

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Gloucestershire Police

Of: Police Headquarters, 1 Waterwells Drive, Quedgeley,
Gloucester, Gloucestershire GL2 2AN

1. The Information Commissioner ("the Commissioner") has decided to issue the Chief Constable of Gloucestershire Constabulary ("GC") 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 GC.
2. This notice explains the Commissioner's decision.

Legal framework

3. GC 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".

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 –

(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.

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 the case

9. At the time of the contravention GC was tasked with the investigation of non-recent allegations of child abuse relating to multiple victims.

10. On 19 December 2016, an officer involved in the investigation sent an email update to 56 recipients by entering the recipient's e-mail addresses into the 'to' field. The recipients of the e-mail could therefore see the full names and e-mail addresses of all the other recipients, who were individuals associated with GC's investigation, including victims of childhood abuse ("the security breach").
11. GC stated that the content of the email itself confirms that the recipients "are interested parties in the investigation. That category included witnesses, journalists and lawyers". The email also made reference to a number of schools and social services that were being investigated in relation to the allegations of abuse.
12. Of the 56 emails sent, all but one was considered deliverable. Three of those delivered were confirmed to have been successfully recalled. Therefore 56 names and email addresses were visible to up to 52 recipients (the exact number is unknown).
13. At the time of the incident the 'bcc' field was not a function automatically selectable on GC's Outlook format. A staff member therefore had to adjust their own settings to be able to use this function. The 'bcc' field was inadvertently not used on this occasion.
14. The full name and email address of each recipient was sent as a result of the officer involved having listed them as contacts on their Microsoft Outlook Account.
15. Once GC had realised its error, it recalled the email and on 21 December 2016 sent an email apology to all recipients, requesting that the original email be deleted. GC also reported the matter to the ICO. One affected data subject contacted the officer involved regarding the incident and a personal apology was given.

16. The Commissioner has made the above findings of fact on the balance of probabilities.
17. The Commissioner has considered whether those facts constitute a contravention of the DPA by GC and, if so, whether the conditions of section 55A DPA are satisfied.

The contravention

18. The Commissioner finds that GC contravened the following provisions of the DPA:
19. GC failed to take appropriate technical and organisational measures against unauthorised processing of personal data in contravention of the seventh data protection principle at Part I of Schedule 1 to the DPA.

In particular:

- GC failed to send a separate e-mail to each participant and instead utilised the bulk email facility;
- GC failed to use the Microsoft Outlook BCC function;
- GC failed to provide staff with any (or any adequate) policies, guidance or training on bulk email communication and the use of the 'bcc' functionality in Outlook, particularly in cases where emails were being sent to multiple victims of sensitive or live cases.

20. This was an ongoing contravention until GC took effective remedial action following the security breach by recalling the email and asking recipients to delete it.
21. The Commissioner is satisfied that GC was responsible for this contravention.
22. The Commissioner has gone on to consider whether the conditions under section 55A DPA were met.

Seriousness of the contravention

23. The Commissioner is satisfied that the contravention identified above was serious. The disclosure identified those interested in an investigation including victims of non-recent child abuse. Recipients of the e-mails could infer from the email content that many of the other recipients were victims of child abuse. This is confidential and sensitive personal data.
24. In the circumstances, the Commissioner considers that the contravention was serious having regard to the number of affected individuals, the nature of the confidential and sensitive personal data involved and the potential consequences.
25. The Commissioner is therefore satisfied that condition (a) from section 55A (1) DPA is met.

Contravention of a kind likely to cause substantial distress

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

27. GC sent an e-mail to 56 participants of which 55 were delivered. Given that 3 emails have been confirmed to be successfully recalled up to 52 recipients could see the full names and e-mail addresses of all 56 intended recipients. They could infer that many the other recipients were, or were associated with victims of child abuse. E-mail addresses can also be searched via social networks and search engines.
28. The Commissioner considers that the contravention identified above had the following potential consequences:
29. The contravention would cause distress to at least some of the participants who know that their full names have been disclosed to unauthorised individuals who could infer that they were victims of child abuse. E-mail addresses can also be searched via social networks and search engines. It would therefore be possible for the unauthorised individuals to identify some of the affected individuals.
30. Further, the participants would be distressed by justifiable concerns that their data has been further disseminated even if those concerns do not actually materialise.
31. In this context it is important to bear in mind that the recipients were suffering from the lifelong consequences of child abuse, and therefore extremely vulnerable. Some of the recipients also had a right to lifelong anonymity.
32. If this information has been misused by those who had access to it, or if it was in fact disclosed to hostile third parties, then the contravention would cause further distress to the participants.

33. The Commissioner considers that the distress described above was likely to arise as a consequence of the kind of contravention.
34. The Commissioner also considers that such distress was likely to be substantial, having regard to the number of affected individuals and the confidential and sensitive nature of the personal data involved.
35. The Commissioner is therefore satisfied that condition (b) from section 55A (1) DPA is met.

