Information Commissioner's Office

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Gloucester City Council

Of: Herbert Warehouse, The Docks, Gloucester GL1 2EQ

1. The Information Commissioner ("Commissioner") has decided to issue Gloucester City Council ("Gloucester") 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 Gloucester.

2. This notice explains the Commissioner's decision.

Legal framework

3. Gloucester 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. From 7 April 2014, a vulnerability known as 'Heartbleed' received widespread publicity in the media. On the same date, a new version of the affected software ('OpenSSL') was released which fixed the flaw.

10. On 17 April 2014, Gloucester's IT staff identified the Heartbleed vulnerability in its own systems as it was using an appliance known as 'SonicWall' which contained an affected version of OpenSSL. By that

time, a patch for the affected software was available. Gloucester intended to apply the patch in accordance with its update policy.

11. However, Gloucester was in the process of outsourcing its IT services to a third party company on 1 May 2014, and updating the software to address the vulnerability was overlooked.

12. On or about 22 July 2014, Gloucester sent an email to its staff warning them that Twitter accounts belonging to senior officers at Gloucester had been compromised by an attacker.

13. The same attacker responded to this email by stating that he had also gained access to 16 users' mailboxes via the Heartbleed vulnerability in the SonicWall appliance that was used for routing traffic to Gloucester's services.

14. In particular, the attacker was able to download over 30,000 emails from (among others) [redacted] officer's mailbox.

15. The emails contained financial and sensitive personal information relating to between 30 to 40 former or current staff, [redacted]

16. The attacker claimed to be a member of the 'Anonymous' group. This group is known for a series of publicity stunts and denial of service attacks on government, religious, and corporate websites.

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

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

The contravention

19. The Commissioner finds that Gloucester contravened the following provisions of the DPA:

20. Gloucester failed to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data in contravention of the seventh data protection principle at Part I of Schedule 1 to the DPA.

21. The Commissioner finds that the contravention was as follows. Gloucester did not have in place appropriate technical and organisational measures for ensuring so far as possible that such an incident would not occur, i.e. for ensuring that emails containing financial and sensitive personal information could not be accessed.

22. In particular, Gloucester did not have a process in place to ensure that during outsourcing of its IT services, the patch for the Heartbleed flaw was applied at the appropriate time.

23. This was an ongoing contravention from 8 April 2014 when a patch for the affected software was available, until Gloucester took remedial action on 22 July 2014.

24. The Commissioner is satisfied that Gloucester was responsible for this contravention.

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

Seriousness of the contravention

26. The Commissioner is satisfied that the contravention identified above was serious due to the number of affected individuals, the nature of the data that was contained in the emails and the potential consequences. In those circumstances, Gloucester's failure to take adequate steps to safeguard against unauthorised or unlawful access 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 damage or substantial distress

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

29. The attacker was able to download over 30,000 emails from (among others) [redacted] officer's mailbox. The emails contained financial and sensitive personal information relating to between 30 to 40 former or current staff, [redacted]. The personal data that was obtained was clearly of interest to the attacker given the targeted nature of the attack. The mailboxes therefore required adequate security measures to protect the personal data contained in the emails.

30. This is all the more so when financial and sensitive personal information is concerned – in particular, as regards former or current

staff who expected that it would be held securely. This heightens the need for robust technical and organisational measures to safeguard against unauthorised or unlawful access. For no good reason, Gloucester appears to have overlooked the need to ensure that it had robust measures in place to ensure that the patch was applied, despite contracting with a third party company that could have applied the patch before the attack.

31. The Commissioner therefore considers that, by reference to the features of the contravention, it was of a kind likely to cause distress to Gloucester's former and current staff if they knew that their financial and sensitive personal information [redacted] have been accessed by an unauthorised third party who claimed to be a member of the Anonymous group.

32. Further, Gloucester's former and current staff would be distressed by justifiable concerns that this information would be further disseminated even if those concerns do not actually materialise.

33. In this context it is important to bear in mind that the attacker has not been identified and the emails have not been recovered.

34. If this information has been misused by the person who had access to it, or if it was in fact disclosed to untrustworthy third parties, then the contravention would cause further distress to Gloucester's former and current staff and damage, [redacted].

35. The Commissioner therefore considers that, by reference to the features of the contravention, it was of a kind likely to cause damage and distress.

36. The Commissioner considers that such damage or distress is likely to be substantial having regard to the number of affected individuals and the nature of the data contained in the emails.

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

Deliberate or foreseeable contravention

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

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

40. The Commissioner has gone on to consider whether Gloucester 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 Gloucester was aware of the nature of the data contained in the emails.

41. Gloucester's IT staff had identified the Heartbleed vulnerability in its own systems and they knew that a patch for the affected software was available. The vulnerability also received widespread publicity in the media. On 13 May 2014, the ICO issued a blog with the title

'Heartbleed and the importance of encrypting internet traffic'.

42. In the circumstances, Gloucester ought reasonably to have known that there was a risk that that such an attack would occur unless it ensured that the mailboxes were appropriately protected.

43. Second, the Commissioner has considered whether Gloucester knew or ought reasonably to have known that there was a risk the contravention would be of a kind likely to cause substantial damage or substantial distress.

44. Gloucester ought to have known that it would cause substantial damage and substantial distress to the affected individuals if the information was accessed by an unauthorised third party who claimed to be a member of the Anonymous group.

45. Therefore, it should have been obvious to Gloucester that such a contravention would be of a kind likely to cause substantial distress to the affected individuals and damage, [redacted].

46. Third, the Commissioner has considered whether Gloucester 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 entailed having a process in place to ensure that during the outsourcing of its IT services, the patch for the Heartbleed flaw was applied at the appropriate time. Gloucester did not take that step. The Commissioner considers there to be no good reason for that failure.

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

The Commissioner's decision to impose a monetary penalty

48. For the above reasons, the Commissioner considers there to have been a serious contravention of the seventh data protection principle on the part of Gloucester with respect to the personal data that was contained in the emails. The contravention was of a kind likely to cause substantial damage and substantial distress. Gloucester knew or ought to have envisaged those risks and it did not take reasonable steps to prevent the contravention. The conditions for issuing a monetary penalty are met in this case.

49. 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 dated 16 December 2016, in which the Commissioner set out her preliminary thinking.

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. She has taken into account the representations made in response to the Notice of Intent and in other correspondence on this matter.

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

54. 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 Gloucester's deficiencies and the impact such deficiencies were likely to have on the affected individuals.

55. 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.

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

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

- Gloucester's website was subjected to a criminal attack.
- Gloucester reported this incident to the Commissioner and was co-operative during her investigation.
- Gloucester has taken substantial remedial action.
- A monetary penalty may have a significant impact on Gloucester's reputation (and to some extent) its resources.

58. The Commissioner has taken into account the following **aggravating feature of this case:**

- Gloucester was not aware of this incident until 22 July 2014 when it was notified by the attacker.
- The attacker had the opportunity to download even more emails if he had chosen to do so.

59. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the DPA and this is an opportunity to remind data controllers to ensure that appropriate and effective security measures are applied to personal data.

60. Taking into account all of the above, the Commissioner has decided that the appropriate amount of the penalty is **£100,000 (One hundred thousand pounds)**.

Conclusion

61. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **28 June 2017** 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.

62. If the Commissioner receives full payment of the monetary penalty by **27 June 2017** the Commissioner will reduce the monetary penalty by 20% to **£80,000 (Eighty thousand pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

63. 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.

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

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

66. 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.

67. 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 May 2017

Signed [redacted]

Stephen Eckersley
Head of Enforcement
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Information Commissioner's Office

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)).