

Data Protection Act 1998

Monetary Penalty Notice

Dated: 15 May 2012

Name: London Borough of Barnet

Address: North London Business Park, Oakleigh Road South, London N11 1NP

Statutory framework

1. The London Borough of Barnet 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 London Borough of Barnet 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. The data controller employs social workers in its Children's Services directorate. On 23 April 2011, one of the social work service managers took home paper records containing confidential and highly sensitive personal data. Although some of the information was anonymised the Commissioner is satisfied that there were a number of documents that identified the data subjects. The paper records were kept in the social worker's laptop bag along with an encrypted computer. The social worker's home was burgled and the laptop bag containing the paper

records was stolen.

5. The paper records contained (among other things) confidential and highly sensitive personal data relating to (i) a complaint about the handling of a child sexual abuse investigation by the police and the data controller, and (ii) a project on child sexual exploitation (the "project") run by the service manager. The data included (among other things) names, addresses, dates of birth and details of their sexual activities affecting, in all, some 15 data subjects. The police were informed of the burglary and the area was searched for any stolen items. To date, the stolen laptop bag and its contents have not been recovered and the data subjects have all been informed about the security breach.
6. The Commissioner understands that social workers and their managers are often required to deal with cases outside normal working hours so they are permitted to take case papers out of the office when there is a business need to do so. The data controller has confirmed that there was no alternative to taking the paper records home in this case because the service manager was preparing a review of the project and therefore required access to all of the paper records contained in the laptop bag for cross-referencing purposes. The Commissioner was told that this work could not have been carried out using alternative secure electronic means.
7. The data controller had an information security policy which covered home-working but the Commissioner is of the view that it did not address the risk identified by this security breach. Although there was limited guidance on the data controller's intranet at the time about its proposed paper handling policy (the "policy") which now requires (among other things) that paper records must be kept secure when off-site and totally separate from valuable items such as laptop computers, the policy was not in force at the time of the incident. The Commissioner considers that, as the data controller signed an Undertaking in relation to data security in June 2010, following an earlier incident in which personal data had been stolen from an employee's home, the policy could have been implemented sooner. The data controller has now formally introduced the policy which (if followed) should minimise the risk of a similar security breach, although the Commissioner considers that further attention still needs to be given to staff training.

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 particular, the data controller has failed to take appropriate organisational measures against the accidental loss of personal data held on paper records such as providing specific guidance and training to social workers on securing paper records at home. The Commissioner considers that the contravention is serious because the measures did not ensure a level of security appropriate to the nature of the data to be protected and the harm that might result from accidental loss.

- The Commissioner is satisfied that the contravention is of a kind likely to cause substantial distress. The data controller’s failure to take appropriate organisational measures was likely to cause substantial distress to data subjects whose confidential and highly sensitive personal data may be disclosed to third parties.

In this particular case the data subjects would suffer from substantial distress knowing that their confidential and highly sensitive personal data may be disclosed to third parties even though, as far as the Commissioner is aware, those concerns have not so far materialised. This is aggravated by the fact that the paper records have still not been recovered. If the data is in fact disclosed to untrustworthy third

parties then it is likely that the contravention would cause further distress to the data subjects.

In this context it is important to bear in mind that most 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 social workers in the Children's Services directorate 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 and that it was often necessary for paper records to be taken out of the office to carry out their business.

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 providing specific guidance and training to social workers on securing paper records at home.

Further, it should have been obvious to the data controller, which employed social workers who were routinely involved in handling large amounts of confidential and highly sensitive personal data 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. It is possible that an unauthorised third party could still obtain this data and may already have done so.

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

Nature of the contravention

- Contravention was serious because of the confidential and highly sensitive personal data involved in the security breach
- The data related to approximately 15 data subjects, all of whom were vulnerable children or young people

Effect of the contravention

- Paper records have still not been recovered
- Some of the data subjects could be at risk if the paper records were disclosed to untrustworthy third parties
- The contravention was of a kind likely to cause substantial distress to the data subjects

Behavioural issues

- Contravention was due to the negligent behaviour of the data controller in failing to take appropriate 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

- Limited guidance on proposed paper handling policy was available on the intranet

Effect of the contravention

- No evidence to suggest that the personal data has been inappropriately processed
- No complaints received from the data subjects to date

Behavioural issues

- Agreed to an ICO audit prior to security breach
- Voluntarily reported to the Commissioner's office
- Data controller fully co-operative with Commissioner's office
- Data controller informed the data subjects about the security breach
- Full investigation carried out
- Some remedial action has now 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

Other considerations

- The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the Act and this is an opportunity to reinforce the need for data controllers to ensure that appropriate and effective security measures are applied to paper records containing personal data

Notice of Intent

A Notice of Intent was served on the data controller dated 14 March 2012. The Commissioner received representations from the data controller in a letter from the Director of Corporate Governance dated 19 April 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 15 June 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 14 June 2012 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 14 June 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 15th day of May 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 14 June 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)).