Data Protection Act 1998

Monetary Penalty Notice

Dated: 10 December 2012

Name: Devon County Council

Address: County Hall, Topsham Road, Exeter, Devon EX2 4QD

Statutory framework

---

1. Devon 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 Devon 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. A social worker who had been employed by the data controller since 1998 prepared an adoption panel report (the "report") using another family's report as a template to remind her of the type of information that should be in the report. The social worker then printed the report and put it in an envelope ready to take to a meeting to give to the service users before an adoption panel meeting. However, the service users forgot to take the envelope with them so the social worker asked them to let her have a postal address so that she could send it by post.

5. The social worker was working at another office when she received a postal address from the service users and she did not have the envelope containing the report with her. The social worker had to give

the report to the service users before the adoption panel meeting so to save time she copied the report that was in the family's adoption folder and sent it to the service users on 12 May 2011 without checking its contents. Unfortunately, the social worker had not shredded the other family's report that she used as a template and had put it back into this family's adoption folder by mistake. Therefore, the social worker had erroneously sent another family's report to the service users.

6. The report contained confidential and highly sensitive personal data relating to approximately 22 data subjects. The report was about the child of a [redacted] couple who was being considered for adoption and included information about the couple's immediate and extended family such as their ethnic origin and religion, mental and physical health, details about [redacted] together with the alleged commission of criminal offences.

7. The data controller had overarching policies on data protection and personal information security, but the data controller couldn't demonstrate that the social worker had read the policies and, in any event, there was no specific guidance on the handling or posting of sensitive information. Although data protection training materials were available on the intranet, the Commissioner understands that this training was not mandatory and the social worker had not undertaken any of the data controller's specific information governance training packages.

8. Following the security breach, the data controller took immediate steps to recover the report but the unintended recipients did not give it to the police until 25 July 2011, just before the data controller was due to obtain an order from the court. The data controller also informed the affected individuals. An investigation was carried out which recommended (among other things) that the "personal information security policy" should include guidance on the handling and posting of sensitive information; that specific information security training should be given to staff involved in this security breach. The Commissioner understands that the data controller is now taking steps to implement these recommendations.

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 organisational measures against unauthorised processing of personal data, such as a peer checking process for envelopes containing confidential and sensitive personal data and/or having appropriate policies, procedures and training for staff working in the data controller's People Services department.

  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 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 has been disclosed to unauthorised third parties who had 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 unauthorised third parties and that their data may have been further disseminated and possibly misused, even if those

concerns do not actually materialise.

This matter is aggravated by the fact that the report was erroneously sent to unauthorised third parties who [redacted]

In this context it is important to bear in mind that many of the affected individuals were considered to be vulnerable.

- 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 data controller's People 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 on a daily basis.

  The Commissioner's office has also received three previous self-reported security breaches resulting in the data controller being given advice in 2010 that appropriate procedures should be in place to protect personal data.

  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 a peer checking process for envelopes containing confidential and sensitive personal data and/or having appropriate policies, procedures and training for staff working in the People Services department.

  Further, it should have been obvious to the data controller whose staff were social workers 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.

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

---

Nature of the contravention

- Confidential and sensitive personal data relating to approximately 22 data subjects (many of whom were vulnerable) was disclosed to unauthorised third parties
- Contravention was particularly serious because of the confidential and sensitive nature of the personal data

Effect of the contravention

- The report was erroneously sent to unauthorised third parties who [redacted]
- The parents of the child who was being considered for adoption complained to the Commissioner's office about the distress they had suffered
- The unauthorised third parties did not return the report for a period of over two months

Behavioural issues

- Three previous self-reported security breaches with compliance advice given to the data controller in 2010
- Data controller placed an over-reliance on the social worker's professional training

Impact on the data controller

- Data controller is a public authority so liability to pay a monetary penalty does not fall on an individual
- 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

---

Effect of the contravention

- Data controller informed the affected individuals about the security breach
- The report has not been further disseminated as far as the Commissioner is aware

Behavioural issues

- Voluntarily reported to the Commissioner's office
- Data controller took immediate steps to recover the report

- Detailed investigation report compiled
- Some remedial action has now been taken
- Fully co-operative 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 this security breach

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 4 October 2012. The Commissioner received representations from the data controller in a letter from the County Solicitor & Monitoring Officer dated 1 November 2012. 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 £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 11 January 2013 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 10 January 2013 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 10 January 2013 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 10th day of December 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 10 January 2013 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)).