Data Protection Act 1998

Monetary Penalty Notice

Dated: 15 October 2013

Name: MINISTRY OF JUSTICE
Address: 102 Petty France, London SW1H 9AJ

Introduction

1. This Monetary Penalty Notice is issued by the Information Commissioner ('the Commissioner') pursuant to section 55A of the Data Protection Act 1998 ('the Act'). A monetary penalty notice is a notice requiring the data controller to pay to the Commissioner a monetary penalty of an amount determined by the Commissioner and specified in the notice.

2. 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'.

3. Following a serious contravention of the data controller's duty, under section 4(4) of the Act, to comply with the seventh data protection principle, the Commissioner considers, for the reasons set out below, to serve on the data controller notice of a monetary penalty in the sum of £140,000 (one hundred and forty thousand pounds).

Statutory framework

---

4. 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.

5. 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 ('MPN') 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.

6. 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.

7. This case involves the disclosure of personal data and sensitive personal data. Personal data is defined in section 1 of the Act.

8. Sensitive personal data is defined in section 2 of the Act (in so far as it is applicable to this case) as follows:-

"In this Act "sensitive personal data" means personal data consisting of information as to- [the data subject's]

(a)the racial or ethnic origin of the data subject,
…
(g) the commission or alleged commission by him of any offence, or
(h)any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings"

Power of Commissioner to impose a monetary penalty

---

9. 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

---

10. On 2 August 2011 a member of the public reported to the data controller that he had received by email details of inmates at HMP Cardiff ('the Prison'). The email had been sent to the individual on the previous day. He was the intended recipient. A file containing the details of 1,182 inmates had accidentally been attached to the email.

11. The data controller completed an internal significant data breach investigation in response to the incident. The initial investigation showed there had been two previous instances of the same error on 4

and 11 July 2011 where the prisoner details had been sent to a separate individual on each occasion. On those occasions the recipients of the emails had not contacted the data controller or the Prison. A total of three emails with the attachment of prisoner details had been sent to three different individuals. Prior to notification on 2 August 2011 the data controller had not been aware that the unauthorised disclosures had taken place.

12. The investigation revealed that a recently appointed booking clerk at the Prison was arranging visits to prisoners. A request for a booking had been made by a family member of an inmate. The clerk had intended to send him an email about the visit. In doing so, she accidentally 'pasted' a text file containing the details of the inmates at the prison as an attachment to the email. The two prior incidents had occurred as a result of the same mistake, by the same clerk.

13. Shortly after the breach was known, a representative of the data controller and the police visited the recipients of the emails. Each recipient confirmed in writing that the email message had not been disseminated further and that it had been fully deleted. For two of the recipients, access was allowed to their email accounts for confirmation of their actions. The other recipient had already double-deleted the message and attachment.

14. The text file contained detailed information on every prisoner at the Prison. The data was stored in a 'comma separated values' (CSV) format and each type of data was contained in a field – with no header information to denote the meaning of each field. The fields of data included; name, DOB, address, details of physical marks including tattoos, wing location in the prison, sentence lengths, release dates and, offence types and ethnicity. Offence types and ethnicity were shown by reference to a code system. In many cases the codes would

be comprehensible without reference to the code system (e.g. BURG for burglary). Six of the prisoners had sex offence information recorded against them. Dates, such as DOB and the date of release were in normal date format but with no heading explanation. Sentence length data was in three consecutive fields – e.g. 06, 01, 00. The Commissioner is satisfied this data was personal data and sensitive personal data.

