Information Commissioner's Office

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Crown Prosecution Service

Of: Rose Court, 2 Southwark Bridge, London, SE1 9HS

1. The Information Commissioner ("Commissioner") has decided to issue the Crown Prosecution Service ("CPS") with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA"). The penalty is being issued because of a serious contravention of the Seventh Data Protection Principle by the CPS.

2. This notice explains the Commissioner's decision.

Legal framework

3. The CPS is a data controller, as defined in section 1(1) of the DPA in respect of the processing of personal data. Section 4(4) of the DPA provides that, subject to section 27(1) of the DPA, 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.

4. The relevant provision of the DPA is the seventh data protection principle which provides, at Part I of Schedule 1 to the DPA, 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".

5. Under section 55A (1) of the DPA 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 DPA 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.

6. The Commissioner has issued statutory guidance under section 55C(1) of the DPA about the issuing of monetary penalties that has been published on the ICO's website. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 prescribe that the amount of any penalty determined by the Commissioner must not exceed £500,000.

7. The DPA implements European legislation (Directive 95/46/EC) aimed at the protection of the individual's fundamental right to the protection of personal data. The Commissioner approaches the data protection principles so as to give effect to the Directive.

Background to the case

8. On 18 November 2016, the CPS received a package of 15 unencrypted DVDs from Surrey Police. Those DVDs contained recordings of Achieving Best Evidence ("ABE") interviews with victims of child sexual abuse, to be used in evidence at the trial of the perpetrator. Originals were retained by Surrey Police. All the DVDs contained the most intimate sensitive personal data of the victims, as well as the sensitive personal data of the perpetrator (subsequently convicted having pleaded guilty) and some identifying information of accompanying persons and interviewing officers.

9. On the same day, the receiving CPS office in Guildford sent the package of DVDs to its office in Brighton, where a specialist unit would review the evidence contained on them. The DVDs were sent by tracked DX delivery in a single box. DX logs confirm that the package was sent to the CPS Brighton office on 18 November 2016.

10. The package was delivered to the Brighton office of the CPS – located in a shared building – on 21 November 2016. DX tracking information records that it was delivered at 06.49. The CPS does not believe that its staff were in the building at that time.

11. The entry doors to the office building are locked and require a card and PIN code for access. DX has a code to enable it to make early morning deliveries before normal working hours. When DX makes early morning deliveries to the CPS Brighton office, they are left in an unsecured area in reception. Once in the building, the CPS offices – including the reception area in which deliveries are left – can be accessed by anyone.

12. It was not until 1 December 2016 that the loss of the DVDs was discovered, upon the return from annual leave of the CPS employee who had requested their provision. Searches were made during December of the CPS offices in Brighton, Guildford and Canterbury. The loss was first reported to Surrey Police on 14 December 2016. The CPS Area Business Manager was not formally notified of the loss until February 2017, whereupon a further search was requested of all CPS offices. Searches were also subsequently carried out by Surrey Police and by DX.

13. The DVDs and the personal data contained on them have not been recovered. So far as the Commissioner is aware, it is unknown what has happened to them and whether there has been unauthorised access of that personal data.

14. The DVDs were not encrypted. The CPS has stated that it is not normal practice to encrypt ABE material. Encryption software is, however, available to all areas of the CPS. Nor were the DVDs transported in tamper-proof packaging, as indicated by Annex N of the Ministry of Justice's ABE Guidance.

15. The Commissioner was not notified of the data loss until 11 April 2017, when the CPS self-reported the matter to her office.

16. The CPS' internal investigation has reportedly identified systemic procedural issues within the relevant offices (not limited to the Brighton office), breaches of existing CPS and MoJ policies and a need for immediate staff re-training.

17. The CPS co-ordinated with Surrey Police during March 2017 to notify the victims of abuse who had provided the ABE interviews about the data loss. CPS representatives subsequently held meetings with the families of at least three of the affected data subjects in relation to the loss.

18. The Commissioner has made the above findings of fact on the balance of probabilities.

19. The Commissioner has considered whether those facts constitute a contravention of the DPA by the CPS and, if so, whether the conditions of section 55A DPA are satisfied.

The contravention

20. The Commissioner finds that the CPS contravened the following provisions of the DPA:

21. The CPS failed to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data in contravention of the Seventh Data Protection Principle at Part I of Schedule 1 to the DPA.

