Data Protection Act 1998

Monetary Penalty Notice

Dated: 28 May 2012

Name: Telford & Wrekin Council

Address: Civic Offices, Coach Central, Telford TF3, 4WZ

Statutory framework

---

1. Telford & Wrekin 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 Telford & Wrekin 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. On 31 March 2011, a member of staff working in Safeguarding Services sent the Social Care Core Assessment (the "Assessment") for child [redacted] by post to child [redacted]'s [redacted] instead of her mother who lived at the same address. The Assessment contained confidential and highly sensitive personal data including the history of child [redacted]'s [redacted] behaviour and its effect on other members of [redacted] family; [redacted] to child [redacted] and his mother together with her views on the situation.

5. Child [redacted]'s Assessment also included the name and address, date of birth and ethnicity of child [redacted] (a [redacted]) who had made an allegation

of [redacted] against Child [redacted]. Likewise, the Social Care Core Assessment sent to child [redacted] included the name and address, date of birth and ethnicity of child [redacted] in error.

6. An investigation carried out by the data controller revealed that the relationship records set up on the children's information system ("Protocol") for child [redacted] and child [redacted] were not populated with adequate information. Further, the Protocol system was set up so that the details of individuals were printed automatically on the Assessment although a user could tick a box to ensure that such details would not be printed. Finally, there was no process in place to check the documents before they were sent out in the post.

7. A Placement Information Record ("PIR") is a document signed by the parents of children who are due to be placed in foster care. It provides information about the children to enable the foster carers to look after them. Certain parts of the PIR were automatically populated by the Protocol system e.g. the foster carers names and addresses, although a Social Worker can exclude the foster carer's details if appropriate.

8. On 27 May 2011, the names and addresses of the foster care placements for two young children were inadvertently included in their PIR. The Social Worker then took a print of the PIR for the children's mother to sign who noticed the address of the foster care placements. The data controller then decided to move the children to alternative foster care placements to minimise the effect on the data subjects concerned.

9. An investigation carried out by the data controller following the second security breach revealed that the default setting on the Protocol system was to include the foster carer's details in the PIR and there was no process in place to check the PIR after it was printed.

10. Following these security breaches the data controller has now taken remedial action which includes providing staff working in Safeguarding Services with further training and support on data protection and information security and on using the Protocol system, introducing formal guidance on checking documents printed off the Protocol system and making changes to its configuration.

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 failed to take appropriate technical and organisational measures against unauthorised processing of personal data, such as having a "privacy friendly" children's information system, a formal checking process for documents printed off the Protocol system and having appropriate training for staff working in Safeguarding Services.

  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 is of a kind likely to cause substantial distress. Confidential and sensitive personal data was disclosed to unauthorised third parties 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 personal data has been disclosed to third parties who have no reason to see it

  In this particular case, the data subjects would suffer from substantial distress knowing that their confidential and sensitive personal data has been disclosed to third parties and 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 some of the affected individuals are vulnerable children, two of whom were moved to alternative foster care placements as a result of the second security breach.

- 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 staff working in the Safeguarding Service were used to dealing with such cases on a daily basis 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 "privacy friendly" children's information system, a formal checking process for documents printed off the Protocol system and appropriate training for staff working in the Safeguarding Service.

  Further, it should have been obvious to the data controller who employed staff who worked in the Safeguarding Service 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.

  In addition, the Commissioner is of the view that the data controller knew there was a risk that the contravention would occur following the first security breach but failed to take reasonable steps in the intervening period to prevent a further contravention.

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

---

Nature of the contravention

- Two similar security breaches within two months of each other
- Unauthorised confidential and sensitive personal data relating to four vulnerable children was disclosed to unauthorised third parties
- Contravention was serious because of the highly confidential and sensitive nature of the personal data

Effect of the contravention

- Two of the affected data subjects were moved to alternative foster care placements as a result of the second security breach
- Potential for extensive media coverage

Behavioural issues

- Data controller failed to take sufficient remedial action following the first incident to prevent a recurrence

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

- To the Commissioner's knowledge the personal data involved in both security breaches has not been further disseminated

Effect of the contravention

- It is possible that child [redacted]'s [redacted] was aware of some of the information relating to her [redacted] and [redacted]
- Child [redacted] and Child [redacted] and their respective addresses were already known to each other
- Affected data subjects were provided with an apology and offered support
- No adverse effects reported to date

Behavioural issues

- Voluntarily reported to Commissioner's office
- Detailed investigation report compiled after first security breach
- Full remedial action has now 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 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
- The Third Data Protection Principle at Part I of Schedule 1 to the Act was also contravened by the data controller in that inadequate personal data was held on its database

Notice of Intent

A notice of intent was served on the data controller dated 26 January 2012. The Commissioner received written representations from the data controller in a letter dated 17 April 2012. The Commissioner has considered the written and 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 £90,000 (Ninety 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 Tuesday 26 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 Monday 25 June 2012 the Commissioner will reduce the monetary penalty by 20% to £72,000 (Seventy two 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 Monday 25 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 28th day of May 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 Monday 25 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)).