DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Chief Constable of Kent Police

Of: Force Headquarters, Sutton Road, Maidstone, Kent ME15 9BZ

Introduction

1. The Information Commissioner ("Commissioner") has decided to issue the Chief Constable of Kent Police ("Kent Police") with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA"). He is minded to do so because of a serious contravention by Kent Police of the seventh data protection principle.

2. This notice explains the Commissioner's decision.

Legal framework

3. Kent Police 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:

7. 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. Interpretative provisions in Part II of Schedule 1 to the DPA provide that:

9. 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.

10. The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

6. 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 –

(1) (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 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.

7. 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.

8. 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 this case

9. An individual ("the data subject") accused her partner, a serving police officer of Kent Police, ("the officer") of domestic abuse. She alleged that she was physically assaulted and suffered criminal damage to her property.

10. The data subject had a video recording on her mobile phone to support the accusation. Her mobile phone held over 13,000 files, including details of the data subject's divorce, texts and intimate photographs containing (sensitive) personal data, all unrelated to the data subject's complaint about the officer.

11. The data subject gave her mobile phone to Kent Police who extracted the entire contents of the data subject's mobile phone.

12. The master copy was not directly readable, so the files were copied onto two CDs: an edited working copy containing only the relevant video recording and a full working copy containing all the files extracted from the mobile phone ("the full working copy").

13. The full working copy included "unused" material in the criminal proceedings. Under the Criminal Procedures and Investigations Act 1996 ("CPIA"), the CPS may have to disclose such material to the defence if it undermines the prosecution case or assists the defence.

14. Subsequently, the data subject did not want to go to court and changed her mind about pursuing her complaint. The criminal proceedings were discontinued. The officer was then the subject of a misconduct investigation conducted by the Professional Standards Department.

15. On 12 February 2014, a manager employed by Kent Police disclosed documents to the officer's solicitor in advance of the misconduct hearing. However, the full working copy was also sent to the officer's solicitor by mistake, as a result of inappropriate security measures.

16. The officer's solicitor disclosed this information to his client who then saw the files that had been extracted from the mobile phone and informed the data subject accordingly. The officer's solicitor has refused to return the full working copy on the grounds that it is relevant to his client's defence.

17. The criminal proceedings were re-instigated and the officer was acquitted. However, the officer has now been dismissed from Kent Police.

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 Kent Police and, if so, whether the conditions of section 55A DPA are satisfied.

The contravention

20. The Commissioner finds that Kent Police processed (sensitive) personal data in contravention of the seventh data protection principle at Part I of Schedule 1 to the DPA. The Commissioner finds that the contravention was as follows.

21. Kent Police has accepted that the full working copy should not have been disclosed to the officer's solicitor in these circumstances. The Commissioner finds that Kent Police did not have in place appropriate organisational measures for ensuring so far as possible that such incidents would not occur, i.e. for ensuring that data obtained from complainants (such as that obtained from the data subject's phone in this instance) was only disclosed to other parties (such as the officer

and/or his representatives) where it was lawfully, necessary and proportionate to do so.

22. In particular:

(a) Kent Police has in place a written procedure for how disclosures to defendants and their representatives should be managed in criminal cases. It has no comparable procedure for misconduct cases. For such cases, it has no written procedures for distinguishing between disclosable evidence and material which is not to be disclosed.

(b) The person to whom Kent Police entrusted the disclosure process was a hearings manager, who had an administrative role. That manager had no prior knowledge of these proceedings, and did not receive any (or any adequate) input, supervision or oversight from officers involved in the investigation (or others with similar experience) which would have enabled the hearings manager to distinguish between what was to be disclosed and what was to be withheld.

(c) Kent Police had in place no procedure for checking the contents of material prepared for disclosure prior to disclosure taking place, even in cases involving highly sensitive personal information.

23. The above deficiencies constitute inadequacies in Kent Police's organisational measures for preventing unauthorised disclosures of personal data. They constitute a contravention of the seventh data protection principle.

24. The Commissioner is satisfied that Kent Police was responsible for this contravention of the seventh data protection principle.

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

Seriousness of the contravention

26. The Commissioner is satisfied that the contravention identified above was serious due to the context in which the (sensitive) personal data was obtained, the number of files that were extracted from the mobile phone (over 13,000) and prepared for disclosure, the highly sensitive nature of some of the personal data and the potential consequences. In those circumstances, Kent Police's failure to take adequate steps to safeguard against unauthorised disclosure was serious.

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

Contravention of a kind likely to cause substantial distress

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

(a) Partial disclosure needed to be made to the officer's representatives. This entailed distinguishing between information which should be disclosed and information which should not be disclosed. Such decisions are likely to require guidance, oversight and/or experience.

(b) This is all the more so when sensitive, intimate and private material is concerned – in particular, as regards a data subject in vulnerable circumstances who approached Kent Police as a complainant in a serious matter involving the person to whom partial disclosure is to be made. This heightens the need for robust measures – in organisational, procedural and staffing terms – to safeguard against unauthorised disclosures.

(c) Kent Police is alive to the need to ensure that it has robust measures in place for criminal matters. It appears to have overlooked the same as regards disciplinary matters, for no good reason.

29. The Commissioner therefore considers that, by reference to the features of this contravention, it was of a kind likely to cause distress. The Commissioner also considers that such distress was likely to be substantial having regard to the highly sensitive nature of some of the personal data, the circumstances of the data subject and the relationship between the data subject and the officer. In the circumstances, the likely distress was certainly much more than trivial.

