**Data Protection Act 1998**

**Monetary Penalty Notice**

**Dated: 4 February 2011**

**Name: London Borough of Hounslow**

**Address: Civic Centre, Lampton Road, Middlesex TW3 4DN**

## Statutory framework

1. London Borough of Hounslow 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 Ealing 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 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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)(Maximum Penalty 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

1. Ealing Council provides an out of hours [redacted] service which is operated by nine members of staff who work from home. The team work between 5pm and 9am and also have an arrangement to provide the same service on behalf of the data controller. When calls come into the data controller's switchboard from a number of sources [redacted], the switchboard contacts the team with the necessary details. The team have to react promptly and take immediate action which is why laptops are used because they provide quick and easy access to past and current records. The team then contacts the client, completes the referral forms and actions the

referral. The completed forms were then faxed back to the data controller by the team who do not have access to the data controller's network.

2. [redacted]. After the team's involvement, updated records are transferred to the data controller's main database but remain on the employee's laptop in case of future referrals. Ealing Council states that the working practice for the team is to use previous contacts for future contact and that this has been the method of operation since January 2005.

3. A laptop issued by Ealing Council during 2006 and a personal laptop were located in a room which was used as an office [redacted] employee's home. They were both stolen during what would appear to be an opportunistic theft. [redacted] The laptop computers have not been recovered but there is no evidence to suggest that the data held on the laptop computers has been accessed and no complaints from clients have been received by the data controller to date.

4. Both laptops held sensitive personal data relating to both the data controller's clients and Ealing Council's clients and whilst the data subjects have been identified, it is not known exactly how the records were split across each laptop. Some of the records contained some duplicates due to repeat contact for the same individual but at different times. 698 of the data controller's clients were affected [redacted]. 958 of Ealing Council's clients were affected [redacted]

5. The records contained data such as first name, surname, date of birth, age, gender, ethnicity, first language, address, postcode, telephone number, reason for contact (in normal text), further information/action taken by the team, action now required by day staff, [redacted]

[redacted]. The laptop issued by Ealing Council and the personal laptop were both unencrypted.

6. The written contract in place between Ealing Council and the data controller [redacted] had expired in 2009 but even then did not contain any requirements about the security of personal data. The data controller did not monitor Ealing Council's compliance with the requirements of the Act and therefore the data controller was unaware of how the personal data relating to its service was being processed. Prior to 2009 the data controller had no security policy in place and the only reference to data protection at that time was a basic list of "Do's and Don'ts". In October 2009 the data controller introduced an Information Security Policy which required, amongst other things, that all of its laptops must be encrypted.

7. Following the incident, the data controller contacted [redacted] affected data subjects [redacted]. The data controller also reviewed the service provided by the team and decided that it should be continued but with a Memorandum of Agreement in place between Ealing Council and the data controller to cover security, regular auditing and compliance statements. The Memorandum of Agreement includes a requirement to comply with the data controller's Information Security Policy that all laptop computers should be encrypted. Finally, the data controller has agreed to consider an ICO 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 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".*

Paragraph 11 at Part II of Schedule 1 to the Act provides that:

*"Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle-*

*(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and*

*(b) take reasonable steps to ensure compliance with those measures.*

Paragraph 12 at Part II of Schedule 1 to the Act further provides that:

*"Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless-*

*(a) the processing is carried out under a contract-*

*(i) which is made or evidenced in writing, and*

*(ii) under which the data processor is to act only on instructions from the data controller, and*

*(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.*

- 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 failed to choose a data processor which provided sufficient guarantees in respect of the technical and organisational security measures governing the processing to be

carried out, and take reasonable steps to ensure compliance with those measures. Further, the data controller did not have a contract in writing with Ealing Council under which the data processor was to act only on instructions from the data controller, and which required Ealing Council to comply with obligations equivalent to those imposed on a data controller by the Seventh Data Protection Principle. The Commissioner would expect that such a contract would, amongst other things, make provision for the encryption of any laptop computer on which personal data is held together with regular auditing of the data processor to ensure compliance with this and other measures. The Commissioner considers that the contravention is serious because there was no contract in place requiring Ealing Council to comply with obligations equivalent to those imposed on a data controller by the Seventh Data Protection Principle.

