Data Protection Act 1998

Monetary Penalty Notice

Dated: 15 October 2013

Name: NORTH EAST LINCOLNSHIRE COUNCIL
Address: Town Hall Square, Grimsby, North East Lincolnshire, DN31 1HU

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. North East Lincolnshire 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 North East Lincolnshire 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 £80,000 (eighty thousand pounds).

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 personal data and sensitive personal data. Personal data is defined in section 1 of the Act.

8. 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,"

Power of Commissioner to impose a monetary penalty

---

9. 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

---

10. On 1 July 2011 an unencrypted USB memory stick containing personal and sensitive personal data was lost on the data controller's premises. A special educational needs teacher had been working with the information held on the USB stick while using a laptop that was connected to the data controller's networked computer system. When logging off the system and leaving the office for the day, the teacher forgot to remove the USB stick. When the teacher realised the mistake and tried to retrieve the USB stick, it was gone. To date, the USB stick has not been recovered. The data controller completed an internal investigation in response to the incident.

11. The teacher worked in the data controller's Special Educational Needs Support Service in the Children's Services Directorate ('the directorate'). The teacher would spend the majority of time away from council offices visiting schools and other community locations. The teacher was not primarily office based and did not have remote access to the data controller's computer system. Information was saved on the USB stick as it enabled access to necessary data during visits to

the different locations. The data controller issued the teacher with the USB stick in 2005.

12. The USB stick holds the personal and sensitive data of 286 pupils with special educational needs who attended schools in the data controller's area. The pupils were aged between 5 and 16 years. The data consists of reports that cover issues such as dyslexia, Irlen syndrome and other mental and physical disabilities, school performance, learning issues and specific teaching strategies for pupils with special educational needs. All of the reports contain the name of the pupil and the school they attended. The majority of the reports contain the DOB of the pupil and some contain pupils' home addresses. A small number of reports identify the parents of a pupil, and contain information about the 'home-life', which includes financial matters and family dynamics. The reports identify whether the pupil is deemed vulnerable and whether the data controller's children's services are involved. The reports are all protectively marked.

13. Following the incident, the data controller carried out a risk assessment for the potential damage and distress to the data subjects. The internal report estimated that the loss of the sensitive personal data is likely to lead to the ill-health of those affected through the disclosure of the data or due to a break in the services which they were receiving. The likely damage and distress to the data subjects is substantial due to the volume of data which has been lost, and that the data subjects are children aged 5 -16, some of whom are deemed vulnerable (and their families). The data subjects were not notified of the data breach.

14. The data controller introduced an information security policy in March 2011, four months prior to the incident occurring. This policy specifies that removable media (e.g. USB sticks) "must be encrypted". This

policy had been in draft form since 2009. Prior to the introduction of the policy in 2011, the data controller's previous policy referred to portable devices, such as laptops, but did not detail specific issues about removable media and USB memory sticks.

15. The data controller up-dated the 'pre-login disclaimer" in April 2011 which refers to the information security policy. By accepting the disclaimer, a staff member confirms agreement to the policies and procedures for information security. The disclaimer must be accepted to allow system log-in. The data controller obtained confirmation from the teacher in June 2011, that they had read and understood the new information security policy.

16. After the introduction of the information security policy, the data controller asked for volunteers to take part in a 'removable media pilot' to test new encryption software. This software automatically encrypts any removable media device placed in a computer on the data controller's system. At the same time, the data controller offered an 'encryption on request' service for removable media. Both of these were presented on a volunteer basis. Prior to these two initiatives, the data controller did not have anything in place to enable staff to comply with the information security policy relating to USB sticks. Following the data loss incident in July 2011, the data controller immediately recalled the unencrypted USB memory sticks in the directorate and erased the data.

17. The data controller provides e-learning training on the Act and information security. The information security training is part of another training module, which is undertaken by staff to obtain a

GCSx email address. The teacher had undertaken the training in order to obtain a GCSx email address prior to the incident, but it cannot be confirmed they had received the Data Protection Act training prior to the incident. The data controller has recognised that staff may not be aware of information security unless they have carried out GCSx training. This training has been reviewed following the incident and it is being launched as a separate module to be communicated to all staff. The training modules were not mandatory. The data controller reviewed this policy following the data loss and the training is now mandatory.

18. On 29 September 2011, the data controller voluntarily reported the loss of the USB memory stick to the Commissioner.

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

---

19. 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

20. 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.

21. 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".*

22. 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"*

23. In particular, in this case, the data controller has failed to take sufficient appropriate technical and organisational measures against accidental loss of personal data such as a combination of, training staff

on the importance of using encrypted USB sticks; technical controls to prevent downloading on to unencrypted portable media; effective organisational policies and controls; and enabling compliance with those policies and controls. The Commissioner considers that the contravention is serious because the measures did not ensure a level of security appropriate to the nature of the data to be protected and the harm that might result from accidental loss.

