Data Protection Act 1998

Monetary Penalty Notice

Dated: 26 March 2015

Name: Serious Fraud Office

Address: 2–4, Cockspur Street, London SW1Y 5BS

Statutory framework

---

1. The Serious Fraud Office is a data controller, as defined in section 1(1) of the Data Protection Act 1998 (the "Act") in respect of the processing of personal data 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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 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. Between 2004 and 2006, the data controller conducted a high profile investigation into serious fraud, bribery and corruption. During the course of the investigation, in excess of 11,000 bags of evidential material ('bags') was obtained from a number of parties including witnesses, suspects, government departments, foreign governments, corporate banks and individuals. The investigation was concluded in February 2010. The bags then had to be restored to their respective owners.

5. In 2010, a witness in the investigation ('witness A') requested the return of his evidential material. In November 2011, the data controller returned 371 of the bags to witness A. Witness A then informed the

data controller that, among other things, some of the information in the bags did not belong to him.

6. The data controller considered witness A's concerns at a senior level and was satisfied that witness A was the owner of the material that had been sent to him and that the restoration was correct. Consequently, in May 2012 a decision was made to resume the process of returning material to witness A. Between May and October 2012, a further 1,782 bags were returned to witness A.

7. The Commissioner understands that the bags that were returned to witness A included documents that had been scanned onto the data controller's 'Autonomy' database. The documents contained confidential personal data relating to approximately 6,000 data subjects, some of whom were in the public eye. The documents also contained sensitive personal data relating to two of the data subjects.

8. In February 2013, a [redacted] in the investigation (via his accountants) requested the return of his evidential material. In May 2013, the [redacted] also requested the return of the same material. The data controller's review of the property revealed that out of the requested material, four bags had been incorrectly sent to witness A and a further 11 bags could not be found. The [redacted] was informed of the position.

9. On 13 June 2013, the data controller was asked to provide a briefing for a 'Parliamentary Question' of whether they had recently lost or returned to the wrong person, any evidence relating to a case. On 17 June 2013, the data controller provided a briefing in relation to the executor's material that had been sent erroneously to witness A.

10. On 18 June 2013, the Departmental Security Officer and Senior Information Risk Owner were notified of the loss and they commenced an investigation.

11. It was discovered that a temporary worker ('Temp') in the '[redacted]' had been given the task of preparing the bags for despatch to witness A. Although he had received some 'on the job' training, the Temp was relatively inexperienced in carrying out restorations, not fully supervised and he did not understand what was required of him in such a large and complex restoration.

12. The Commissioner understands that the Temp removed the bags from the boxes he had correctly retrieved from archive. However, the boxes would not necessarily just contain bags belonging to witness A. The Temp did not then check each bag number against the spreadsheet that

identified the owners of each bag before despatch, as required. As a result, the Temp had sent erroneously 407 bags belonging to 64 third parties (including the suspect) to witness A.

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

13. 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".

14. 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".

15. 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 (S55A (1)(a))

16. The Commissioner is satisfied that there has been a serious contravention of the Seventh Data Protection Principle.

17. In particular, the data controller failed to take appropriate organisational measures against the accidental loss of personal data contained in the bags.

18. Such measures might have included:

- Engaging an experienced Temp who had received sufficient training to carry out such a large and complex restoration;
- Providing the Temp with appropriate management supervision to check the quality of his work; and
- Using a system of work that was user friendly with a documented process.

19. The Commissioner considers that the contravention is **very serious** because there has been an underlying failure by the data controller to put appropriate (or any) security measures in place for what was a large and complex restoration. This is unacceptable in view of the nature of the information contained in the bags which should have been afforded the highest levels of security.

Likely to cause substantial damage or substantial distress (S55A (1) (b))

---

20. The Commissioner is satisfied that the contravention is of a kind likely to cause substantial distress.

21. The failure to take appropriate organisational measures was likely to cause substantial distress to the data subjects even if this is simply by knowing that their confidential personal data (in two cases sensitive) has been disclosed to an unauthorised third party. Such information includes the fact that an individual has been involved in an investigation into serious fraud, bribery or corruption.