22. The Commissioner finds that the contravention was as follows:

- The unencrypted DVDs containing the videos were delivered to a CPS office by a delivery service which did not require signed receipt or delivery into the hands of a CPS employee;
- The CPS had the technological capacity to encrypt the DVDs but did not do so;
- Having failed to encrypt the DVDs, the CPS also failed to transport them in sealed or tamper-proof packaging, despite their intention to use the material in a criminal prosecution;
- The unencrypted and unsealed DVDs were sent to a CPS office where the CPS was aware that they may be delivered and left in an unsecured environment to which anyone in the building had access; and,
- The CPS itself recognises that systemic procedural failings existed in its offices which allowed this data loss to occur.

This was an ongoing contravention until the CPS began remedial action following the security breach in February 2017.

23. The Commissioner is satisfied that the CPS was responsible for this contravention.

24. The Commissioner has gone on to consider whether the conditions under section 55A DPA were met.

Seriousness of the contravention

25. The Commissioner is satisfied that the contravention identified above was serious. This is because the videos contained confidential

and highly sensitive personal data of a substantial number of data subjects.

26. In the circumstances, the Commissioner considers that the contravention was serious having regard to the number of affected individuals and the nature of the personal data involved.

27. The Commissioner is therefore satisfied that condition (a) of section 55A(1) DPA is met.

Contraventions of a kind likely to cause substantial damage or substantial distress

28. The relevant features of the kind of contravention are:

29. Unencrypted DVDs containing videos of police ABE interviews with 15 victims of child sexual abuse, as part of an ongoing criminal prosecution, describing the crimes perpetrated against them. It is indisputable that this type of data is at the very uppermost in sensitivity terms.

30. The Commissioner considers that the contravention identified above had the following potential consequences:

31. The contravention would cause distress to the victims who may suspect that their confidential and highly sensitive personal data has been disclosed to a recipient who has no right to see that information.

32. Further, the victims would be distressed by justifiable concerns (given the highly sensitive nature of some of the information) that their data has been further disseminated even if those concerns do not actually

materialise. Victims may also have been distressed at the possibility that the loss of the data could, if it were to appear in the public domain, adversely affect the prosecution or conviction of the perpetrator. The distress suffered by the victims would be of a significant order.

33. In this context it is important to bear in mind that many of the victims were vulnerable and had already endured distressing interviews with the police.

34. If this information has been misused by those who had access to it, or if it was in fact disclosed to untrustworthy third parties, then the contravention would cause further distress and also substantial damage to the victims, for example, by way of reprisals or adverse comment.

35. The Commissioner considers that the damage and/or distress described above was likely to arise as a consequence of the kind of contravention. In other words, the Commissioner's view is that there was a significant and weighty chance that a contravention of the kind described would have such consequences.

36. The Commissioner considers that that conclusion is borne out by the fact that upon being notified of the data loss a number of the affected victims and their families sought meetings with the CPS. The CPS has not provided the Commissioner with details of those meetings, but the Commissioner considers it inconceivable that the victims sought to do anything other than express their gravest concerns and distress to the CPS.

37. The Commissioner also considers that such damage and/or distress was likely to be substantial, having regard to the number of affected

individuals and the nature of the personal data involved. In the circumstances, the likely damage or distress was certainly more than trivial.

38. The Commissioner has also given weight to the number of affected individuals. The Commissioner considers that even if the damage or distress likely to have been suffered by each affected individual was less than substantial, the cumulative impact would clearly pass the threshold of "substantial". In addition, given the number of affected individuals and the nature of the data lost, it was inherently likely that at least some of those individuals would have been likely to suffer substantial damage or substantial distress on account of their particular circumstances.

39. The Commissioner is therefore satisfied that condition (b) of section 55A(1) DPA is met.

Deliberate or negligent contraventions

40. The Commissioner has considered whether the contraventions identified above were deliberate, but has concluded that the CPS did not deliberately contravene the DPA.

41. The Commissioner has gone on to consider whether the contraventions identified above were negligent. First, she has considered whether the CPS knew or ought reasonably to have known that there was a risk that these contraventions would occur. She is satisfied that this condition is plainly met, given that the CPS was used to handling videos of ABE interviews containing confidential and highly sensitive personal data. The CPS is also responsible for prosecuting criminal

cases investigated by the police in England and Wales. Therefore, the CPS must have been aware that the videos must be kept secure.

