**Data Protection Act 1998**

**Monetary Penalty Notice**

**Dated: 10 September 2012**

**Name: Scottish Borders Council**

**Address: Council Headquarters, Newtown St. Boswells, Melrose TD6 0SA**

## Statutory framework

1. Scottish Borders 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 Scottish Borders 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. Since 2005, GS (the "data processor") had been digitising the pension records of the data controller's past employees and former members of the pension scheme on behalf of the data controller's pension team. The Commissioner understands that there was no contract in place between the data controller and the data processor to carry out this work although GS had previously been engaged by other Council departments to undertake miscellaneous scanning work.

5. On 10 September 2011, a member of the public noticed that a paper recycling bank had been overfilled with discarded files. On closer inspection it was clear that some of the files contained personal data so they handed them into the police. The police attended the scene and removed any files that were easily retrievable before later returning them to the data controller. The remaining contents of the paper recycling bank were secured and then moved to a protected area designated by the data controller.

6. The Commissioner understands that eight boxes containing 676 files had been deposited in the paper recycling bank by the data processor on 10 September 2011. He had also deposited two other boxes containing 172 files in a different paper recycling bank on the same day. The files contained confidential personal data including the name, address, national insurance number and date of birth of past employees and former members of the pension scheme and (where applicable) their spouse. The files also contained salary and bank account details in approximately 43% of the cases. The 676 files were recovered, cross checked against the digitised images, and later securely destroyed. The other 172 files are likely to have been recycled following a completely mechanical process.

7. Prior to the security breach, the data processor had digitised an estimated 8000 pension records which would also have included details of ill health benefits in a small number of cases. The data processor would normally collect the files from the data controller in three year cycles and then scan the documents at his place of business to make digital files. He would place the files on unencrypted discs, which he would then return to the data controller using standard post. However, the data controller was not aware that the data processor had been depositing the original documents in paper recycling banks over a potential seven year period.

8. The data controller terminated the arrangement with the data processor as soon as the security breach was discovered and its pension records are not being digitised at the present time.

**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 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".*

Paragraph 11 at Part II of Schedule 1 to the Act provides that:

*"Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle-*

*(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and*

*(b) take reasonable steps to ensure compliance with those measures.*

Paragraph 12 at Part II of Schedule 1 to the Act further provides that:

*"Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless-*

*(a) the processing is carried out under a contract-*

*(i) which is made or evidenced in writing, and*

*(ii) under which the data processor is to act only on instructions from the data controller, and*

*(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.*

- The Commissioner is satisfied that there has been a serious contravention of section 4(4) of the Act.

In particular, the data controller failed to choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and take reasonable steps to ensure compliance with those measures. Such security measures might have provided for the secure disposal of the files after scanning and stipulated that the data processor would either return the documents to the data controller in person, or securely destroy them, providing the data controller with a certificate of destruction.

The data controller should also have put in place regular monitoring to ensure compliance with these and other measures.

Further, the processing was not carried out under a contract between the data controller and the data processor under which the data processor was to act only on instructions from the data controller, and which required the data processor to comply with obligations equivalent to those imposed on a data controller by the Seventh Data Protection Principle.

The Commissioner considers that the contravention is serious because the data controller failed to comply with the requirements set out in paragraphs 11 and 12 in Part II of Schedule 1 to the Act.

Consequently, the data controller failed to ensure a level of security appropriate to the harm that might result from the accidental loss of the documents and the nature of the data to be protected.

- The Commissioner is satisfied that the contravention was of a kind likely to cause substantial damage or substantial distress to data subjects whose confidential personal data (including financial information) was seen by a member of the public who had no right to see that information.

  Further, the data subjects would be justifiably concerned that their data may have been further disseminated even if those concerns do not actually materialise. If the data has been disclosed to untrustworthy third parties then it is likely that the contravention would cause further distress and also substantial damage to the data subjects such as exposing them to identity fraud and possible financial loss.

- 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 the view that the data controller knew or ought to have known that there was a risk that the contravention would occur because a large amount of confidential personal data (including financial information) relating to the data controller's past employees and former members of the pension scheme was contained in the files. The data controller was used to dealing with such information on a daily basis and as such had its own pension team.

The data controller did not take steps to establish whether the data processor offered secure destruction facilities, and did not provide any instruction on what should happen to the documents after they had been scanned. The data processor also sent an email to the data controller in March 2010 raising the possibility of either destroying the documents or returning them to the data controller after scanning, but received no response.

Further, this was a long term arrangement which involved the digitisation of approximately 9000 pension records since 2005. These records contained a large amount of confidential personal data (including details of ill health benefits in a small number of cases and financial information) and should therefore have been afforded the highest level of security. It should have been obvious to the data controller 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 the circumstances, the data controller failed to take reasonable steps to prevent the contravention, such as complying with the "data processor" requirements of the Seventh Data Protection Principle which if properly complied with should have alerted the data controller to the fact that there was no provision for the secure disposal of the files after scanning. The data controller could then have taken steps to ensure that the documents were either returned to the data controller in person after they had been scanned, or securely destroyed, and that the data controller was provided with a certificate of destruction. The data controller could also have put in place regular monitoring to ensure compliance with these and other measures.

**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 nature of the confidential personal data
- Contravention had occurred since 2005
- Data processor was free to have disposed of the documents in an even less secure manner

*Effect of the contravention*

- Contravention affected a maximum of 848 individuals although another 8000 pension records were potentially at risk
- Contravention could result in identity fraud and possible financial loss

*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*

- As far as the Commissioner is aware the security breach was contained

*Effect of the contravention*

- 676 files were recovered, cross checked against the digitised images, and later securely destroyed. The other 172 files are likely to have been recycled following a completely mechanical process
- Risk of access was relatively low unless a paper recycling bank had been overfilled
- No adverse effects have been reported to date

*Behavioural issues*

- Voluntarily reported to ICO
- Detailed investigation report compiled
- Some remedial action has now been taken
- Fully cooperative with ICO

*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 and this is an opportunity to reinforce the need for data controllers to ensure that appropriate and effective security measures are applied to hard copy personal data held in files.

**Notice of Intent**

A notice of intent was served on the data controller dated 2 August 2012. The Commissioner received written representations from the data controller's Chief Executive in a letter dated 15 August 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 very serious and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of £250,000 (Two hundred and fifty 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 12 October 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 11 October 2012 the Commissioner will reduce the monetary penalty by 20% to £200,000 (Two hundred 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 11 October 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 10th day of September 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 11 October 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)).