15. The prisoner data is stored on a database which is held on a network system called Quantum. It is a secure accredited network system meeting HM Government IT standards for handling information up to a RESTRICTED marking, and access to it is strictly controlled. There is a separate non-networked system, the biometrics system, used for booking and processing visits, and other security-related matters for prisoners. The two systems are physically separate. There are daily transfers of data from the Quantum system to update the biometrics system, to facilitate visits and other prisoner movements. The only way the information can be transferred from the Quantum system to the biometrics system is to carry out a 'profile dump' of all inmate details. The transfer is done at the start of each day by the booking clerk who locates the text file via Windows Explorer on the Quantum system and then, using the 'copy and paste' function, places the file on an unencrypted floppy disc. The disc with the copy file is then removed from Quantum and physically placed in the biometric system to load the copy file to facilitate the update, which takes place by checking for differences between that file and the biometric system's own database. Following the transfer the copy file is erased from the disc. The disc is then stored securely in a locked drawer.

16. The email program used by the data controller is Outlook. It is run on the Quantum system (the main network infrastructure) as it requires

network connectivity. The text files in question had remained on the 'clipboard' of Quantum, which allowed the accidental pasting as email attachments. The Prison uses 'rich text' email format which displays attachments in the body of the email message as a fairly large icon. The emails in question were sent in HTML format, which displays the attachments as a single line of text immediately below the email header. The attachments to the emails were in excess of 250Kb. There is no monitoring software installed on the Quantum network to detect emails with attachments over a certain size, or those containing protectively-marked information. The data controller has stated that it would be too expensive to purchase and host commercially-available scanning software on the Quantum system and such costs would not be proportionate to the risk associated with the incidents that occurred at the Prison.

17. The data controller has in place a number of policies and procedures relating to the use of protectively-marked information and IT. These policies make it clear that prisoner/offender personal data should be treated as RESTRICTED as a minimum until determined otherwise; there is no requirement for an electronic file to be electronically marked with the protective marking; monitoring software may be used to check the content and use of emails (although it is not in use for detecting attachments); protectively-marked material must not be sent over the internet; staff should not send very large files by email (over 250Kb) unnecessarily; and emails should be spell-checked and read through prior to sending as they are unlikely to be retrievable after sending.

18. The clerk who sent the emails was a relatively new employee. She had received induction and general training, along with specific training on the booking system in her first two weeks. Training on the update

procedure took place a week later, and the following week she was given responsibility for the procedure. The standard supervision arrangements at the Prison for the visit bookings clerk involve one-to-one shadowing for 1 or 2 days, with a further 15 working days under supervision before the employee is permitted to work without assistance. The clerk who sent the emails worked on her own four weeks after starting at the Prison and two weeks after commencing training on the update procedure.

19. The data controller states that it is normal procedure for all employees to undertake security awareness and IT induction training as a minimum requirement prior to system access being granted. This is followed by the employee shadowing a more experienced member of staff, and then by a more experienced staff member shadowing the new employee to ensure they understand their role. As there is no formal audit trail, it is not possible to say with full confidence whether the clerk had demonstrated the appropriate level of competence.

20. At the time of the incidents there was no formal written guidance in place to detail how the data transfer process should have operated. Since this incident occurred, the existing training and on-going support has been enhanced by monthly checks. The new procedure ensures there is an appropriate audit trail in place. The data controller has stated the data transfer procedure has been modified. A floppy disc is no longer used. In its place an encrypted memory stick is used for the data transfer. The method used for placing the data on the USB stick is to locate the text file and use the 'send to' function, not the 'copy and paste' method. Therefore the file is not retained on the 'clipboard', which the data controller considered to be a key factor in this case. Following the successful update, the PC used to copy the file is rebooted to clear any temporary files and this is checked by trying a

'paste' in a Word document. However, the new procedure still does not remove the risk of manual error or oversight. Further, the new instructions provided to the Commissioner do not mention using the 'send to' function, rebooting the PC or attempting to paste into a new Word document. It appears these particular instructions may be given verbally.

21. The data controller explained that it was necessary for all prisoner data to be transferred on a daily basis, as opposed to only the necessary updated data fields, due to constraints of the IT system. It maintains that the new process in place ensures accuracy and integrity of the data transfer in the most cost-effective and pragmatic manner.

