Data Protection Act 1998

Monetary Penalty Notice

Dated: 22 November 2010

Name: Hertfordshire County Council

Address: Room 203, County Hall, Pegs Lane, Hertford, Hertfordshire SG13 8DE

Statutory framework

---

1. Hertfordshire 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 on by Hertfordshire 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 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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 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 11 June 2010 a member of staff working in the data controller's Childcare Litigation Unit sent 17 pages which contained confidential and sensitive personal data relating to seven individuals by fax to an unintended number belonging to a member of the public. The documents related to a sexual abuse case involving a child which was being heard at the High Court. The intended address for the faxed documents was a Barristers' Chambers in London ("Chambers") who were instructed to act on behalf of the data controller in the High Court

proceedings. The fax machine in the Childcare Litigation Unit had the fax number for Chambers programmed into its memory and had an 'auto dial' button. Having used the 'auto dial' button in accordance with the standard practice and found the line to be busy, the member of staff then dialled the full number into the fax machine and sent the fax. The member of staff had input the wrong STD code for Chambers and also failed to use a fax header sheet which would have provided an unintended recipient with details of the sender and instructions on what to do with a misdirected fax.

5. The member of the public who received the fax claims that this also happened earlier the same day although the data controller has no record of this and no evidence has been produced by the member of the public to support his claim. This member of the public immediately emailed the data controller to make them aware of the error. Until then the data controller was unaware of the error because their procedures did not cover this eventuality. Subsequently both the data controller and the member of the public reported the security breach to the Commissioner's office. Due to the confidential and sensitive nature of the data the data controller also obtained a High Court injunction (still in force) prohibiting the member of the public from disclosing any information about the sexual abuse case so as not to prejudice the High Court hearing and ordering him to destroy the data.

6. While it was recognised that the circumstances of the security breach and hence the possibility of a monetary penalty could not be fully investigated at that time due to the High Court injunction and the ongoing sexual abuse case, the Commissioner's office was so concerned about the security breach that two members of staff from the Enforcement team attended the data controller's premises on 24 June 2010 to evaluate its response to the incident and advise on any remedial action that should be taken.

7. The data controller was co-operative and receptive to a meeting with the Commissioner's staff with a view to obtaining their advice and assistance. The Commissioner's staff met with senior managers namely the Director of Strategy and Partnerships, Chief Legal Officer, Assistant Chief Legal Officer, Information Governance Manager and Data Protection Manager. The Chief Executive, Leader of the Council, Director of Children Schools and Families and relevant Council members were also kept informed. It was clear that the data controller was aware of the seriousness of the situation and had diverted resources to address the security breach.

8. Following the incident on 11 June 2010 the data controller began an immediate investigation resulting in an interim report which was

produced at the meeting on 24 June 2010. It was noted that the following remedial action had been taken. The Information Governance Unit informed the Commissioner's office of the security breach; all support staff in Legal Services were reminded of the requirement to use a fax header sheet which includes instructions on appropriate action for unintended recipients; an instruction was issued by the Chief Legal Officer that no confidential documents should be transmitted by fax without first having been sanctioned by the Assistant Chief Legal Officer or Consultant Solicitor (Practice and Quality Assurance); all staff in Legal Services were instructed to use password protected/encrypted mail as the default option for transmitting confidential data. Finally, the Information Governance Unit was required to undertake a full investigation.

9. The Commissioner's staff were of the view that the action taken so far to prevent and detect further breaches was insufficient. They informed the data controller's staff that the security breach could "happen again tomorrow". Although the Childcare Litigation Unit did have a protocol in place whereby its fax machine had pre-programmed approved fax numbers and staff using the fax machine were aware that the pre-programmed numbers should be used, this procedure was not sufficiently robust. In particular there was no evidence of appropriate organisational measures being taken, such as a procedure that required phoning ahead or the recipient to immediately confirm receipt of a fax (known as "ring ahead"). The data controller's staff explained that the work to address the security breach was still in progress but that it was important to understand the remedial work they had undertaken to date. The Commissioner's staff detected a reluctance to implement a ring ahead system but acknowledged the action taken so far and it was agreed that following the meeting the Commissioner's office would consider the interim report into the incident and make appropriate recommendations.

10. On 24 June 2010 (the same date as the meeting with the Commissioner's staff) another member of staff in the data controller's Childcare Litigation Unit sent 11 pages containing confidential and sensitive personal data by fax to an unintended number belonging to Chambers. The intended recipient for the faxed documents this time was the Court Manager at Watford County Court. Chambers were not instructed in this particular case so there was no reason to send the documents to them. As a fax header sheet had been used on this occasion as a result of the tightening of procedures referred to in paragraph 8 above, Counsel's clerk informed the data controller of its error. The data controller understands that Counsel's clerk destroyed the documents without examining the information.

