

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Humberside Police

Of: Police Headquarters, Priory Road, Hull, East Yorkshire, HU5 5SF

1. The Information Commissioner ("Commissioner") has decided to issue Humberside Police 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 Humberside Police.
2. This notice explains the Commissioner's decision.

Legal framework

3. Humberside 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:

"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. Paragraph 9 at Part II of Schedule 1 to the DPA 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".

8. 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.

9. 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.

10. 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

11. On 13 June 2015 Humberside Police conducted an interview of an alleged rape victim on behalf of Cleveland Police. The interview was recorded at the Sexual Assault Referral Centre in Hull and was recorded on three disks (with video footage), comprising the master

copy and two further copies. The three disks, with accompanying written notes, were passed to the Protecting Vulnerable People (PVP) Unit with the intention of sending all three disks to Cleveland Police.

12. The disks themselves had the victim's name, date of birth and date of interview written on them. One copy would have had a master tape paper seal around it along with signatures of the alleged victim and interviewing officers.
13. The disks comprised an interview with the alleged victim and contained information relating to the period prior to the alleged rape, how the alleged victim and alleged perpetrator met, travel arrangements, details relating to the scene of the alleged rape, the alleged rape itself, actions of both alleged victim and perpetrator, and the alleged victim's mental health status.
14. The disks were accompanied by notes on a Form 891 ("Index of Video recorded Interview") and a typed page of notes with summary details. Form 891, as well as detailing of the alleged offence, contained the alleged victim's name, date of birth, medication and mental health conditions, address and name of friend that accompanied the alleged victim post incident, and the alleged perpetrator's name and date of birth.
15. The unencrypted disks, along with the notes, were placed in the same envelope on an officer's desk. The intention was that the envelope would be posted, however the envelope has subsequently been unable to be located and determined to be lost by Humberside Police. It is not known whether the envelope was actually sent to Cleveland Police.

16. Some 14 months later, on 11 August 2016, Cleveland Police notified Humberside Police of the potential loss of the disks, because there was no record of the disks having been received.
17. An internal search by Humberside Police failed to locate the disks and they are still missing.
18. The lost disks were the only copies and no alternative to the disks, working copies or otherwise, were held by Humberside Police
19. The alleged victim was informed of the loss on 23 November 2016.
20. The Commissioner has made the above findings of fact on the balance of probabilities.
21. The Commissioner has considered whether those facts constitute a contravention of the DPA by Humberside Police and, if so, whether the conditions of section 55A DPA are satisfied.

The contravention

22. The Commissioner finds that Humberside Police contravened the following provisions of the DPA:
23. Humberside Police 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.

24. Humberside Police also failed to comply with the requirements set out in paragraph 9 at Part II of Schedule 1 to the DPA.

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

- Humberside Police failed to encrypt the disks before sending (or intending to send) by unsecure mail.
- Humberside Police failed to maintain a detailed audit trail of the package, either on the case or by way of other auditable record;
- The PVP Unit within Humberside Police failed to adhere to its 'Information Security policy' in relation to removable media.

This was an ongoing contravention until Humberside Police took remedial action following notification of the loss by Cleveland Police on 11 August 2016.

26. The Commissioner is satisfied that Humberside Police was responsible for this contravention.

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

Seriousness of the contravention

28. The Commissioner is satisfied that the contravention identified above was serious.

29. This is because the disks and written notes contained confidential and highly sensitive personal data.

30. In the circumstances, the Commissioner considers that the contravention was serious having regard to the nature of the personal data involved.
31. Furthermore, it appears in this case, and routinely within the PVP Unit, that officers did not adhere to existing policies and procedures.
32. The Commissioner is therefore satisfied that condition (a) from section 55A (1) DPA is met.

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

33. The relevant features of the kind of contravention are:
34. Unencrypted disks containing video of a police interview with one alleged victim in a case. No other copies of the information are held. The case was ongoing and of a violent or sexual nature. The interviews contain details of the identity of the alleged victim, mental health status, together with detailed circumstances of and surrounding the commission of the alleged offence. The notes contain a summary of the alleged offence together with the name and date of birth of both alleged victim and perpetrator. The information has not been recovered and is still missing. The victim has been notified of the loss of the information.
35. The Commissioner considers that the contravention identified above had the following potential consequences:
36. The contravention would cause distress to the data subjects 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.

37. Further, the data subjects would be distressed by concerns that their data has been further disseminated, even if those concerns do not actually materialise. Such concerns would be compounded by the fact that the disks and notes have still not been recovered by the data controller. In the circumstances, the distress suffered by the data subjects is considered to extend beyond mere irritation.
38. 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 data subjects, for example, by way of reprisal attacks.
39. The victim was aware that the information has been lost and has indicated that they are not keen to engage again with the police, and is reluctant and unhappy at the prospect of participating in a further interview. The Commissioner considers it reasonable to assume in the circumstances (given that no other copy of the information was held) that the victim could be further distressed by the prospect that the loss of the information could jeopardise any future prosecution.
40. The alleged perpetrator's right to a fair hearing could also be affected by the loss of the data causing substantial distress to them as a data subject.
41. 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.

42. The Commissioner also considers that such damage and/or distress was likely to be substantial, having regard to the nature of the personal data involved. In the circumstances, the likely damage or distress was certainly more than trivial.
43. The Commissioner is therefore satisfied that condition (b) from section 55A (1) DPA is met.