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

Deliberate or foreseeable contravention

31. The Commissioner has considered whether the contravention identified above was deliberate. In the Commissioner's view, this means that Kent Police's actions which constituted those contraventions were deliberate actions (even if Kent Police did not actually intend thereby to contravene the DPA).

32. The Commissioner considers that in this case Kent Police did not deliberately contravene the DPA in that sense. He considers that the inadequacies outlined above were matters of serious oversight rather than deliberate intent to ignore or bypass provisions of the DPA.

33. The Commissioner has gone on to consider whether Kent Police knew or ought reasonably to have known that there was a risk that this contravention would occur. He is satisfied that this condition is met, given that Kent Police was used to handling the mobile phones of victims and witnesses containing highly sensitive personal data, and also used to undertaking disclosure processes of such a kind. Kent Police was or ought reasonably to have been aware that it needed to ensure so far as possible that the correct distinctions were drawn between disclosable material and material which was not be disclosed.

34. In the circumstances, Kent Police ought reasonably to have known that there was a risk that this contravention would occur unless it ensured the process was governed by written procedures, undertaken by staff with appropriate experience and supervision, and that material was checked prior to disclosure.

35. Second, the Commissioner has considered whether Kent Police knew or ought reasonably to have known that the contravention would be of a kind likely to cause substantial distress. He is satisfied that this condition is met, given that Kent Police was aware of the sensitive material (including intimate photographs) that were held on the mobile phone. Kent Police ought to have known that the mobile phones of the average person (including this data subject) contained personal information of a very private and sensitive nature that would cause substantial distress if used in ways the data subject did not envisage.

36. Kent Police should also have known that inappropriate disclosures in the context of this relationship (the data subject as complainant against the officer, her former partner) and the seriousness of the allegations were likely to result in substantial distress if excessive and unauthorised disclosures of personal data took place.

37. Therefore, it should have been obvious to Kent Police that such a contravention would be of a kind likely to cause substantial distress to the data subject.

38. Third, the Commissioner has considered whether Kent Police failed to take reasonable steps to prevent the contravention. Again, he is satisfied that this condition is met. Reasonable steps in these circumstances would have entailed putting in place written procedures governing disclosures in misconduct cases, ensuring that appropriately experienced and/or supervised staff undertook the disclosure process and that the outcome of their work was checked by someone else before disclosure was undertaken. Kent Police did not take those steps. The Commissioner considers there to be no good reason for that failure.

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

The Commissioner's decision to issue a monetary penalty

40. For the above reasons, the Commissioner considers there to have been a serious contravention of the seventh data protection principle on the part of Kent Police with respect to the disclosure of the full working copy to the officer. The contravention was of a kind likely to cause substantial distress. Kent Police knew or ought to have envisaged those risks and it did not take reasonable steps to prevent the contravention.

The Commissioner is satisfied that the conditions from section 55A(1) DPA have been met in this case. He is also satisfied that section 55A(3A) and the procedural rights under section 55B have been complied with.

41. The latter has included the issuing of a Notice of Intent dated 17 February 2016, in which the Commissioner set out his preliminary thinking.

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

43. The Commissioner has considered whether, in the circumstances, he should exercise his discretion so as to issue a monetary penalty. He has taken into account the representations made in response to the Notice of Intent and in other correspondence on this matter. Having considered these further submissions, the Commissioner is persuaded as regards the first data protection principle.

44. The Commissioner has also considered whether the contravention identified above could be characterised as one-off events or attributable to mere human error. He does not consider that the contravention could be characterised in those ways.

45. The Commissioner has concluded that it is appropriate for him to exercise his discretion in favour of issuing a monetary penalty in the circumstances. The contravention is serious in terms of both Kent Police's deficiencies and the impact such deficiencies were likely to (and in this case did) have on the data subject.

46. The issuing of a monetary penalty in this case would be fair and just. It would accord with the Commissioner's statutory guidance and regulatory objectives. It would act as an encouragement to ensure that such deficiencies are not repeated elsewhere.

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

The amount of the penalty

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

a. Kent Police made prompt efforts to secure the return of the full working copy. However, those efforts are the bare minimum to be expected of any data controller in such circumstances, and those efforts have in this case been unsuccessful, resulting in ongoing distress to the data subject.

b. Kent Police acted promptly to ensure that, in future, administrative staff members are not given full responsibility for such disclosure procedures.

c. Kent Police referred this incident to the Commissioner itself and was co-operative during the Commissioner's investigation.

d. A monetary penalty may have a significant impact on Kent Police's reputation.

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

a. The data subject has made a formal complaint to Kent Police.

50. The Commissioner has considered the likely impact of a monetary penalty on Kent Police. He has decided that Kent Police has access to sufficient financial resources to pay the proposed monetary penalty without causing undue financial hardship.

51. 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 the police forces to ensure that they have complied with the seventh data protection principle before they disclose (sensitive) personal data from the mobile phone of a victim, complainant or witness.

52. Taking into account all of the above, the Commissioner has decided that the appropriate amount of the penalty is **£80,000 (Eighty thousand pounds).**

Conclusion

53. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **19 May 2016** 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.

54. If the Commissioner receives full payment of the monetary penalty by **18 May 2016** the Commissioner will reduce the monetary penalty by 20% to **£64,000 (Sixty four thousand pounds).** However, you

should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

55. 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.

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

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

58. 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.

59. 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 18th day of April 2016

Signed ……..

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) 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)).