42. In the circumstances, the CPS ought reasonably to have known that the videos containing the ABE interviews would be vulnerable to a security breach in the absence of appropriate security measures.

43. The Commissioner has also had regard in this respect to a previous breach of the Seventh Principle by the CPS in relation to failing properly to secure recordings of victim and witness evidence in sexual abuse cases and their subsequent theft. Despite a monetary penalty notice being issued in 2015, the CPS does not appear to have ensured that appropriate care is being taken to avoid similar breaches re-occurring.

44. Second, the Commissioner has considered whether the CPS knew or ought reasonably to have known that those contraventions would be of a kind likely to cause substantial damage or substantial distress. She is satisfied that this condition is met, given that the CPS was aware of the graphic and highly distressing nature of the personal data contained in the videos. Therefore, it should have been obvious to the CPS that such a contravention would be of a kind likely to cause substantial damage or substantial distress to the affected individuals.

45. Third, the Commissioner has considered whether the CPS failed to take reasonable steps to prevent the contravention. Again, she is satisfied that this condition is met. Reasonable steps in these circumstances would have included: transporting DVDs only in encrypted form; transporting DVDs in sealed and tamper-proof packaging at the least; delivering the unencrypted DVDs by secure courier with a requirement that an individual sign for them; and ensuring that deliveries could be

made into a secure area. The CPS failed to take any of those steps.

46. The Commissioner is therefore satisfied that condition (c) of section 55A(1), read with section 55A(3), DPA is met.

The Commissioner's decision to issue a monetary penalty

47. The Commissioner has taken into account the following **mitigating features** of this case:

- The breach was eventually voluntarily reported to the ICO.
- The DVDs have been not accessed by an unauthorised third party as far as the Commissioner is aware.
- The CPS eventually notified the affected individuals.
- The CPS has been fully co-operative with the ICO.
- The CPS has self-identified systemic failings and is taking action to remedy them.
- There is likely to be a significant impact on the CPS's reputation as a result of this security breach.

48. The Commissioner has also taken into account the following **aggravating features** of this case:

- Only in 2015, the CPS was the subject of a monetary penalty notice of £200,000 resulting from a failure to encrypt and/or secure recordings of victim and witness interviews in the context of sexual abuse. Despite this, CPS employees have continued not to take basic encryption and security precautions in respect of such recordings, and there remain, on the CPS's own conclusions, systemic procedural failings.
- The ICO was not notified of the breach for more than four months after the CPS became aware of it.

- Affected data subjects were not notified until some three months after the CPS became aware of it.
- The CPS was slow internally in escalating the breach to the appropriate level of management.
- The lost DVDs have never been recovered.

49. For the reasons explained above, the Commissioner is satisfied that the conditions from section 55A (1) DPA have been met in this case. She is also satisfied that section 55A (3A) and the procedural rights under section 55B have been complied with.

50. The latter has included the issuing of a Notice of Intent, in which the Commissioner set out her preliminary thinking. In reaching her final view, the Commissioner has taken into account the representations made by the CPS in their correspondence of 1 May 2018 on this matter.

51. The Commissioner is accordingly entitled to issue a monetary penalty in this case.

52. The Commissioner has considered whether, in the circumstances, she should exercise her discretion so as to issue a monetary penalty.

53. The Commissioner has had regard to the fact that the CPS is a public authority so liability to pay a monetary penalty will not fall on any individual, and that it has access to sufficient financial resources to pay the proposed monetary penalty without causing undue financial hardship, nevertheless, the CPS's representations in this regard have been taken into account by the Commissioner when reaching a determination as to the final penalty amount.

54. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the DPA 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.

55. For these reasons, the Commissioner has decided to issue a monetary penalty in this case.

The amount of the penalty

56. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of **£325,000 (Three hundred and twenty five thousand pounds)** is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

Conclusion

57. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **14 June 2018** 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.

58. If the Commissioner receives full payment of the monetary penalty by **13 June 2018** the Commissioner will reduce the monetary penalty by 20% to **£260,000 (two hundred and sixty thousand pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

59. 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.

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

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

62. 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.

63. 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 14th day of May 2018.

Signed [redacted]

Stephen Eckersley
Head of Enforcement
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 (Information Rights) (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 she ought to have exercised her 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;

g) you must provide with the notice of appeal a copy of the monetary penalty notice or variation notice;

h) 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)).