11. An investigation by the data controller revealed that the number dialled on the fax machine had again been input manually rather than using the 'auto dial' facility in accordance with the standard practice. The disclosed documents contained confidential and sensitive personal data relating to a total of 18 data subjects. The information related to three children who were the subject of the care proceedings and identified by their name and date of birth (an address was included for one of the children); care arrangements for the children; six adults who were identified by their name and familial relationship; the date of birth, address and previous convictions of two of the data subjects; records of domestic violence and the opinions of care professionals such as social workers and police about data subjects' interaction with social services and the police, data subjects' ability to care for children and information relating to data subjects' personal relationships. On the instruction of the Director of Strategy & Partnerships a moratorium was placed on the sending of any faxes until a secure procedure was in place. This took effect from 2pm on Friday 25 June 2010 and was lifted on Monday 28 June 2010 once a secure fax system had been implemented.

12. The data controller has now taken further remedial action which includes the introduction of a fax usage policy for Legal Services which took effect from 28 June 2010; the implementation in Legal Services of a "phone ahead" and "confirmation of receipt of fax" process; the nomination in Legal Services of officers authorised to send faxes via a clearance/sign off process through qualified lawyers; establishing a record of faxes sent/confirmation received in Legal Services. In addition an audit of preset fax numbers used by Legal Services was undertaken by the data controller's Internal Audit team and the data controller's Business Improvement Team were asked to work with Legal Services on implementation of secure email/electronic communication facilities across Legal Services. Finally, a further report into these security breaches dated 6 August 2010 was produced by the data controller and sent to the Commissioner's office.

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 had failed to take appropriate organisational measures against unauthorised processing of personal data such as a "phone ahead" and "confirmation of receipt of fax" process. 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 damage or substantial distress. Unauthorised confidential and sensitive personal data was disclosed to 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 damage and/or substantial distress to data subjects whose unauthorised confidential and sensitive personal data could be disclosed to third parties.

  In this particular case the data subjects would suffer from substantial distress knowing that their confidential and sensitive personal data has in fact been disclosed to third parties and that their data may be further disclosed even if those concerns do not actually materialise. If it is further disclosed and obtained by less trustworthy third parties, then it is likely that the contravention would also cause substantial damage to the data subjects such as damage to reputation. Further, the contravention could have prejudiced the High Court hearing of the sexual abuse case which would have caused substantial distress to the data subject concerned.

- The Commissioner is satisfied that section 55A (3) of the Act applies in that the data controller 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 Childcare Litigation Unit was used to dealing with such cases and would have been aware of the confidential and sensitive nature of the personal data they were sending by fax which would produce an unencrypted paper copy of the data at the destination address.

  In the circumstances the Childcare Litigation Unit 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 an alternative more secure system of transmission than the use of fax or at the very least having a "phone ahead" and "confirmation of receipt of fax" process in place. The risks of using simple fax facilities are self evident and, in the Commissioner's view, widely known. Further it should have been obvious to the data controller's staff who were routinely involved in childcare litigation 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 complete sufficient remedial measures 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 weeks
- Recipient of first fax claims this has happened before
- Unauthorised confidential and sensitive personal data was disclosed to third parties
- Contravention was very serious because of the highly confidential and sensitive nature of the personal data which included, amongst other things, details of child sexual abuse/prospective care proceedings/previous convictions/domestic violence records

Effect of the contravention

- The contravention was of a kind likely to cause substantial damage and substantial distress to the data subjects
- Potential for media coverage relating to these security breaches to cause the data subject's further distress
- Potential to disrupt ongoing legal case and interfere with the administration of justice

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
- Lack of immediate and effective remedial action following the first incident
- Apparent reluctance of senior managers to accept potential for reoccurrence when alerted by Commissioner's staff

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
- No evidence to support claim by recipient of first fax that this has happened before and the data controller has no record of it
- Personal data related to only 18 data subjects in the second incident and 29 data subjects in the first incident
- To the Commissioner's knowledge the personal data involved in both security breaches has not been further disseminated

Effect of the contravention

- An injunction was obtained by the data controller to prevent the member of the public from disclosing the personal data involved in the first security breach and ordering him to destroy the data

Behavioural issues

- Voluntarily reported to Commissioner's office
- Detailed investigative reports were compiled
- Further remedial action taken following second security breach
- Insufficient time to consider the points raised by the Commissioner's staff prior to the second security breach
- Substantial remedial action has been taken
- Now fully cooperative with Commissioner's office and will consent to an audit if necessary

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 sending of confidential and sensitive personal data by fax and to ensure either that alternative more secure means are used or that, at a minimum, appropriate and effective security measures are applied to the use of fax
- This will be one of the first monetary penalty notices issued by the Commissioner and is likely to set a precedent by which future notices will be judged

Notice of Intent

A Notice of Intent was served on the data controller dated 28 September 2010. The Commissioner received representations from the data controller by letter dated 18 October 2010. 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 has taken full account of the representations made by the data controller and considers that the contravention of section 4(4) of the Act is very serious and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of £100,000 (One hundred thousand pounds) is a 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 22 December 2010 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 21 December 2010 the Commissioner will reduce the monetary penalty by 20% to £80,000 (eighty thousand pounds).

Right of Appeal

There is a right of appeal to the (First-tier Tribunal) General Regulatory Chamber against:

(i) the imposition of the monetary penalty

and/or;

(ii) the amount of the penalty specified in the monetary penalty notice.

Any Notice of Appeal should be served on the Tribunal by 5pm on 21 December 2010 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 22nd day of November 2010

Signed: ……..

Christopher Graham
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 21 December 2010 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)).