Data Protection Act 1998

Monetary Penalty Notice

Dated: 6 June 2011

Name: Surrey County Council

Address: **County Hall, Penrhyn Road, Kingston upon Thames, Surrey KT1 2DN**

Statutory framework

---

1. Surrey 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 Surrey 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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)(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. One of the data controller's Adult Social Care Teams received an email asking its Managers and Assistant Team Managers to urgently populate an Excel spreadsheet with information about the adult social care service users including their names; type of accommodation; support needs; days of attendance at the Day Service Centre and means of transport. Sensitive personal data about the complex needs of the adult social care service users was also to be added to the spreadsheet including an indication of their wheelchair use; autistic spectrum; mental health; downs syndrome; dementia; epilepsy; hearing impairment; visual impairment impacting on daily life; physical

disabilities affecting mobility; challenging behaviour; increasing health considerations and behaviour that makes them vulnerable.

5. One of the data controller's employees carrying out this task was deputising for another member of her Team as she had done on several occasions in the past. Although the employee was fully aware of the confidential and sensitive nature of the information she was inputting, was conversant with the Lotus Notes application in use at the time and had received advice and support from a colleague, she had limited experience of computers, had not attended all appropriate IT training and was unfamiliar with Excel. She therefore expressed concern that she was uncomfortable with the task she had been asked to carry out by the data controller.

6. On 17 May 2010, whilst returning the now populated Excel spreadsheet relating to 241 adult social care service users to an internal colleague, the employee erroneously copied the email to "Transport-ETRANS Addresses" which is a global email distribution list owned by the data controller's Transport Co-ordination Centre. The email distribution list consisted of contacts in 361 transportation companies comprising both taxi hire and mini cab firms and some coach and mini bus hire services, although the Commissioner understands that some of those email addresses were internal and some were invalid. The email and attached Excel spreadsheet could be accessed by individuals within the transportation companies although it was protectively marked and the sensitivity of the contents was clear from the face of the email.

7. Following the security breach an attempt to recall the email and attached Excel spreadsheet failed because it had been delivered to servers outside the data controller's network. The data controller also attempted to prevent further dissemination of the information by emailing a retraction letter to the transportation companies asking them to delete the email and attached Excel spreadsheet. 213 of the transportation companies deleted the information, or did not receive it in the first instance because the email address was not valid. Two follow up letters were sent to the transportation companies although it is not possible to determine whether all copies of the email and attached Excel spreadsheet have now been deleted. The data controller notified the individuals affected (or their representatives) about the security breach. The data controller explained that the information formed part of a larger spreadsheet which was reduced to the minimum necessary to complete the task. Finally, the data controller reported this security breach to the Commissioner.

8. Within days of the security breach a "Safeguarding Adults Action Plan" was drafted setting out 16 action points including a reminder to Team Managers about providing IT training and guidance to employees. A

more detailed investigation into the security breach was carried out resulting in a report dated 6 September 2010 which recommended, amongst other things, that a training needs analysis should be conducted for frontline officers in line with their regular activities and that any training needs gaps should be rectified through staff development. Further, that where the work activities of employees are not included on their job description, these documents should be amended accordingly. It was also recommended that a naming convention for global email distribution lists that cannot easily be mistaken should be established and that all current lists should be transferred to this convention. A technical solution was also to be investigated that would warn a member of staff when an email or document marked Protected or Restricted is about to be sent to an external email address. The data controller also carried out an audit of email security in November 2010 which recommended, amongst other things, that to ensure the safe transfer of sensitive information an email should be encrypted if appropriate. The Commissioner understands that the majority of the recommendations referred to above were implemented by the data controller by 8 February 2011.

9. In the meantime a second security breach occurred on 22 June 2010 when one of the data controller's employees erroneously emailed the Minutes of a Strategy Discussion containing confidential personal data to a newsletter distribution group entitled "Newsletter Contacts". This address group contained, amongst others, the email addresses of 124 unintended external recipients. A third security breach occurred on 21 January 2011 when a locum Family Support Worker in the data controller's Children's Services erroneously sent a "NHS Continuing Healthcare Checklist" form and a "County Transition Team Referral Form" to an internal email contact group titled "CHC mailing list" which was an internal email group based at County Hall instead of the Transition Team as requested. The Commissioner understands that both documents contained confidential sensitive personal data. Further remedial action specific to both of these security breaches was taken by the data controller and the third security breach was reported 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 technical and organisational measures against unauthorised processing of personal data such as providing its employees with appropriate IT training and support, establishing naming conventions for group email distribution lists that cannot easily be mistaken by its employees and considering a more secure means of transmission such as encrypting any emails that contain sensitive personal data. 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. Unauthorised confidential and sensitive personal data relating to 241 individuals was unintentionally disclosed to 361 transportation companies (although some of those email addresses were internal and some were invalid) 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 would know or suspect that their confidential sensitive personal data has been disclosed to a large number of people that have no right to know that information. Furthermore they would be justifiably concerned that their data may be further disclosed and possibly misused even if those concerns do not actually materialise. In this context it is important to bear in mind that many of the affected individuals are considered to be vulnerable.

- 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 distress, but failed to take reasonable steps to prevent the contravention.

  The Commissioner has taken this view because employees working in the data controller's Adult Social Care Teams were used to dealing with confidential sensitive personal data and should have realised the potential for human error in wrongly selecting drop down boxes when sending emails containing sensitive personal data, particularly when an employee is not working in their normal role or environment and has had limited IT training and support.

  In the circumstances, the data controller 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 IT training and support, establishing naming conventions for group email distribution lists that cannot easily be mistaken by its employees and considering a more secure means of transmission such as encrypting any emails that contain sensitive personal data. The risks of drop down boxes being wrongly selected are self evident and, in the Commissioner's view, widely known. Further it should have been obvious to the data controller who was routinely involved in dealing with vulnerable individuals who required day care 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

- Two similar security breaches
- Unauthorised confidential and sensitive personal data relating to 241 individuals was unintentionally disclosed to 361 transportation companies
- Personal data and sensitive personal data relating to 241 individuals could still be available to third parties
- Contravention was serious because of the confidential and sensitive nature of the personal data

Effect of the contravention

- The contravention was of a kind likely to cause substantial distress to the data subjects

Behavioural issues

- Lack of appropriate IT training and support
- Whilst some early remedial was action taken it was insufficient to prevent two similar security breaches
- Contravention was due to the negligent behaviour of the data controller in failing to take appropriate technical and organisational measures against the unauthorised processing of personal data

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 the security breach has not been further disseminated

Effect of the contravention

- Email and attachment was protectively marked and the sensitivity of the contents was clear from the face of the email
- Information contained in the spreadsheet was reduced to the minimum necessary to complete the task
- Several attempts were made to prevent further dissemination of the email and attachment
- 213 of the transportation companies have now confirmed that they either deleted the information or did not receive the email

Behavioural issues

- Appropriate training in the use of Lotus Notes email system had been provided
- A failed attempt was made to recall the email and attachment
- Voluntarily reported to Commissioner's office
- Detailed investigation reports were compiled

- Individuals affected (or their representatives) were notified about the security breach.
- Substantial remedial action has 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 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

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 £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 5 July 2011 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 July 2011 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 4 July 2011 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 6th day of June 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 July 2011 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)).