Data Protection Act 1998

Monetary Penalty Notice

Dated: 16 November 2012

Name: Leeds City Council

Address: Civic Hall, Leeds LS1 1UR

Statutory framework

---

1. Leeds City 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 Leeds City 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. On 28 July 2011, a support assistant working in the data controller's Children Services department intended to send some documents internally to the professional who was involved in the review of a child's care plan. It was standard practice at the time to send internal mail in used envelopes because it was cost-efficient and environmentally friendly. Therefore the support assistant re-used an envelope which she had intended to send to an unrelated external user.

5. However, there was nothing on the front of the envelope to distinguish it from an envelope intended for the external mail and the support

assistant forgot to cross out the address of the external user. When the support worker came across the envelope later that day she mistakenly assumed that the envelope was intended for the external post tray and it was erroneously sent out.

6. The documents contained personal data relating to four data subjects including confidential/highly sensitive personal data relating to a "looked after" young person, including reports containing details of a criminal offence committed by the young person, details of where he was allowed to reside, details of his non-attendance at school, the level of contact agreed with his siblings and information about his relationship with his mother.

7. The Commissioner understands that although the data controller had overarching policies relating to data protection and information security (among others) which were available to staff on the intranet together with limited training, there were no specific policies or training on security measures to be applied when sending sensitive personal data to internal or external third parties.

8. Following the security breach, the unintended recipient (the external user referred to in paragraph 5 above) sent an email to inform the data controller that she had received the letter the previous day. The unintended recipient was a grandmother who had previously received correspondence from the data controller in relation to one of her grandchildren. The data controller then contacted the unintended recipient and arranged for the collection of the documents on 1 August 2011. The data controller also sent a letter of apology to the affected individuals.

9. Following an internal investigation, the data controller has now taken remedial action which includes having different envelopes for internal mail and using new envelopes for external mail. In addition, the external mail has to be marked up with a budget code to distinguish it from the internal mail and envelopes containing sensitive personal data are also peer checked before delivering such mail by hand. Finally, the data controller has introduced a comprehensive training programme on information governance for all staff.

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 particular, the data controller had failed to take appropriate organisational measures against unauthorised processing of personal data such as using different envelopes for internal and external mail that are clearly distinguishable and having a peer checking process for envelopes containing sensitive personal data and appropriate training for all staff.

  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.

  The failure to take appropriate organisational measures has the potential to cause substantial distress to data subjects whose personal data has been disclosed to a third party who had no right to see 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 one of the data

subjects is considered to be a vulnerable young person.

- 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 staff who worked in the data controller's Children Services department were used to dealing with such cases and the data controller would have been aware of the confidential and highly sensitive nature of the personal data they were dealing with. Any effective security risk assessment would have identified the risks involved in the system of working and ensured they were addressed.

  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 using different envelopes for internal and external mail that are clearly distinguishable and having a peer checking process for envelopes containing sensitive personal data and appropriate training for all staff.

  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 at least one of 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

- System of work at the time of security breach was fundamentally flawed
- No checks were undertaken prior to dispatch
- Contravention was particularly serious because of the highly confidential and sensitive nature of the personal data

Effect of the contravention

- One of the data subject was considered to be a vulnerable young person

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

- To the Commissioner's knowledge the personal data has not been further disseminated
- There have been no similar security breaches as far as the Commissioner is aware

Behavioural issues

- Voluntarily reported to Commissioner's office
- Immediate steps taken to recover the information from the unintended recipient
- Letter of apology sent to the affected individuals
- Remedial action has 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 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

Notice of Intent

A notice of intent was served on the data controller dated 11 September 2012. The Commissioner received written representations from the data controller's Chief Executive in a letter dated 12 October 2012. 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 £95,000 (Ninety five 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 21 December 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 20 December 2012 the Commissioner will reduce the monetary penalty by 20% to £76,000 (Seventy six 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 20 December 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 16th day of November 2012

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

   a) The notice of appeal should be served on the Tribunal by 5pm on 20 December 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)).