Deliberate or negligent contraventions

44. The Commissioner has considered whether the contraventions identified above were deliberate. In the Commissioner's view, this means that Humberside Police's actions which constituted those contraventions were deliberate actions (even if Humberside did not actually intend thereby to contravene the DPA).
45. The Commissioner considers that in this case Humberside Police did not deliberately contravene the DPA in that sense.
46. The Commissioner has gone on to consider whether the contraventions identified above were negligent. First, she has considered whether Humberside Police knew or ought reasonably to have known that there was a risk that these contraventions would occur. She is satisfied that this condition is met, given that Humberside Police was used to handling recordings of police interviews containing confidential and highly sensitive personal data, and was aware of its importance in any subsequent prosecution by the CPS. In particular, the PVP Unit's primary function was to routinely deal with vulnerable individuals.

Therefore, Humberside Police must have been aware that the disks and accompanying notes must be kept secure.

47. Furthermore, Humberside Police had in place at the time of the contravention security safeguards (Information Security Policy, Management of Digital Interview Recordings, encryption guidance and Removable Media process) which would suggest to the Commissioner that Humberside Police had an awareness of security risks.
48. The Commissioner has also taken into account that the Association of Chief Police Officers issued guidance in 2007 (Digital Imaging Procedure) emphasising the need to store master copies securely. In addition, the Ministry of Justice issued guidance in March 2011 (Achieving Best Evidence in Criminal Proceedings) that it was an 'essential' requirement to have a policy on the storage of such disks.
49. In the circumstances, Humberside Police ought reasonably to have known that the disks containing the police interviews would be vulnerable to a security breach in the absence of appropriate security measures.
50. Second, the Commissioner has considered whether Humberside Police 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 Humberside Police was aware of the graphic and distressing nature of the personal data contained in the interviews. Therefore, it should have been obvious to Humberside Police that such a contravention would be of a kind likely to cause substantial damage or substantial distress to the affected individuals.

51. Third, the Commissioner has considered whether Humberside Police 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:

- Ensuring the disks were encrypted/in a suitable format for transferring outside the Force area;
- Physical separation of the master disk from the working copies when transferring outside the Force, in order to reduce the risk of loss of all evidence in the case;
- Ensuring adherence to existing policies regarding information security;
- Maintaining an audit trail;
- Strengthening existing policies and procedures regarding storage of and transfer of data, particularly in relation to police interview disks and master copies. For example, extending the Removable Media process to incorporate PVP Unit interview disks;
- Provision of adequate data protection training and monitoring to officers.

52. Humberside Police failed to take any of those steps.

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

The Commissioner's decision to impose a monetary penalty

54. 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(3) and the procedural rights under section 55B have been complied with.

55. The latter has included the issuing of a Notice of Intent dated 23 January 2018 in which the Commissioner set out her preliminary thinking. Humberside Police received the Notice of Intent on 24 January 2018.
56. The Commissioner received representations from Humberside Police on 20 February 2018 which she has taken into consideration when reaching her decision.
57. The Commissioner is accordingly entitled to issue a monetary penalty in this case.
58. The Commissioner has taken into account the following **mitigating features** of this case:
- Humberside Police were not informed of the data loss by Cleveland Police until some 14 months after the event, which impaired Humberside Police's ability to make prompt and effective enquiries in order to adequately trace the missing disks and to identify the specific individual responsible for the loss.
 - Humberside Police voluntarily reported to the ICO.
 - The data has been not accessed by an unauthorised third party as far as the Commissioner is aware.
 - Humberside Police notified the alleged victim.
 - Humberside Police has been fully co-operative with the ICO.
 - Humberside Police has taken remedial action.
 - There will be a significant impact on Humberside Police's reputation as a result of this security breach.

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

- Loss of the master disk and two copies along with written notes heightens the impact of loss and potential for distress;
- Loss of the master disk has implications for the effectiveness of the remedial measures taken in response, as unless the master or copy should be recovered, the evidence contained on the disks has been permanently lost.
- Humberside Police is a public authority so liability to pay a monetary penalty will not fall on any individual.
- Humberside Police has access to sufficient financial resources to pay the proposed monetary penalty without causing undue financial hardship.

60. 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.

The amount of the monetary penalty

61. Taking into account all of the above, the Commissioner has decided that the amount of the penalty is **£130,000 (One hundred and thirty thousand pounds)**.

Conclusion

62. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **2 May 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.

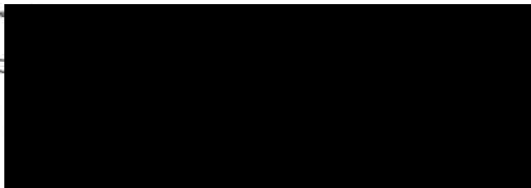
63. If the Commissioner receives full payment of the monetary penalty by **1 May 2018** the Commissioner will reduce the monetary penalty by 20% to **£104,000 (One hundred and four thousand pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.
64. 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.
65. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.
66. Information about appeals is set out in Annex 1.
67. 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.

68. 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 28th day of March 2018

Signed

A large black rectangular box redacting the signature of Stephen Eckersley.

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 (Information Rights) 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)).