Data Protection Act 1998

Monetary Penalty Notice

Dated: 5 December 2011

Name: Powys County Council

Address: County Hall, Llandrindod Wells, Powys, LD1 5LG

Statutory framework

---

1. Powys County 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 Powys County 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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 4 February 2011, social worker 1 was working on the cases of child B1 and child B2, the daughters of Mrs B. Having finalised her social worker reports [redacted] she printed these out on the printer situated in her room. This printer is also shared with (among others) social worker 2, the social worker for family A. Social worker 1 then collated both reports into one document (the "report") which she photocopied. That same afternoon social worker 2 had been working on the report for child A. This document was also printed off on the shared printer. As social worker 1 was late for an appointment she gave social worker 3 the combined report in relation to child B1 and child B2 which she had put in an envelope

addressed to Mrs B for social worker 3 to deliver it by hand.

5. On 7 February 2011, Mrs B and her mother attended the data controller's offices to meet social workers to discuss her children's cases. Mrs B produced her children's report and informed the data controller that page 8 of a 9-page report relating to child A had been included with it. Further, Mrs B confirmed that she knew the identities of child A and her mother.

7. It is not known exactly how page 8 of child A's 9-page report came to be included in the report addressed to Mrs B. However, the most likely scenario (given that social worker 2 had been working on the report for child A which was also printed off on the shared printer the same afternoon) is that social worker 1 was in a hurry and inadvertently picked up a copy of page 8 of child A's 9-page report from the shared printer which then became mixed up with the report relating to children B1 and B2 before it was photocopied by social worker 1 and put in the envelope for hand delivery. In any event it is clear that no checks were carried out by social worker 1 (or anyone else for that matter) prior to the document being copied, put in an envelope and hand delivered to Mrs B by social worker 3.

8. The data controller has received two formal complaints about this incident, one from Mrs B via her solicitor, and one from Mrs B's mother via her MP. Mr A has apparently also indicated that he is considering legal action against the data controller although the Commissioner understands that a claim has not yet materialised.

9. At the same meeting, Mrs B also reminded the data controller that in the previous year the data controller had sent a [redacted] about an unrelated child X in the same envelope

as a child protection report about her daughter B1. Again, Mrs B knew the families involved [redacted] In the circumstances, Mrs B was not prepared to hand back page 8 of child A's 9-page report at that meeting, although the document has now been recovered from Mrs B's solicitor after some delay. The first security breach was reported to the Commissioner's office by the data controller. Although, in the Commissioner's view, the data disclosed in that case was less likely to cause substantial distress to child X than the information presently under consideration, [redacted] This incident was blamed mainly on the fact that the social workers shared a printer.

10. Following the first security breach the data controller informed the Commissioner's office that further staff training would be carried out and that social workers would be reminded to check work before sending any documents out in the post. Further, it was confirmed that an additional printer would be placed in the social work department, as an attempt to introduce secure printing via activation of the job code function on the existing printers had not been successful for all staff. The data controller was advised by the Commissioner's office that the case would be re-visited if there was a similar security breach again and that a monetary penalty would be considered. It is clear that insufficient steps were taken by the data controller following the first security breach to prevent a recurrence.

11. Following the second security breach an internal investigation was carried out. The investigation report made several recommendations such as developing a peer checking process for envelopes containing confidential or sensitive information in the Children Services department to include written logs of post sent, when, by whom and who checked it, together with mandatory data protection training courses for all staff.

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 it is the data controller.

  In particular the data controller had failed to take appropriate organisational measures against unauthorised processing of personal data, such as a peer checking process for envelopes containing sensitive personal data and appropriate training for all staff. 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 a third party without authorisation due to the inappropriate organisational measures taken by the data controller. The failure to take appropriate organisational measures has the potential to cause substantial distress to data subjects whose confidential and sensitive personal data could be disclosed without authorisation to third parties.

  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 disclosed. There is also potential for damage through misuse of the personal data by the third party even though there is no evidence that, in this case, this actually occurred. This matter is aggravated by the fact that the identities of the data subjects were known to the

unintended recipient who lives in the same locality.

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

  In the circumstances the Children Services department 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 a peer checking process for envelopes containing sensitive personal data and appropriate training for all staff. Further, it should have been obvious to the data controller's staff who were 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.

  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 seven months involving the same recipient
- No checks were undertaken prior to dispatch
- Unauthorised confidential and sensitive personal data was disclosed to a third party
- Identities of the individuals in the disclosed document were known to the recipient on both occasions
- Contravention was very serious because of the highly confidential and sensitive nature of the personal data

Effect of the contravention

- The identities of the data subjects were known to the recipient who lives in the same locality
- The contravention was of a kind likely to cause substantial damage or 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 unauthorised processing of personal data
- Data controller failed to take appropriate 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

Behavioural issues

- Voluntarily reported to Commissioner's office
- Detailed investigation report compiled
- Some remedial action taken following the first incident and further remedial action taken following second security breach
- 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 29 September 2011. The Commissioner received representations from the data controller in a letter from the Head of Legal, Scrutiny and Democratic Services dated 21 October 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 £130,000 (One hundred and thirty 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 5 January 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 4 January 2012 the Commissioner will reduce the monetary penalty by 20% to £104,000 (one hundred and 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 4 January 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 5th day of December 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 4 January 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)).