Data Protection Act 1998

Monetary Penalty Notice

Dated: 9 November 2011

Name: North Somerset Council

Address: Town Hall, Walliscote Grove Road, Weston-super-Mare BS23 1UJ

Statutory framework

---

1. North Somerset Council is the data controller, as defined in section 1(1) of the Data Protection Act 1998 (the "Act"), in respect of the processing of personal data carried on by North Somerset Council and is referred to in this notice as the "data controller". 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 he is the data controller.

2. The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act"). By virtue of section 6(1) of the Act, the office of the Data Protection Registrar originally established by section 3(1) (a) of the 1984 Act became known as the Data Protection Commissioner. From 30 January 2001, by virtue of section 18(1) of the Freedom of Information Act 2000 the Data Protection Commissioner became known instead as the Information Commissioner (the "Commissioner").

3. 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 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. 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)(Maximum Penalty and Notices) Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010.

Power of Commissioner to impose a monetary penalty

(1) Under section 55A of the Act 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

4. On 12 November 2010, an employee of the data controller working in the [redacted], attached the draft minutes of a Serious Case Review Initial Incident Panel meeting to an email which was then sent using a personally created email distribution list. The name of the intended recipient was substituted for the name of an unintended recipient in the distribution list due to the fact that the names were the same in abbreviated form. Subsequently an employee of [redacted] inadvertently received this email and attachment which was unencrypted although it was protectively marked and the sensitivity of the contents was clear from the face of the email.

5. The data controller's employee was alerted to the error by the unintended recipient within minutes of the email being sent. The Commissioner has noted that [redacted] did not inform the data controller's Information Governance Team about the incident.

6. It is accepted by the data controller that the draft minutes contained confidential and sensitive personal data relating to eight individuals including details of [redacted] The draft minutes also contained (amongst other things) [redacted] The email distribution error was repeated by this employee on four further occasions.

7. On 24 November 2010, [redacted] emailed a letter from the Chair of the data controller's Local Safeguarding Children Board to the same unintended recipient at [redacted], although the letter only contained the names of the Local Safeguarding Children Board Partners which were already in the public domain.

8. On 30 November 2010, two further emails were inadvertently sent to the same unintended recipient at [redacted]. The first email attached a letter from the Chair of the Local Safeguarding Children Board Partners to the data controller's Chief Executive regarding the Serious Case Review. The letter contained an invitation to undertake an informal management review of NHS involvement with the case. The letter was headed with the [redacted] The second email contained the password that allowed access to the letter.

9. The Head of Information Governance at [redacted] contacted the data controller on 6 December 2010 to ask for the correct contact details for the data controller's Head of Information Governance. On 9 December 2010, the Head of Information Governance at [redacted] contacted the data controller to flag these issues which prompted a discussion between two of the data controller's Assistant Directors and this employee to prevent a recurrence. But later on the same day, an email containing a blank business action plan for use as part of the Serious Case Review was again inadvertently emailed to the same unintended recipient at [redacted]. Fortunately this email did not contain any personal data. On 10 December 2010, [redacted] made further contact with the data controller to report this incident.

10. The Commissioner understands that this employee (who worked in the [redacted]) was in a position of considerable responsibility with regard to the handling of

confidential and sensitive personal data and that [redacted] had been in post for approximately [redacted] years. In the circumstances, the Commissioner finds it surprising that [redacted] had "slipped through the net" and not completed any of the mandatory information governance training courses endorsed by the data controller.

11. The Commissioner understands that at the time of the security breaches, the data controller's "Information Security Incident Policy" and "Personal Information Security Policy" were available on its intranet. These policies cover the reporting and identification of information security incidents and the classification and sending of email messages according to the sensitivity of the content. These policies were also referred to in an article published in the data controller's in-house magazine in October 2010 which would have been available to all staff.

12. Although it is possible that this employee was aware from the intranet of the data controller's policies and acted in contravention of those policies, the Commissioner considers that any relevant policies should have been actively communicated by the data controller to all staff responsible for handling confidential and sensitive personal data (by way of training or otherwise) thereby ensuring that [redacted] was fully aware of their content.

13. The Commissioner acknowledges that the data controller has taken remedial action which includes publishing an article in the weekly newsletter to all staff highlighting the risks of using and managing distribution lists and that distribution lists should not be used for emailing sensitive or voluminous personal data to external bodies. In addition prioritised information governance training for staff handling sensitive personal data was to be completed by the end of June 2011.

14. The data controller has also implemented a recommendation from an internal audit investigation to introduce a management review and sign-off of e-mail distribution/circulation lists used to send sensitive personal data and commissioned a paper on the options for secure use of email. The data controller had already published an article in the weekly newsletter raising staff awareness of the need to report security incidents.