- The Commissioner is satisfied that the contravention is of a kind likely to cause substantial damage or substantial distress. The data controller's failure to comply with paragraphs 11 and 12 at Part II of Schedule 1 to the Act was likely to cause substantial damage and/or substantial distress to data subjects whose personal data and sensitive personal data may be disclosed to third parties.

  In this particular case the data subjects are likely to have suffered from substantial distress knowing that their personal data and 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 laptops 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 and also substantial damage to the data subjects such as exposing them to identity fraud or causing damage to their personal reputations and relationships.

- 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 damage or substantial distress, but failed to take reasonable steps to prevent the contravention.

  The Commissioner has taken this view because a large amount of personal data relating to the data controller's clients had been processed on unencrypted laptops by Ealing Council since approximately 2005. The nature of the job role required significant home working, and none of the nine members of the team had access to the data controller's network. There was no contract in place

between the data controller and Ealing Council so the data controller had no assurances about how the personal data relating to its service was being processed by Ealing Council. Although Ealing Council had been processing personal data on behalf of the data controller for approximately six years, the data controller had not carried out any monitoring to ensure the data processor's compliance with the Seventh Data Protection Principle. The data controller did not take any steps to find out whether unencrypted laptops were being used by the team.

At the time of the loss the data controller had an Information Security Policy in place (October 2009) which required, amongst other things, that all of its laptop computers must be encrypted. It is regrettable that the data controller did not have a written contract in place with Ealing Council which included a similar requirement. However, the fact that the data controller had an Information Security Policy in place at the time of the incident demonstrates that it recognised the risks of a security breach.

In the circumstances the data controller knew there was a risk that the contravention would occur unless reasonable steps were taken to prevent the contravention, such as having a written contract in place with Ealing Council which included provision for the encryption of any laptop computer on which personal data is held together with regular auditing of the data processor to ensure compliance with this and other measures.

In any event the data controller ought to have known that there was a risk that the contravention would occur unless the laptop computers used to process personal data relating to its clients were encrypted.

In view of the number of high profile data losses, the Commissioner's office provided published guidance on its website in November 2007 which clearly states that "there have been a number of reports recently of laptop computers, containing personal information which have been stolen from vehicles, dwellings or left in inappropriate places without being protected adequately. The Information Commissioner has formed the view that in future, where such losses occur and where encryption software has not been used to protect data, enforcement action will be pursued".

Further it should have been obvious to the data controller who was itself routinely involved in handling large amounts of personal data that such a contravention would be of a kind likely to cause substantial damage or substantial distress to the data subjects [redacted]

[redacted]

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

*Nature of the contravention*

- [redacted]Contravention was particularly serious because of the sensitive nature of some of the personal data [redacted]

*Effect of the contravention*

- Large amount of personal data and sensitive personal data held on the laptop relating to [redacted] 630 data subjects [redacted]
- The contravention was of a kind likely to cause substantial damage and substantial distress to the data subjects

*Behavioural issues*

- No written contract in place between data controller and Ealing Council and no assurances about how personal data processed
- No monitoring or auditing of Ealing Council's policies and procedures
- Prior to 2009 data controller had no personal data security policies in place
- All of the "data processor" requirements of the Seventh Data Protection Principle have been contravened
- 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
- Information Security Policy was actually in place
- Both laptops were password protected
- The contravention was exacerbated by circumstances outside the direct control of the data controller

*Effect of the contravention*

- No evidence to suggest that the personal data has been accessed
- No complaints received to date

*Behavioural issues*

- Data controller selected another local authority to act as its processor and might reasonably have expected it to be familiar with the nature of the personal data in question and the need for appropriate security
- A Memorandum of Agreement is now in place containing data security requirements
- The Memorandum of Agreement also includes regular auditing requirements and compliance statements
- Data controller informed [redacted] data subjects
- Remedial action has now been taken
- Data controller will consider an audit by the ICO

*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 Third and Fifth Data Protection Principles at Part I of Schedule 1 to the Act were also contravened by the data controller in that irrelevant and excessive personal data was held on the laptops and kept for longer than was necessary for the purpose of providing a social care service
- 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, such as encryption, are applied to personal data held on laptop computers

## Notice of Intent

A notice of intent was served on the data controller dated 3 December 2010. The Commissioner received representations from the data controller in a letter from their Principal Lawyer dated 7 January 2011. The Commissioner has now 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 8 March 2011 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 7 March 2011 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 8 March 2011 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 4th day of February 2011

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 8 March 2011 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)).