Data Protection Act 1998

Monetary Penalty Notice

Dated: 23 October 2012

Name: Stoke-on-Trent City Council

Address: **Civic Centre, Glebe Street, Stoke-on-Trent ST4 1HH**

Statutory framework

---

1. Stoke-on-Trent 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 Stoke-on-Trent 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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)(Maximum Penalty 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 14 December 2011, a Solicitor employed by the data controller was working on a child protection case and sent 11 emails (intended for Counsel instructed on the case) to the wrong email address by mistake. The emails varied in sensitivity but some of them contained confidential and highly sensitive personal data about the non-accidental injuries sustained by a child together with medical information relating to two adults and two children. The emails also contained the Brief to Counsel, suggested directions and miscellaneous comments about the conduct of the case.

5. The Solicitor had just been provided with a new computer by the data controller's IT department which meant that her stored email

addresses were no longer accessible. She therefore copied from the paper file Counsel's internet email address that he used for work, but made two crucial errors which she then repeated when typing the email address. The Solicitor realised her mistake the following day when she spoke to Counsel who confirmed that he had not received any emails from her on 14 December 2011. The service provider has since confirmed that the email address to which the emails were erroneously sent was a live internet email account.

6. The Commissioner understands that the Solicitor was acting in breach of the data controller's email and information protection policies (among others) because the emails should either have been sent via the GCSx secure network or encrypted. The email should also have been protectively marked. However, the Solicitor was not disciplined because the data controller was aware that the legal department did not have access to encryption software and frequently had to send emails outside the secure network in order to carry out their work. Further, the data controller has accepted that the policy on information protection in particular was not widely known to staff and that no relevant training had been provided.

7. Following the security breach, the data controller sent a further email to the incorrect address, apologising for the error and asking the unintended recipient to confirm deletion of the emails. However, the data controller has not received any response from the unintended recipient and has been unable to get any further information from the service provider about the email account. The Judge who was presiding over the child protection proceedings and the clinical staff whose reports had been compromised were informed about the security breach. Fortunately, the security breach did not have any effect on the court proceedings.

8. The data controller has also taken some remedial action which includes introducing e-learning data protection training for staff, ensuring that all emails containing sensitive personal data are password protected and in the longer term implementing a secure portal for emails.

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 providing its employees with appropriate information protection training and ensuring that a secure means of sending emails containing sensitive personal data was available such as GCSx or alternatively that emails could be encrypted. 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 highly sensitive personal data relating to four individuals was unintentionally disclosed to an unauthorised recipient 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 individuals who may know or suspect that their confidential and highly sensitive personal data has been disclosed to a recipient who has no right to see that information.

  Furthermore they would be justifiably concerned 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 two of the affected individuals are considered to be vulnerable children.

- 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 Solicitors working in the legal department were used to handling confidential and sensitive personal data and the data controller was aware that they did not have access to encryption software and frequently had to send emails outside the secure network in order to carry out their work.

  In the circumstances, the data controller should have realised the potential for human error in typing in the wrong email address when sending unencrypted emails containing confidential and sensitive personal data, particularly when the Solicitor no longer had access to her stored email addresses and had not been provided with any information protection training.

  In addition, the data controller signed an undertaking with the Commissioner's office in 2010 following the loss of an unencrypted USB stick holding sensitive personal data. This should have raised the data controller's awareness about the importance of having appropriate security measures in place.

  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 providing its employees with appropriate information protection training and ensuring that a secure means of sending emails containing sensitive personal data was available, such as GCSx, or alternatively that emails could be encrypted.

  The risk of email addresses being wrongly typed is self-evident and, in the Commissioner's view, widely known. Further it should have been obvious to the data controller whose Solicitors were used to handling confidential and sensitive personal data relating to vulnerable individuals 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

- Contravention was particularly serious because of the confidential and highly sensitive nature of the personal data
- Two of the data subjects were vulnerable children
- Data controller was aware that sensitive personal data was routinely being sent outside secure networks by unencrypted email

Effect of the contravention

- 11 emails containing confidential and highly sensitive personal data were sent to a live email address via the internet and have not been recovered

Behavioural issues

- Lack of appropriate information protection training
- Previous security breach in 2010 should have raised the data controller's awareness

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

---

Effect of the contravention

- To the Commissioner's knowledge the personal data involved has not been accessed or further disseminated
- Security breach did not affect the child protection proceedings

Behavioural issues

- Voluntarily reported to Commissioner's office
- 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 sending of confidential and sensitive personal data by unencrypted email and to ensure either that more secure means are used or that, at a minimum, appropriate and effective security measures are applied to the use of email

Notice of Intent

A notice of intent was served on the data controller dated 13 September 2012. The Commissioner has not received any representations from the data controller in response to the notice of intent. In the circumstances, the Commissioner has now 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 very serious and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of £120,000 (One hundred and twenty 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 26 November 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 23 November 2012 the Commissioner will reduce the monetary penalty by 20% to £96,000 (Ninety six 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 23 November 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 23rd day of October 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 23 November 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)).