Data Protection Act 1998

Monetary Penalty Notice

Dated: 6 February 2012

Name: London Borough of Croydon

Address: Taberner House, Park Lane, Croydon CR9 3JS

Statutory framework

---

1. London Borough of Croydon 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 Croydon 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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 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 20 April 2011, a bag containing a file of papers relating to a child in the care of the data controller was stolen from a Public House in London. The bag belonged to a Social Worker who worked in the data controller's Children and Young People's Department. The Commissioner understands that the Social Worker had taken the file home at 5pm that day so that he could travel straight to an appointment about the case the following morning to save travelling time. The Social Worker went home via a crowded Public House and left the unlocked bag in between the chairs in which he was sitting with

his colleagues.

5. The file of papers in the stolen bag contained highly confidential and sensitive personal data relating to the sexual abuse of a child which resulted in care proceedings at Court. At least seven data subjects were affected by the security breach namely the child, the child's Solicitor, both of the child's parents and their respective Solicitors and the Social Worker. The information contained in the file of papers included details of the sexual abuse, extracts from the child's psychiatrist report and highly personal information obtained from the foster carer about the child's behaviour.

6. The data controller's Corporate Policy on information security (available on the Intranet) included a security list of "do's and don'ts", the only relevant section being "don't leave files of papers containing personally identifiable or other sensitive information unattended in an unsecure environment." The "Caldicott and Data Protection Policy" includes a code of practice requiring that "Data/Information should not be left unattended in public areas and should be protected against loss, damage or unauthorised disclosure at all times". The "Storing Information" guidelines in the Corporate Policy simply required staff to "ensure that hard copies of confidential data are securely transported and stored when shared with Partners or taken out of the office".

7. The data controller has informed the Commissioner that staff who work with children all receive training on "compliance with the Act and other relevant legislation." However, the Social Worker involved in this security breach does not appear to have received any information security training from the data controller, the onus being on staff to read the data controller's policies on the data controller's intranet and update their own knowledge. Further, the data controller did not check or monitor that staff had read and understood the information security policies on the intranet. This was despite the fact that Social Worker's were routinely involved in childcare litigation and there was a recognised business need for Social Worker's to take confidential and sensitive personal data out of the office.

8. When the Social Worker realised that the bag was missing at approximately 11pm that evening he immediately reported the theft to the police. However, the bag containing the file of papers has not been recovered to date. The data controller also took steps to inform the data subjects and the Court about the security breach. Following the security breach the data controller sent an email reminding all staff, amongst other things, not to take information out with them socially after work, for example, to restaurants and licensed premises.

9. The data controller has now taken further remedial action which includes providing staff with refresher training; reminding staff of the importance of keeping information secure on a regular basis; making greater use of encrypted laptops and USB pens when taking information out of the office and carrying out a data protection audit.

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 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 taking sensitive personal data out of the office, for example, using encrypted laptops and 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 sensitive personal data was stolen 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 data subjects whose confidential and sensitive personal data has still not been recovered.

  In this particular case the contravention is likely to cause substantial distress to individuals who know or suspect that their confidential and sensitive personal data has been stolen by an individual 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 one of the affected individuals is considered to be a vulnerable child.

  Further, the contravention could have prejudiced the Court hearing of the sexual abuse case which would have caused substantial distress to the child concerned and to others involved.

- 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 Social Workers working in the data controller's Children and Young People's 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 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 taking sensitive personal data out of the office, for example, using encrypted laptops and 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 and has not been recovered to date
- Contravention was serious because of the highly 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
- Potential for extensive media coverage about the data subjects intimate personal lives
- Potential to disrupt ongoing legal case and interfere with the administration of justice

Behavioural issues

- Contravention was due to the negligent behaviour of the data controller in failing to take appropriate technical and organisational measures against the accidental loss 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

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

Effect of the contravention

- No complaints have been received from any of the affected individuals
- 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, the data subjects and the Court about the security breach
- Substantial 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 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 25 November 2011. The Commissioner received representations from the data controller in a letter from the Director of Legal and Democratic Services dated 23 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 £100,000 (One hundred 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 6 March 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 5 March 2012 the Commissioner will reduce the monetary penalty by 20% to £80,000 (eighty 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 5 March 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 6th day of February 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 5 March 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)).