Deliberate or negligent contravention

36. The Commissioner has considered whether the contravention identified above was deliberate. In the Commissioner's view, this means that the GC's actions which constituted the contravention were deliberate actions (even if GC did not actually intend thereby to contravene the DPA).
37. The Commissioner considers that in this case GC did not deliberately contravene the DPA in that sense.
38. The Commissioner has gone on to consider whether the contravention identified above was negligent. First, she has considered whether GC knew or ought reasonably to have known that there was a risk that this contravention would occur. She is satisfied that this condition is met, given that emails were an important mechanism by which it engaged with and updated victims of child abuse.
39. GC is an organisation which routinely processes highly sensitive data and which regularly communicates with highly vulnerable victims of crime. At the time of the security breach, 56 individuals were sent mail updates from members of staff who did not use the 'bcc' field to

protect the identity of the other recipients. Therefore, GC should have been aware that there was a risk that its staff could enter the participant's e-mail addresses into the wrong field.

40. It is worth noting that the Commissioner's office issued two monetary penalty notices on 11 December 2015 (Bloomsbury Patients Network) and 4 May 2016 (Chelsea & Westminster Hospital NHS Trust) which raised awareness about the risks of sending bulk e-mails using the 'bcc' field.
41. In the circumstances, GC ought reasonably to have known that the participant's names and e-mail addresses would be vulnerable to a security breach in the absence of appropriate technical and organisational measures.
42. Second, the Commissioner has considered whether GC knew or ought reasonably to have known that the contravention would be of a kind likely to cause substantial distress. She is satisfied that this condition is met, given that GC should have been aware that the e-mail addresses contained the full names of the participants. The recipients of the e-mails could infer that many of the other recipients were victims of child abuse. This is confidential and sensitive personal data. Therefore, it should have been obvious to GC (in the context of the investigation) that such a contravention would be of a kind likely to cause substantial distress to the affected individuals.
43. Third, the Commissioner has considered whether GC failed to take reasonable steps to prevent the contravention. Again, she is satisfied that this condition is met. Reasonable steps in these circumstances could have included carrying out a Privacy Impact Assessment at the outset, deciding to send separate e-mails to each participant, or at the very least providing staff with adequate guidance and training on the

importance of double checking that the participant's e-mail addresses were entered into the 'bcc' field. GC failed to take any of these steps.

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

The Commissioner's decision to issue a monetary penalty

45. For the above reasons, the Commissioner considers there to have been a serious contravention of the seventh data protection principle on the part of GC. The contravention was of a kind likely to cause substantial damage or substantial distress. GC knew or ought to have envisaged those risks and it did not take reasonable steps to prevent the contravention.
46. The Commissioner is satisfied that 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.
47. The latter has included the issuing of a Notice of Intent dated 13 March 2018, in which the Commissioner set out her preliminary thinking.
48. The Commissioner is accordingly entitled to issue a monetary penalty in this case.
49. The Commissioner has considered whether, in the circumstances, she should exercise her discretion so as to issue a monetary penalty. She has taken into account representations dated 5 April 2018 made in response to the Notice of Intent and in other correspondence on this matter.
50. The Commissioner has concluded that it is appropriate for her to exercise her discretion in favour of issuing a monetary penalty in the circumstances. The contravention is serious in terms of both GC's

deficiencies and the impact such deficiencies were likely to have on the affected individuals.

51. 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.

The amount of the penalty

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

- GC recognised its error and initiated prompt action to remedy the problem;
- GC has apologised to the affected individuals.
- GC self-reported the incident and fully co-operated with the ICO during its investigation;
- GC referred to officer involved to its professional standards department;
- Some of the recipients of the email were already known to each other via social networking and the media;
- The issuing of a penalty may result in a loss of trust by victims of crime who may be reluctant to report crimes of a similar nature;
- GC is in the process of improving its technical and organisational measures in order to prevent a similar occurrence in the future.

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

- Some of the affected individual's right to anonymity for life has been removed by this incident;
 - There is no guarantee that the information has been recovered in full;
 - An ICO Audit in 2014 provided a limited assurance rating, and highlighted concerns about the quality, standard and content of training on certain key systems. This incident can be partially attributed to lack of policies and poor standards and inconsistency in relation to the provision of staff training;
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. 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

56. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **12 July 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.
57. If the Commissioner receives full payment of the monetary penalty by **11 July 2018** the Commissioner will reduce the monetary penalty by 20% to **£64,000 (Sixty four thousand pounds)**. However, you

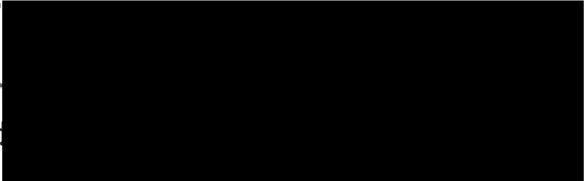
should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

58. 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.
59. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.
60. Information about appeals is set out in Annex 1.
61. 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.
62. 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 11th day of June 2018

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 (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)).