Data Protection Act 1998

Monetary Penalty Notice

Dated: 4 February 2011

Name: Ealing Council

Address: Perceval House, 14-16 Uxbridge Road, Ealing, London W5 2HL

Statutory framework

1. Ealing 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 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. The data controller provides an out of hours [redacted] service which is operated by nine members of staff who work from home. This team work between 5pm and 9am [redacted] This team receive contact from a number of sources [redacted]. They 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. Mainframe/network

service access is limited out of hours due to maintenance down time.

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

3. A laptop issued by the data controller 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 although 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 London Borough of Hounslow'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 duplication due to repeat contact for the same individual but at different times. 958 of the data controller's clients were affected [redacted]. 698 of the London Borough of Hounslow'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 the data controller and the personal laptop were both unencrypted in breach of the data controller's own policy which stated that all portable and removable media containing personal data should be encrypted.

6. The data controller has stated that all its employees are provided with its Information and Data Management Policies at induction which they are obliged to follow. It is understood that the employee in question had been in the post for 12 years and had breached a number of these policies including the Removable Media Policy (June 2009) by not encrypting both laptops, and failing to obtain the approval of the data controller to use the personal laptop. However, no confirmation was sought by the data controller that these policies had been read and understood by the employee. The employees' managers were also responsible for ensuring that Home working policies are adhered to and a 'Working from Home' risk assessment should be carried out at commencement of home working along with quarterly assessments. None of this had taken place in this instance.

7. Following the incident an Emergency Data Breach Taskforce was appointed to evaluate the situation and closely monitor the remedial activity. This group included several Heads of Department and Directors. The group was extended to include Business Service Partners and Legal Representatives. The London Borough of Hounslow was also informed of the incident so that they could formulate their own action plan. As of 17 May 2010 all of the data controller's laptops and memory sticks had been fully encrypted. The data controller also contacted [redacted] affected data subjects [redacted] Focused data protection training programmes have also been provided to several departments [redacted]

8. Further, a new 'Information Protection Policy' has been implemented which will enhance the data controller's other policies on ICT and Data Management. A new Removable Media Policy was reissued in May 2010 and disseminated via the data controller's intranet and referred to in team meetings and one-to-ones. A 'Meta-compliance policy affirmation programme' has been implemented to ensure compliance with policies together with the implementation of a final software solution to detect unencrypted devices planned for Q4 2010/11. The data controller's relevant database provides a high level reference to data protection and information security and all staff are required to attend this training. Finally, the data controller has agreed to consider an audit by the ICO.

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 has failed to take appropriate technical and organisational measures against the accidental loss of personal data held on the laptop computers such as a combination of encrypting the laptop computers, providing the employee with security devices for the laptop computers, for example, a Kensington lock or a cable, providing guidance to the employee on securing laptop computers when working at home, "working from home" risk assessment and monitoring of staff equipment usage and having "out of hours" remote access to the central secure network. 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 damage or substantial distress. The data controller's failure to take appropriate technical and organisational

measures 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 the data controller issued the employee with an unencrypted laptop computer in breach of its own policies. The data controller did this despite being aware of the risks of failing to take appropriate technical and organisational measures against the accidental loss of personal data.

  At the time of the loss the data controller had a Removable Media Policy (June 2009) which required, amongst other things, that all portable and removable media containing personal data must be encrypted. In addition the data controller had commenced a programme of work to embed encryption of all its laptops across Ealing Council. It is regrettable that the data controller breached its own policies in not carrying out a "home working" risk assessment. However, the fact that the data controller had these policies and processes in place 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 encrypting the laptop computers, having "out of hours" remote access to the data on the data controller's central secure network, providing security devices for the laptop computers, for example, a Kensington lock or a cable, and issuing guidance on securing laptop computers when working at home.

In any event the data controller ought to have known that there was a risk that the contravention would occur unless the laptop computers 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 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]. It is possible that an unauthorised third party could still access 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

[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 nearly 800 data subjects [redacted]
- The contravention was of a kind likely to cause substantial damage and substantial distress to the data subjects

Behavioural issues

- Data controller issued employee with an unencrypted laptop in breach of its own policies
- No risk assessment was carried out on employee's home in breach of its own policies

- Data controller was unaware the employee was using a personal laptop and did not monitor staff equipment usage
- 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
- Security policies were actually in place
- Both laptops were password protected

Effect of the contravention

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

Behavioural issues

- Voluntarily reported to Commissioner's office
- Data controller cooperative with Commissioner's office
- [redacted]The data controller informed [redacted] data subjects, [redacted]
- Helplines were established to assist and provide information
- Programme of encryption has now been fully embedded
- Substantial remedial action has 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 the data controller's 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 the Chief Executive dated 11 January 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 £80,000 (Eighty 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 £64,000 (sixty four 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)).