Data Protection Act 1998

Monetary Penalty Notice

Dated: 12 December 2012

Name: London Borough of Lewisham

Address: Town Hall, Catford, London SE6 4RU

Statutory framework

---

1. London Borough of Lewisham 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 London Borough of Lewisham 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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 Friday 16 March 2012, a social worker employed by the data controller on a probationary period, took case papers relating to a child protection matter out of the office so that he could prepare for an upcoming court hearing over the week-end. The social worker carried the papers in an opaque plastic shopping bag which he then mistakenly left on the train on his journey home. The bag containing the papers was recovered from the train company's lost property office seven days later.

5. The case papers contained confidential and highly sensitive data relating to a family with [redacted] children who were the subject of care proceedings due to allegations of abuse and neglect against the perpetrators, including sexual abuse. There were also a number of internal reports, case reviews and supporting statements from a variety of agencies such as schools and GPs. Confidential police reports were included in the papers which contained details of suspected perpetrators where abuse had been alleged.

6. The Commissioner understands that social workers were often required to deal with cases outside normal working hours. Therefore they were allowed to take case papers out of the office without permission even though social workers were given an encrypted laptop computer to provide remote access to the data controller's network.

7. The data controller had overarching policies on data protection and information security but there was no specific guidance on how sensitive personal data should be transported. Although training materials were available on the intranet, the social worker had not completed the e-learning program which briefly touched on this issue.

8. The data controller has now taken remedial action which includes the provision of lockable bags in which to carry any such case papers and the provision of a restricted number of encrypted USB pens which will be used in a controlled manner. The data controller is also considering a more secure means of accessing sensitive personal data out of the office such as using their encrypted laptop computers to provide remote access to the data controller's network.

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 technical and organisational measures against the accidental loss of personal data such as having robust policies/guidelines in place; training for staff who have a business need to take paper files containing sensitive personal data out of the office; providing security locks for bags and considering a more secure means of accessing sensitive personal data out of the office, for example, using encrypted USB pens.

  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 accidental loss 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 highly sensitive personal data was lost 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 highly sensitive personal data has been disclosed to a recipient who has no right to see that information.

  Further, 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 [redacted] of the affected individuals are considered to be vulnerable children.

  Further, the contravention could have prejudiced the court hearing of the child protection case which would have caused substantial distress to the children concerned and to others involved.

- 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 social workers working in the Children's Social Care department were used to dealing with such cases. Further, the data controller recognised that social workers had a business need to take paper files containing confidential and sensitive personal data out of the office.

  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 having robust policies/guidelines in place; training for staff who have a business need to take paper files containing sensitive personal data out of the office; providing security locks for bags and considering a more secure means of accessing sensitive personal data out of the office, for example, using encrypted USB pens.

  Further, it should have been obvious to the data controller whose staff were routinely involved in childcare litigation 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

- Confidential and sensitive personal data was lost for a period of seven days
- Contravention was particularly serious because of the confidential and sensitive nature of the personal data

Effect of the contravention

- Potential to disrupt ongoing legal case and interfere with the administration of justice
- Potential for extensive media coverage about the data subjects intimate personal lives

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

- No previous similar security breach that the Commissioner is aware of

Effect of the contravention

- No evidence that the file of papers has been further disseminated to date

Behavioural issues

- Voluntarily reported to Commissioner's office
- Data controller informed the police, contacted the train company and subsequently recovered the bag from the train company's lost property office
- Data controller's Information Governance Team had been completing a risk assessment of the Social Care Departments at the time of this incident and had identified some of the risks posed but had not completed their review before the breach occurred
- Fully cooperative with Commissioner's office
- Substantial remedial action has been taken

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
- There has been no press coverage to date

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 remind data controllers to ensure that appropriate and effective security measures are applied to paper files containing confidential and sensitive personal data that are taken out of the office

Notice of Intent

A notice of intent was served on the data controller dated 23 October 2012. The Commissioner received representations from the data controller in an email from the Corporate Information and Records Manager dated 22 November 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 £70,000 (Seventy 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 16 January 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

If the Commissioner receives full payment of the monetary penalty by 15 January 2013 the Commissioner will reduce the monetary penalty by 20% to £56,000 (Fifty 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 15 January 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

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 12th day of December 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 15 January 2013 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)).