22. The data controller has argued that most of the information revealed was, by virtue of the judicial process, already in the public domain. Some of the information would be available via court records and similar, such as voter lists. However, it would be necessary for someone to access these records proactively to compile a data set of this type. Data relating to prisoners' physical descriptions, wing location in the prison and anticipated release date would not be in the public domain.

23. The Prison is a Category C closed prison, housing categories C and B and stage 1 and 2 lifer prisoners, mainly from the local area. These are prisoners for whom maximum security is not necessary, but for whom escape must be made difficult, or those who may not pose a significant risk of escape, but cannot be trusted in an open prison.

24. The data controller has not notified the prisoners of the disclosures. This decision was made following an assessment of the impact of disclosure on those prisoners released and due for release since the

date of the original data loss, and liaison with local police on measures to safeguard those individuals if required. The data controller thought there was little the inmates could do to mitigate any risk from the disclosure and that those prisoners at risk of self-harm would suffer additional unnecessary anxiety if informed.

25. The data controller reported the unauthorised disclosures to the Commissioner on 8 September 2011.

Grounds on which the Commissioner proposes to serve a monetary penalty notice

---

26. 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.

Serious contravention of section 4(4) of the DPA

27. 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.

28. The Seventh Data Protection Principle 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".

29. 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"

30. In particular, the data controller has failed to take sufficient appropriate technical and organisational measures against unauthorised processing and accidental loss of personal data so as to effectively prevent such unauthorised processing or accidental loss occurring. As well as technical measures such measures may include providing its employees with appropriate and adequate training, the outcomes of which are suitably monitored; sufficient supervision of employees undertaking a new procedure which is adequately documented; providing clear written procedures and checklists for the daily data transfer; and management checks on the operation of the procedure to ensure the process was sufficiently adhered to. The data controller should have taken timely steps to introduce the use of a more secure means of carrying out daily routine transfers of high

volumes of personal data. The Commissioner notes that the breach to which this notice relates arises from an error repeated on three occasions over a period of several weeks and that this was not detected until the Prison was notified by a member of the public.

31. The Commissioner considers that the contravention is serious for the following reasons:

i) The activity involved was a daily routine involving the transfer of high volumes of sensitive personal data between two internal databases that had been the practice for some time.

ii) The process for undertaking the transfer had not been appropriately risk assessed or scoped. The significant volume of personal data involved is of a kind that would be likely to cause substantial distress if lost or inappropriately disclosed.

iii) The data controller had not adopted any appropriate checking procedures and failed to explore appropriate technical measures to reduce the risk of such an incident.

iv) Those measures which were put in place by the data controller did not ensure a level of security appropriate to the harm that might result from such unauthorised processing or accidental loss and the nature of the data to be protected.

The contravention is of a kind likely to cause substantial distress

32. The Commissioner is further satisfied that the contravention in this particular case is of a kind likely to cause substantial damage and substantial distress for the following reasons:-

i) A large amount of sensitive personal data relating to 1,182 prisoners was unintentionally disclosed to three members of the public due to inappropriate technical and organisational measures taken by the data controller.

ii) The personal data included, the fact that an individual was an offender/prisoner, coded offences (almost all easily recognisable), multiple offences, last known address, DOB, and other identifying physical characteristics and their current location within the Prison.

iii) In specific reference to the third incident, as the information had been sent to an inmate's relative, they would have been familiar with the details of that inmate, thus making it more likely that they would have been able to decipher the coding of the information to learn the details of the other 1,181 individuals.

iv) Even without this knowledge, the offence codes used are basic and most of them would be easily deciphered by an ordinary member of the public. For people with knowledge of the criminal justice system, even the less obvious codes would be likely to be deciphered.

v) It was fortuitous that the emails had been sent to one person on each occasion, and that on the third occasion of the breach, the recipient had notified the data controller and it was possible to obtain assurances and, in two instances, physical access to the email accounts to ensure the information was destroyed.

vi) The data controller had taken the decision not to disclose the breach to the prisoners because it may cause some at risk of 'self-harm' to suffer additional anxiety. Therefore some prisoners

may have been considered likely to suffer greater distress than others, including some of the affected prisoners who have recorded offences for rape or other sexual offences.

vii) If the data had got into the wrong hands (e.g. those involved with criminality or a rival of a particular inmate) this would be considered to raise the level of distress caused by the disclosures.