22. Further, the data subjects would be likely to be distressed by justifiable concerns that their data may be further disseminated even if those concerns do not actually materialise. There is evidence that some of the information may have been disclosed to a national newspaper and possibly disseminated overseas.

23. Therefore, not only was the contravention of a kind likely to cause substantial distress, but there is evidence to suggest that it may in fact have done so.

Knew or ought to have known that there was a risk that the contravention would occur and that it would be of a kind likely to cause substantial damage or distress (S55A (3)(a)(i) and (ii)).

---

24. The Commissioner is satisfied that section 55A(3) of the Act applies in that the data controller knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial distress, but failed to take reasonable steps to prevent the contravention.

25. The Commissioner has taken this view because the data controller should have been aware of the risks associated with such a large and complex restoration. In particular, the data controller was used to handling confidential personal data (sometimes sensitive) during an investigation and then restoring it to the relevant owners on its conclusion. At the time of the security breach, the data controller was storing approximately 47,000 bags of evidential material in archive and was aware that the system of work for restoring the bags was antiquated and required a certain level of understanding.

26. The data controller should also have been aware that there was a risk that the contravention would occur when witness A reported his concerns after the first restoration.

27. In the circumstances, the data controller knew or ought to have known that there was a risk that the contravention would occur unless reasonable steps were taken to prevent the contravention, such as those outlined above.

28. Further, it should have been obvious to the data controller who was aware of the nature and amount of the personal data stored in archive that such a contravention would be of a kind likely to cause substantial distress to the data subjects.

Aggravating features the Commissioner has taken into account in determining the amount of a monetary penalty

---

29. *Effect of the contravention*

    - Some of the information may have been disclosed to a national newspaper and possibly disseminated overseas.

30. *Behavioural issues*

- The data controller should have been aware that there was a risk that the contravention would occur when witness A reported his concerns after the first restoration.

31. *Impact on the data controller*

- The data controller is an independent government department so liability to pay a monetary penalty will not fall on any individual.

- The data controller has access to sufficient financial resources to pay the proposed monetary penalty without causing undue financial hardship.

Mitigating features the Commissioner has taken into account in determining the amount of the monetary penalty

---

32. *Nature of the contravention*

- No previous similar security breach that the Commissioner is aware of.

33. *Effect of the contravention*

- 98% of the information was recovered by the data controller.
- The seals of the bags containing the data were still intact.

34. *Behavioural issues*

- A full investigation was carried out as soon as the data controller became aware of the security breach.
- The data controller made immediate attempts to recover the information from witness A.
- Voluntarily reported to the Commissioner's Office.
- The data controller has been co-operative with the Commissioner's Office.
- The data controller has taken substantial remedial action.

35. *Impact on the data controller*

- Significant impact on reputation of data controller as a result of this security breach.

Other considerations

36. 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 personal data.

Notice of Intent

37. A notice of intent dated 24 February 2015 was served on the data controller. The Commissioner received written representations from the data controller in response to the notice of intent in a letter dated 10 March 2015. The Commissioner has considered those representations 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

38. 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.

39. 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

40. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 28 April 2015 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

41. If the Commissioner receives full payment of the monetary penalty by 27 April 2015 the Commissioner will reduce the monetary penalty by 20% to **£144,000 (one hundred and forty four thousand pounds)**. However, you should be aware that the early payment discount is not available if you decided to exercise your right of appeal.

Right of Appeal

42. There is a right of appeal to the First-tier Tribunal (Information Rights) against:

    a) the imposition of the monetary penalty and/or;

    b) the amount of the penalty specified in the monetary penalty notice.

43. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice. 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.

44. Information about appeals is set out in Annex 1.

Enforcement

45. The Commissioner will not take action to enforce a monetary penalty unless:

- the period specified within 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 appealing against the monetary penalty and any variation of it has expired.

46. 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 of any sheriffdom in Scotland.

Dated the 26th day of March 2015

Signed ……..

David Smith
Deputy Information Commissioner
Information Commissioner's Office
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 sent so it is received by the Tribunal within 28 days of the date of the notice.

   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)).