Data Protection Act 1998

Monetary Penalty Notice

Dated: 20 August 2014

Name: Ministry of Justice

Address: 102, Petty France, London SW1H 9AJ

Statutory framework

1. The National Offender Management Service ("NOMS") is an Executive Agency of the Ministry of Justice. NOMS has responsibility for commissioning and delivering Prison and Probation Services across England and Wales. The Ministry of Justice 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 Ministry of Justice, including its executive agencies, 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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

Section 55A of the Act provides that:

(1) 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 24 May 2013, a portable hard drive stored in a prison's Security Department and used to back up the prisoner intelligence database, was discovered to be missing. The hard drive had last been used on 18 May 2013 for the weekly back up but had not been locked up afterwards in the fireproof safe, as required. The hard drive had not

been password protected and was unencrypted for the reasons explained in paragraph 8 below.

5. The Commissioner understands that access to the area where the hard drive was used and stored was limited to nine staff from the Security Department and controlled by a keypad system. However, the main door of the Security Department could be opened by any of the prison staff, all of whom had been security vetted.

6. The information on the hard drive related to 2,935 prisoners and included confidential and highly sensitive personal data such as their name, date of birth, length of sentence, offence(s), physical description including details of any tattoos or other distinguishing marks, intelligence information such as links to other prisoners or organised crime, involvement with drug use, prison discipline, establishment location and some victim and/or visitor details.

7. In October 2011, a virtually identical security breach occurred at another prison involving intelligence information relating to approximately 16,000 prisoners. Following that security breach, the Commissioner's office was informed that remedial action had been taken including the distribution of encrypted hard drives to 75 prisons that had also been using unencrypted portable hard drives to back up prisoner intelligence information.

8. Although the new drives were installed by the IT provider in May 2012, NOMS did not realise that the encryption software required manual activation and failed to instruct the IT provider to check that the encryption software was working when carrying out a review in September 2012. Therefore, prisoner intelligence information was being held on portable unencrypted devices supplied by NOMS in 75 prisons for a period of at least 12 months.

9. Following the second security breach, the encryption software for the remaining hard drives was activated or upgraded and a new intelligence system has now been implemented in all of the prisons thereby removing the need for manual backup.

10. Despite an extensive search of the Security Department building and the prison grounds by six members of staff over a two day period, the hard drive was not recovered. However, there is no evidence that any of the information held on this hard drive has been disseminated 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 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".

In deciding to issue this monetary penalty notice, the Commissioner has considered the facts of the case and the deliberations of those within his office who have recommended this course of action. In particular, he has considered whether the criteria for the imposition of a monetary penalty have been met; whether, given the particular circumstances of this case and the underlying objective in imposing a monetary penalty, the imposition of such a penalty is justified, and whether the amount of the proposed penalty is proportionate.

- 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 particular, the data controller has failed to take appropriate technical measures against unauthorised processing and accidental loss of personal data such as taking steps to ensure that the portable hard drives that were used to back up the prisoner intelligence database in 75 prisons had been encrypted.

  The Commissioner considers that the contravention is particularly serious because the data controller failed to take effective remedial action following a virtually identical security breach in October 2011. This resulted in prisoner intelligence information in 75 prisons being

held on the unencrypted devices supplied by NOMS for a period of at least 12 months prior to this second security breach. This is unacceptable in view of the nature of the information held on the portable hard drives which should have been afforded the highest levels of security.

- The Commissioner is satisfied that the contravention is of a kind likely to cause substantial damage and/or substantial distress to the data subjects.

  The remedial action taken by the data controller in October 2011 was ineffective resulting in 75 prisons holding confidential and highly sensitive personal data on unencrypted devices for a period of at least 12 months. It is fortunate that none of these devices have been lost and/or accessed by unauthorised third parties as far as the Commissioner is aware.

  However, the contravention was still "of a kind" likely to cause substantial damage and/or substantial distress to the data subjects. This scale of this contravention posed a significant risk of causing serious detriment to thousands of prisoner's in England and Wales.

  In this particular case, the data subjects would be likely to suffer from substantial distress knowing that their confidential and sensitive personal data may be accessed by unauthorised third parties even though, as far as the Commissioner is aware, those concerns have not so far materialised. This is aggravated by the fact that the hard drive has still not been recovered.

  If the data has in fact been accessed by untrustworthy third parties then it is likely that the contravention would cause further distress and substantial damage to the data subjects such as exposing them to physical harm.

- 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 and/or substantial distress, but it failed to take reasonable steps to prevent the contravention.

  The Commissioner has taken this view because the prisoner intelligence database was backed up onto a portable hard drive on a weekly basis. The data controller was aware that prisons across the entire estate were backing up this information on a weekly basis pending the implementation of a new intelligence system.

As a result of a virtually identical security breach in October 2011, the data controller was also aware that the portable hard drives used to back up this intelligence information in 75 prisons were unencrypted. As a result, the data controller made the decision to distribute 75 encrypted hard drives to those prisons, albeit the remedial action taken was completely ineffective.

In the circumstances, the data controller knew that there was a risk that the contravention would occur unless reasonable steps were taken to prevent the contravention, such as taking steps to ensure that the portable hard drives used to back up the prisoner intelligence database in 75 prisons had been encrypted.

As the data controller routinely handles sensitive personal data relating to prisoners it should have been obvious that such a contravention would be of a kind likely to cause substantial damage and/or substantial distress to the data subjects due to the nature of the data involved. It is possible that an unauthorised third party could still access this data and may have already done so.

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

Behavioural issues

- The data controller failed to take effective remedial action following a virtually identical security breach in October 2011

Impact on the data controller

- The data controller has sufficient financial resources to pay a monetary penalty up to the maximum without it 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, none of the personal data involved in this security breach has been disseminated
- The unencrypted hard drive should have been stored in a fireproof safe

Behavioural issues

- The data controller attempted to take remedial action following a virtually identical security breach in October 2011 albeit that this action was ineffective
- The data controller has recently implemented a new intelligence system across the entire prison estate which has eliminated the need for the weekly back up
- The breach was self-reported and data controller has been co-operative with Commissioner's investigation

Impact on the data controller

- There is likely to be a significant impact on the reputation of the data controller as a result of this security breach
- The liability to pay the monetary penalty will fall on the public purse although the penalty will be paid into the Consolidated Fund

Other considerations

- The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the Act

- The data controller holds responsibility within Government for Government policy on data protection matters and could therefore be expected to be a model of best practice and exemplary in respect of data protection compliance

Notice of Intent

A notice of intent was served on the data controller dated 26 June 2014.

The Commissioner received written representations from the data controller in in a letter from the Permanent Secretary dated 22 July 2014. 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:

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 the seventh data protection principle is **very serious** and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of **£180,000** (One hundred and eighty thousand pounds) is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

In reaching this decision, the Commissioner considered other cases of a similar nature in which a monetary penalty had been imposed, and the facts and aggravating and mitigating features referred to above.

Payment

The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 22 September 2014 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

19 September 2014 the Commissioner will reduce the monetary penalty by 20% to **£144,000** (One hundred and forty four thousand pounds). You should be aware that if you decide to take advantage of the early payment discount you will forfeit your right of appeal.

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 19 September 2014 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 20th day of August 2014

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 19 September 2014 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)).