The data controller ought to have known that there was a risk that the contravention would occur, that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to reasonable steps to prevent the contravention

33. 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 it failed to take reasonable steps to prevent the contravention for the following reasons:-

i) The data transfer was undertaken on a daily routine basis involving a large volume of sensitive personal data. There were no written procedures or checking mechanisms in place for the daily data transfer.

ii) Management should have realised the potential for human error in using the 'copy and paste' function particularly by a new member of staff with limited training and experience.

iii) The data controller did not take reasonable steps to prevent the contravention, such as technical measures and providing its employees with appropriate and adequate training, the outcomes of which are suitably monitored; sufficient supervision of employees undertaking a new procedure which is adequately documented; providing clear written procedures and checklists for the daily data transfer; and management checks on the operation of the procedure to ensure the process was sufficiently adhered to.

iv) The data controller should have taken timely steps to introduce the use of a more secure means of carrying out daily routine transfers of high volumes of personal data.

34. In the circumstances, 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 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

Effect of the contravention

35. The contravention was particularly serious because of the confidential and sensitive nature of the personal data.

Behavioural issues

36. There was no means of identifying when this type of incident occurred. It was unknown to the data controller until a recipient of the unauthorised disclosure had contacted the Prison.

37. The data controller and in particular its Executive Agency, NOMS appears to have limited oversight of the specific operational activities of the business areas under its control.

Impact on the data controller

38. 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

39. Although multiple disclosures were made, the data was sent to a small number of individuals. One individual brought the unauthorised disclosure to the attention of the data controller.

40. As far as the Commissioner is aware, none of the personal data involved in any of the security breaches has been further disseminated.

Effect of the contravention

41. The personal data compromised in these breaches has been confirmed by the data controller as having destroyed and written assurances have been received from the recipients that there has been no further dissemination.

Behavioural issues

42. The data controller has taken some remedial action in respect of these breaches, with a view to preventing a recurrence.

43. The breach was self-reported and data controller has been co-operative with Commissioner's investigation.

Impact on the data controller

44. There is likely to be a significant impact on the reputation of the data controller as a result of these security breaches.

45. 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

---

46. 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 standardisation across the prison service as it is possible similar practices could be happening elsewhere.

This will highlight this poor practice, encourage improvements and have a broader impact on compliance across this business area.

47. Contravention of the Third Data Protection Principle in that excessive personal data was routinely transferred by manual means on a daily basis.

48. 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

---

49. A notice of intent was served on the data controller dated 13 August 2013. The Commissioner received written representations from the data controller's Permanent Secretary dated 16 September 2013. 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 proposes to impose

---

50. 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, he considers that a monetary penalty in the sum of £140,000 (one hundred and forty thousand pounds) is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

51. In reaching this decision, the Commissioner considered other cases of a similar nature in which a monetary penalty has been imposed and the facts and aggravating and mitigating features referred to above. Of particular relevance in this case is the nature of the personal data lost, the potential for harm and likelihood of distress.

Payment

---

52. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 19 November 2013 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

53. If the Commissioner receives full payment of the monetary penalty by 18 November 2013 the Commissioner will reduce the monetary penalty by 20% to £112,000 (one hundred and twelve thousand pounds).

Right of Appeal

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

    a. the imposition of the monetary penalty
    b. and/or;
    c. the amount of the penalty specified in the monetary penalty notice.

55. Any Notice of Appeal should be served on the Tribunal by 5pm on 19 November 2013 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

56. 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.

Dated the 15 October 2013

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

4. The notice of appeal should be served on the Tribunal by 5pm on 19 November 2013 at the latest.

5. 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.

6. 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.

7. 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.

8. 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)).