mitigating features the Commissioner has taken into account in determining the amount of the monetary penalty

---

Nature of the contravention

42. The Commissioner acknowledges that it is unfortunate for the data controller that the employee in this case had a computer with a program installed on it that automatically uploaded documents onto the internet.

Behavioural issues

43. Action was taken to remove the data and limit press exposure as soon as the incident was realised.

44. Policy has been strengthened and all Council issued computers are now encrypted (although staff can still access Council material from non-Council owned equipment).

45. Data protection training has been improved and is now a mandatory requirement.

46. The data controller submitted to an audit which was offered as part of a general campaign in November 2011 when they were unaware that this breach had occurred only 2 weeks previously. The audit has only just taken place and the final report is currently being drafted with a possible completion and publication date of the end of June 2013.

Impact on the data controller

47. The incident has received press coverage already, causing damage to the data controller's reputation. Further action by the Commissioner

will revive the issue, causing further reputational damage to the data controller.

Other considerations

48. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the Act. This is an opportunity to reinforce the need for data controllers to review the sending of confidential and sensitive personal data by email and to ensure either that alternative more secure means are used or that, at a minimum, appropriate and effective security measures are applied to the use of email.

Notice of Intent

49. A notice of intent was served on the data controller dated 27 June 2013. The Commissioner received written representations from the data controller's Chief Executive dated 29 July 2013. The Commissioner has considered the written representations made in relation to the notice of intent when deciding whether to serve a monetary penalty notice. In particular, the Commissioner has taken the following steps:

- reconsidered the amount of the monetary penalty generally, and whether it is a reasonable and proportionate means of achieving the objective which the Commissioner seeks to achieve by this imposition;

- ensured that the monetary penalty is within the prescribed limit of £500,000; and

- ensured that the Commissioner is not, by imposing a monetary penalty, acting inconsistently with any of his statutory or public law duties and that a monetary penalty notice will not impose undue financial hardship on an otherwise responsible data controller.

Amount of the monetary penalty the Commissioner proposes to impose

---

50. The Commissioner considers that the contravention of section 4(4) of the Act is serious and that the imposition of a monetary penalty is appropriate. Further, he considers that a monetary penalty in the sum

of £100,000 (one hundred thousand pounds) is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

51. In reaching this decision, the Commissioner considered other cases of a similar nature in which a monetary penalty has been imposed and the facts and aggravating and mitigating features referred to above. Of particular relevance in this case is the nature of the personal data disclosed, the potential for harm and likelihood of distress.

Payment

52. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 24 September 2013 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.

Early payment discount

53. If the Commissioner receives full payment of the monetary penalty by 24 September 2013 the Commissioner will reduce the monetary penalty by 20% to £80,000 (eighty thousand pounds).

Right of Appeal

54. There is a right of appeal to the (First-tier Tribunal) General Regulatory Chamber against:

    a. the imposition of the monetary penalty

    b. and/or;

    c. the amount of the penalty specified in the monetary penalty notice.

55. Any Notice of Appeal should be served on the Tribunal by 5pm on 24 September 2013 at the latest. If the notice of appeal is served late the Tribunal will not accept it unless the Tribunal has extended the time for complying with this rule. Information about appeals is set out in the attached Annex 1.

56. The Commissioner will not take action to enforce a monetary penalty unless:

- the period specified in 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 the data controller to appeal against the monetary penalty and any variation of it has expired.

57. 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 or any sheriffdom in Scotland.

Dated the 2013

Signed: .....

David Smith

Deputy Information Commissioner

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) General Regulatory Chamber (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 he ought to have exercised his 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

4. The notice of appeal should be served on the Tribunal by 5pm on September 2013 at the latest.

5. 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.

6. 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;

   d) you must provide with the notice of appeal a copy of the monetary penalty notice or variation notice;

   e) 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.

7. 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.

8. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) 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)).