Data Protection Act 1998

Monetary Penalty Notice

Dated: 24 January 2012

Name: Midlothian Council

Address: Midlothian House, 40-46 Buccleuch Street, Dalkeith, EH22 1YG

Statutory framework

---

1. Midlothian 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 out by Midlothian 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 it 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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 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. In March 2011, the data controller was informed by a [redacted] that he had received confidential personal data relating to a child [redacted]. The Commissioner understands that a social worker in the data controller's Children & Families Service had been working on several files at the same time and had entered the wrong child's name on the [redacted] agreement and sent it to the [redacted] in error. The data subject (a child) whose name was on the [redacted] agreement was not informed because the data controller took the view that it would cause significant distress to those involved in the [redacted] process.

5. In May 2011, a social worker in the Children & Families Service inadvertently sent a 'looked after' child review and care plan to the child's mother's GP requesting a report on the mother's health. The child was not registered with the GP's practice and this had not been checked against the data controller's database. Again, the data controller decided not to inform the data subject because it would cause significant distress to those involved in the care process. The Commissioner has noted that the recipient in this incident was a health professional and used to dealing with confidential and sensitive personal data.

6. On 14 May 2011, a child's "looked after care review" and "accommodated review" were attached to the papers of other children and posted to four unintended recipients by a social worker working in the data controller's Children & Families Service. The data controller did not inform the data subject for the same reason as stated in paragraphs 4 and 5 above.

7. On 1 June 2011, a social worker in the data controller's Children & Families Service erroneously sent minutes of a child protection conference by recorded delivery to the former address of the child's mother's partner. The mother's partner's address had not been updated on the data controller's database. The minutes were received by his former partner who had no reason to see them. The Commissioner understands that the former partner may have further disseminated this information to individuals in the wider local community.

8. On 6 June 2011, a social worker in the data controller's Children & Families Service inadvertently sent a letter regarding the status of a foster carer to seven individuals who had attended a child case conference. This was caused by one social worker using a shared printer to print out the letter which was then collected in error by another social worker who had printed out the case protection conference papers. The Commissioner has noted that the recipients in this last incident were all health professionals working at external agencies and used to dealing with confidential and sensitive personal data. The data controller did not inform the data subject because the impact had not been fully assessed.

9. At the time of these security breaches the data controller had an overarching policy covering data protection, information security and data sharing. However the Children & Families Service, whose staff deal with confidential and sensitive personal data on a daily basis, did not have any role-specific guidance or working procedures that promoted good practice in data handling. The data controller's

investigation into these security breaches revealed that training in the Children & Families Service was inadequate and that staff were largely unaware of their responsibilities under the Act, which had significantly contributed to these systemic failures.

10. The data controller has now taken remedial action which includes recovering the information from the unintended recipients; providing all staff working in the Children & Families Service with an "Introduction to information management awareness" training session; asking all staff working in the Children & Families Service to check that data is accurate before sending it out by post and that the database is updated with new addresses; peer checking envelopes containing confidential and sensitive personal data before it is sent out by post; ensuring that any 'looked after' or 'accommodated' children reports are not sent to GPs unless the address is checked against the NHS register and finally, providing the Children & Families Service with experienced staff to assist in developing appropriate policies and procedures in relation to future compliance.

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 it is the data controller.

In particular, the data controller had failed to take appropriate organisational measures against unauthorised processing of personal data, such as a peer checking process for envelopes containing confidential and sensitive personal data and having appropriate policies, procedures and training for staff working in the Children & Families Service. 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. Confidential and sensitive personal data was disclosed to unauthorised third parties due to the inappropriate organisational measures taken by the data controller. The failure to take appropriate organisational measures has the potential to cause substantial distress to data subjects whose confidential and sensitive personal data has been disclosed to third parties who have no reason to see it.

  In this particular case, the data subjects would suffer from substantial distress knowing that their confidential and sensitive personal data has been disclosed to third parties and that their data may have been further disseminated and possibly misused, even if those concerns do not actually materialise. This matter is aggravated by the fact that in one of the security breaches the information may have been further disclosed to individuals who live in the same locality as the data subject. In this context it is important to bear in mind that many of the affected individuals are children and considered to be vulnerable.

- The Commissioner is satisfied that section 55A (3) of the Act applies in that the data controller knew or 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 the data controller's Children & Families Service was used to dealing with such cases and would have been aware of the confidential and sensitive nature of the personal data they were dealing with. In addition, the first security breach was reported in March 2011 therefore the data controller was alerted to the risk from that time onwards.

  In the circumstances, the data controller knew or 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 a peer checking process for envelopes containing confidential and sensitive personal data and having appropriate policies, procedures and training for staff working in the Children & Families Service. Further, it should have been obvious to the data controller's staff (who were social workers) 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.

In addition, the Commissioner is of the view that the data controller knew there was a risk that the contravention would occur following the first security breach but failed to take reasonable steps in the intervening period to prevent a further contravention.

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

---

Nature of the contravention

- At least five similar security breaches occurred within five months of each other
- Unauthorised confidential and sensitive personal data relating to at least six vulnerable children was disclosed to unauthorised third parties
- Contraventions were serious because of the highly confidential and sensitive nature of the personal data

Effect of the contravention

- In one of the security breaches the information may have been further disseminated to individuals who live in the same locality as the data subject
- The contraventions were of a kind likely to cause substantial distress to the data subjects

Behavioural issues

- Data controller should have notified the Commissioner's office after the first security breach in March 2011
- Data controller failed to take sufficient remedial action following the first security breach to prevent a recurrence
- Contraventions were due to the negligent behaviour of the data controller in failing to take appropriate organisational measures

against the unauthorised processing of personal data

Impact on the data controller

- Data controller is a public authority so liability to pay a monetary penalty does not fall on an individual
- 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

- Unintended recipients in two of the security breaches were health professionals and used to dealing with confidential and sensitive personal data (although this was largely fortuitous)

Effect of the contravention

- Data subjects were not informed due to the data controller's assessment that this would cause them significant distress
- Personal data has either been recovered by the data controller or destroyed by the unintended recipients

Behavioural issues

- Voluntarily reported to Commissioner's office, albeit late in the day
- Detailed investigation report compiled
- Remedial action has now been taken
- Fully co-operative 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 these security breaches

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 handling of confidential and sensitive personal data and to ensure that appropriate and effective security measures are applied
- The Fourth Data Protection Principle at Part I of Schedule 1 to the Act was also contravened by the data controller in that inaccurate personal data was held on its database

Notice of Intent

A Notice of Intent was served on the data controller dated 11 November 2011. The Commissioner received representations from the data controller in a letter from a Director in the Education and Children's Services Department dated 9 December 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 £140,000 (One hundred and forty 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 24 February 2012 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 23 February 2012 the Commissioner will reduce the monetary penalty by 20% to £112,000 (one hundred and twelve 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 23 February 2012 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 24th day of January 2012

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 23 February 2012 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)).