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

---

The relevant provision of the Act is the Seventh Data Protection Principle which 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".

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".

- 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 in relation to all personal data with respect to which he is the data controller.

  In particular, the data controller had failed to take appropriate technical and organisational measures against unauthorised processing of personal data such as providing its employees with appropriate information governance training, management sign-off of email distribution lists to ensure that recipients cannot easily be mistaken by its employees and considering a more secure means of transmission such as encrypting any emails that contain sensitive personal data. The Commissioner considers that the contravention is serious because the measures did not ensure a level of security appropriate to the harm that might result from such unauthorised processing and the nature of the data to be protected.

- The Commissioner is satisfied that the contravention is of a kind likely to cause substantial distress. Unauthorised confidential and sensitive personal data relating to eight individuals was unintentionally disclosed to an employee of [redacted] due to the inappropriate technical and organisational measures taken by the data controller. The failure to take appropriate technical and organisational measures has the potential to cause substantial distress to individuals who may know or suspect that their confidential and sensitive personal data has been disclosed to an individual who has no right to know that information. Furthermore they would be justifiably concerned that

their data may be further disseminated and possibly misused even if those concerns do not actually materialise. In this context it is important to bear in mind that some of the affected individuals are considered to be vulnerable.

- 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 failed to take reasonable steps to prevent the contravention.

  The Commissioner has taken this view because employees working in the data controller's [redacted] were used to handling confidential and sensitive personal data and the data controller should have realised the potential for human error in wrongly selecting drop down boxes from personally created email distribution lists when sending unencrypted emails containing confidential and sensitive personal data particularly when an employee has not received any information governance training.

  In the circumstances, the data controller ought to have known that there was a risk that the contravention would occur unless reasonable steps were taken to prevent the contravention, such as providing its employees with appropriate information governance training, ensuring management sign off of email distribution lists and considering a more secure means of transmission such as encrypting any emails that contain sensitive personal data. The risks of drop down boxes being wrongly selected are self evident and, in the Commissioner's view, widely known. Further it should have been obvious to the data controller whose [redacted] were used to handling confidential and sensitive personal data relating to vulnerable individuals 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

---

Nature of the contravention

- Five similar security breaches, two of which involved confidential and sensitive personal data
- Confidential and sensitive personal data was disclosed to a person who had no reason to see it

- Contravention was serious because of the confidential and sensitive nature of the personal data

Effect of the contravention

- The contravention was of a kind likely to cause substantial distress to the data subjects

Behavioural issues

- Lack of appropriate security training over a [redacted] year period
- Contravention was due to the negligent behaviour of the data controller in failing to take appropriate technical and organisational measures against the unauthorised processing of personal data

Impact on the data controller

- Sufficient financial resources to pay a monetary penalty up to the maximum without causing undue financial hardship

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

---

Nature of the contravention

- Small number of data subjects affected
- To the Commissioner's knowledge the personal data involved has not been further disseminated

Effect of the contravention

- The unintended recipient was a health professional and used to dealing with confidential and sensitive personal data (although this was largely fortuitous)
- Email and attachment was protectively marked and the sensitivity of the contents was clear from the face of the email
- The confidential and sensitive personal data received in error has been destroyed

Behavioural issues

- Voluntarily reported to Commissioner's office
- Detailed investigation report was compiled
- Substantial remedial action has now been taken

- Fully cooperative with Commissioner's office

Impact on the data controller

- Liability to pay monetary penalty will fall on the public purse although the penalty will be paid into the Consolidated Fund
- Significant impact on reputation of data controller as a result of this security breach

Other considerations

- 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 unencrypted email and to ensure either that 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

A Notice of Intent was served on the data controller dated 31 August 2011. The Commissioner received representations from the data controller in a letter from the Head of Legal & Democratic Services dated 29 September 2011. 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 considers that the contravention of section 4(4) of the Act is serious and that the imposition of a monetary penalty is

appropriate. Further that a monetary penalty in the sum of £60,000 (Sixty thousand pounds) is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

Payment

The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 9 December 2011 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

If the Commissioner receives full payment of the monetary penalty by 8 December2011 the Commissioner will reduce the monetary penalty by 20% to £48,000 (forty eight thousand pounds).

Right of Appeal

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

a. the imposition of the monetary penalty

and/or;

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

Any Notice of Appeal should be served on the Tribunal by 5pm on 8 December 2011 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

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.

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 or any sheriffdom in Scotland.

Dated the 9th day of November 2011

Signed: .....

David Smith
Deputy Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5A

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

   a) The notice of appeal should be served on the Tribunal by 5pm on 8 December 2011 at the latest.

   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;

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.

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 (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)).