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

i) Personal data and sensitive personal data was placed on an unencrypted USB stick which has been lost.

ii) There were insufficient 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

25. 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) Personal data and sensitive personal data were lost due to the inappropriate technical and organisational measures taken by the data controller.

ii) The data in this case is sensitive. The data, contained in hundreds of files, identifies school children with special

educational needs. It constitutes reports about issues of physical and mental health, learning disabilities, home-life, whether the child is deemed vulnerable and teaching strategies for the pupils. The data was current at the time of the loss.

iii) The data subjects would suffer from substantial distress knowing that their sensitive personal data may be disclosed to third parties, even though, so far as the Commissioner is aware, those concerns have so far not materialised. The USB memory stick has not been recovered.

iv) If the data is in fact accessed by untrustworthy third parties then it is likely the contravention would cause further substantial distress and substantial damage to the data subjects such as exposing them to damage to their health, education and personal relationships.

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

26. 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) Staff employed by the data controller were used to handling sensitive personal information on a routine basis and the data controller was aware of the sensitive nature of this personal data.

ii) A large amount of personal data relating to pupils had been stored on unencrypted USB sticks since at least 2005. The nature of the teacher's job required routinely working outside of the secure office environment at different locations which did not have access to the data controller's network.

iii) The data controller was aware that staff members were routinely downloading information from the network and the data controller would have been aware of the sensitive nature of the personal information being stored on USB sticks.

iv) The data controller identified a requirement for an encryption policy in 2009, policy but this was not implemented until 2011. Despite having identified the risks of using unencrypted USB sticks, the data controller still allowed their use.

v) Following implementation of the Information Security Policy in 2011, the data controller continued to allow staff to use unencrypted USB sticks, in breach of its own policy.

vi) While there was an encryption service available, its use was voluntary. The data controller has accepted that the initial attempt to raise awareness of the encryption service was not adequate.

vii) The data controller therefore knew, or ought to have known, there were inherent risks attached to using unencrypted removable media devices.

viii) The data controller did not take reasonable steps to prevent the contravention such as a combination of training staff on the importance of using encrypted USB sticks; technical controls to prevent downloading on to unencrypted portable media; effective organisational policies and controls; and enabling compliance with those policies and controls.

27. In the circumstances, the data controller knew, or ought to have known that there was a risk that this contravention would occur, unless reasonable steps were taken to prevent the contravention.

28. 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

29. The contravention was serious because of the sensitive nature of the personal data involved in the data loss.

30. The data related to approximately 286 pupils aged 5 -16 with special educational needs; some of whom were considered to be vulnerable children.

31. The USB stick has not been recovered.

32. The data controller is unable to determine whether any unauthorised third parties may have had access to the data.

33. There is a risk of further substantial damage or substantial distress if the data is accessed by untrustworthy third parties.

Behavioural issues

34. The data controller had been using unencrypted USB sticks for at least six years prior to the incident.

35. Although the data controller had a long term plan to eliminate the risks associated with removable media it had failed to implement any effective short term plan to limit the risks.

36. The data controller considered recalling *all* the USB sticks but decided against doing so as it did not have a record of the number of sticks in use and could not guarantee the success of a recall.

37. The data controller continued to issue unencrypted USB sticks for use with non-personal data after the policy was implemented in 2011. Even though it was aware of the inherent risk in continuing to issue these types of memory sticks to staff.

38. The data controller failed to notify the parents/carers of the data loss, despite its internal investigation report recommending notification.

Impact on the data controller

39. The data controller has sufficient financial resources to pay a monetary penalty up to the maximum without it causing undue financial hardship.

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

---

Nature of the contravention

40. The data controller issued an information security policy in March 2011 requiring the use of encrypted USB sticks.

Effect of the contravention

41. As far as the Commissioner is aware, there is no evidence that the personal data involved in this incident has been inappropriately accessed.

Behavioural issues

42. The data controller has taken organisational and technical remedial action in respect of removable media, with a view to preventing a recurrence. Immediate action was taken following the incident to recall the USB memory sticks in the directorate and encrypt them.

43. Remedial measures were in progress at the time of the incident. The data controller had recognised the risk and was proactively working to avoid an incident.

44. The data controller voluntarily reported the data loss and has co-operated with the Commissioner's investigation.

Impact on the data controller

45. Significant impact on the reputation of the data controller.

Other considerations

---

46. 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 ensure that appropriate and effective security measures are applied to personal data and to review the use of removable media devices, such as USB memory sticks to ensure appropriate and effective encrypted devices are used.

47. The data controller has now taken organisational and technical steps to eliminate the possibility of a further incident of this nature occurring.

Notice of Intent

---

48. A notice of intent was served on the data controller dated 8 August 2013. The Commissioner received written representations from the data controller's Chief Executive dated 4 September 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

---

49. 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 £80,000 (eighty thousand pounds) is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

50. 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 lost, the potential for harm and likelihood of distress.

Payment

51. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 19 November 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

52. If the Commissioner receives full payment of the monetary penalty by 18 November 2013 the Commissioner will reduce the monetary penalty by 20% to £64,000 (sixty-four thousand pounds).

Right of Appeal

53. 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.

54. Any Notice of Appeal should be served on the Tribunal by 5pm on 19 November 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.

Enforcement

---

55. 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.

Dated the 15 October 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 19 November 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)).