Data Protection Act 1998

Monetary Penalty Notice

Dated: 19 November 2012

Name: Plymouth City Council

Address: Civic Centre, Armada Way, Plymouth PL1 2AA

Statutory framework

---

1. Plymouth City 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 out by Plymouth City 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 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. Social worker 1 and social worker 2 were both employed by the data controller and worked in the same building in the Children's Services department. Social worker 2 had difficulty in printing a report on the printer on his floor so he attempted to print the report on the printer on the first floor that is normally used by social worker 1. Unfortunately, the printer on the first floor did not print this report immediately and it was stored in the system for the time being. However, social worker 2 did not wait by the printer on the first floor to collect the report.

5. Social worker 1 then sent a similar report to be printed on the first floor printer which was printed at the same time as the stored report

belonging to social worker 2. Both reports were picked up from the printer by social worker 1 who assumed that the printing just consisted of his report. On 23 November 2011, social worker 1 gave his report to family B's mother. Unfortunately, the report also included three pages of a photocopied report relating to family A. The photocopied report contained confidential and highly sensitive personal data relating to two parents and their four children including allegations of child neglect resulting in ongoing care proceedings.

6. The Commissioner understands that family B's mother read the report and then telephoned the data controller to report their mistake. The data controller recovered the photocopied report from family B's mother within two hours and advised her that the information was confidential. However, family B's mother also contacted family A via a private message on a social networking site to inform them that she had received information about their family. The data controller was also unaware that family B's mother had sent a copy of the photocopied report to her Solicitor which was subsequently destroyed.

7. An independent audit carried out at the time of the security breach concluded that "the incident occurred as a result of human error compounded by the fact that the system in place, for the printing and despatch of sensitive data to clients, did not incorporate an adequate level of checks in order to ensure the documents were being sent to the correct recipient. At the time of the incident, there was an inherent weakness within the system and it was clear that unless steps were taken to rectify this, a similar incident could happen again".

8. Subsequently, the data controller carried out a review of the printing process and it was discovered that over a 15 minute period that one of the printers in the Children's Services department was in constant use by up to five members of staff, during which time it jammed on six occasions. These difficulties meant that staff were leaving the printer location before their printing had been produced which increased the risk of it being picked up by another user.

9. The Commissioner understands that the data controller has now taken remedial action which includes introducing a new printing procedure for the Children's Services department which requires staff to enter a user ID before their documents can be printed. Further, any items that are not printed within twelve hours are now automatically deleted from the print queue. Finally, the data controller has taken steps to raise staff awareness on information security.

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 unauthorised processing of personal data, such as having a more secure system for printing reports containing sensitive personal data and ensuring that such reports are peer checked to make sure they are not disclosed to unauthorised third parties.

  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 unauthorised processing and the nature of the data to be protected.

- The Commissioner is satisfied that the contravention was of a kind likely to cause substantial damage or substantial distress to data subjects whose confidential and sensitive personal data was disclosed to a third party who had no right to see that information.

  In this particular case, the data subjects would suffer from substantial distress knowing that their confidential and sensitive personal data has been disclosed to a third party and that their data may be further disseminated even if those concerns do not actually materialise. If the

data has been 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 physical harm or even blackmail.

This matter is aggravated by the fact that family B's mother contacted family A via a private message on a social networking site to inform them that she had received the information.

- 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 staff working in the Children's Services department were used to dealing with such cases and the data controller would have been aware of the confidential and sensitive nature of the personal data they were dealing with.

  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 a more secure system for printing reports containing sensitive personal data and ensuring that such reports are peer checked to make sure they are not disclosed to unauthorised third parties.

  Further, it should have been obvious to the data controller who employed social workers that such a contravention would be of a kind likely to cause substantial damage or 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

- Contravention was particularly serious because of the confidential and sensitive nature of the personal data
- No checks were undertaken before the report was disclosed to the third party

Effect of the contravention

- Family B's mother contacted family A via a private message on a social networking site to inform them that she had received the information
- The security breach put family A at risk of physical harm or even blackmail
- Both family A and family B are the subject of care proceedings and the disclosure may affect the care plan for their children
- No formal complaints have been received to date but the data controller received separate representations from both families

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

- The Commissioner is not aware of any similar contraventions

Effect of the contravention

- To the Commissioner's knowledge the photocopied report has not been further disseminated

Behavioural issues

- Voluntarily reported to the Commissioner's office
- Data subjects were quickly notified about the security breach
- Immediate action was taken to recover the photocopied report
- Family B's mother was advised that the photocopied report was confidential
- Independent audit carried out
- Remedial action 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 these security breaches

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 reinforce the need for data controllers to review the handling of confidential and sensitive personal data and to ensure that appropriate and effective security measures are applied

Notice of Intent

A notice of intent was served on the data controller dated 11 September 2012. The data controller's Corporate Information Manger informed the Commissioner by email dated 19 October 2012 that they would not be making any representations in response to the notice of intent. 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 £60,000 (Sixty 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 21 December 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 20 December 2012 the Commissioner will reduce the monetary penalty by 20% to £48,000 (Forty eight 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 20 December 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 19th day of November 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 20 December 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)).