

**DATA PROTECTION ACT 1998**

**SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER**

**MONETARY PENALTY NOTICE**

To: Bupa Insurance Services Limited

Of: 1, Angel Court, London EC2R 7HJ

**Introduction**

1. Bupa Insurance Services Limited ("the data controller") manages domestic and global insurance policies. Bupa Global customers are able to access healthcare services in more than one country, and typically work abroad or travel on a regular basis.
2. The Information Commissioner ("the Commissioner") has decided to issue the data controller with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA").
3. The amount of the monetary penalty is **£175,000**.
4. The monetary penalty concerns Bupa Global's customer relationship management system ("SWAN") which holds customer records relating to 1.5 million data subjects. SWAN is used to manage claims made by Bupa Global customers under their international health insurance policies.

5. The data controller authorised 20 users working in its Partnership Advisory Team ("PAT members") and 1,351 other users to have access to SWAN, based on the individual user's business function.
6. On 16 June 2017, it was discovered that personal data of Bupa Global's customers was being offered for sale on the dark web. A PAT member in Bupa Global's Brighton office ("AA") was subsequently discovered to have made unauthorised use of personal data accessed via SWAN to do this.
7. For the reasons set out below, the Commissioner considers that the data controller failed to take appropriate technical and organisational measures against unauthorised and unlawful processing of the personal data which was accessible through SWAN.
8. The Commissioner's view is that, in all the circumstances, this failure constituted a serious contravention by the data controller of the seventh data protection principle ("DPP7") from Schedule 1 to the DPA. The Commissioner further considers that the conditions for issuing a monetary penalty are satisfied, that it is appropriate to issue such a penalty in this case, and that the amount of £175,000 is reasonable and proportionate.
9. This Notice of Intent is served under section 55B of the DPA. It explains the grounds on which the Commissioner has issued the monetary penalty.

### **Legal framework**

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 DPA must be applied so as to give effect to that Directive.

11. Bupa Insurance Services Limited is a data controller of its customers' 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.
12. Schedule 1 of the DPA contains the eight data protection principles. In the present case, the relevant principle is DPP7, which stipulates as follows:

*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.*

13. As regards DPP7, the 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.*

14. Section 55A of the DPA empowers the Commissioner to issue monetary penalties. The relevant provisions are as follows:

*(1) 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) 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.*

15. 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.
16. The Commissioner has issued and published statutory guidance under section 55C (1) of the DPA about the issuing of monetary penalties.

### **Background to the contravention**

17. At the relevant time for the purposes of this Notice of Intent, 20 PAT members and 1,351 other users were provided with access to SWAN, based on the individual user's business function.
18. For the purposes of this Notice, the affected personal data comprised, for each data subject: name, date of birth, nationality, administrative information for the policy and its beneficiaries including membership number, email address, phone and fax number, but not any medical information. This is referred to below as "the relevant personal data".

19. Bupa Global had approximately 1.5 million customers with international health insurance policies at the relevant time.
20. 20 PAT members were authorised to make searches, view customer data and run reports from SWAN without restriction. SWAN reports could then be downloaded and held on shared drives and personal drives in order to respond to broker enquiries on a 'first time resolution' basis. This illustrates the tension between customer satisfaction and information security.
21. At the relevant time, the data controller did not routinely monitor SWAN's activity log. It was therefore unaware that the log had a defect which resulted in certain reports not being logged, and other reports being logged inaccurately. Therefore the data controller was unable to detect any unusual activity in SWAN, such as bulk extractions of data.
22. On 16 June 2017, a staff member in Bupa Global was informed by an external partner that the customer data of an international health insurer was being offered for sale on the popular dark web site, AlphaBay Market which was accessed via the onion routing ("Tor"), for anonymous communications. It was reported to have over 400,000 users.
23. The advertisement stated:

*DB [database] full of 500k+ Medically insured persons info from a well-known international blue chip Medical Insurance Company. Data lists 122 countries with info per person consisting of Full name, Gender, DOB, Email Address plus Membership Details excluding CC Details.*
24. A sample of the data was provided to the data controller which was revealed to be identical to that held on SWAN.

25. On 17 June 2017, the data controller began an investigation, convened a Crisis Management Team and engaged specialist advisors.
26. Between 6 January and 11 March 2017, AA had exfiltrated the relevant personal data of 547,000 data subjects (108,000 Bupa Global policy holders and policy beneficiaries) by generating bulk data reports from SWAN, attaching the data to six emails in zip files and sending it to his personal account. This was the data that was offered for sale on the dark web.
27. In addition to the zip files, there were two other excel files attached to emails sent to AA's personal account. These files contain records relating to a non-UK hospital showing the amount of treatment and dates relating to 36 data subjects (11 of whom appear in the relevant personal data set), but not including any medical information.
28. Between 19 December 2013 and 18 January 2017, AA also saved three more data sets to his desktop likely to have been copied from mandate forms, including credit card details for 15 data subjects (13 of whom appear in the relevant personal data set). However, there is no evidence that it was exfiltrated from the data controller's systems.
29. On 18 and 19 June 2017, the data controller informed the ICO, the Financial Conduct Authority and Sussex police. At the same time, the data controller also took steps to block AA's log-in details and account so that AA could not access Bupa's network and SWAN system. On 19 June 2017, AA was suspended. On 20 June 2017, the data controller commenced injunction proceedings against AA. On 22 June 2017, the Prudential Regulation Authority was also informed.
30. The data controller then progressed its internal investigations with assistance from external advisers. On 10 July 2017, the data controller

introduced additional internal security measures and increased its customer identity checks to prevent fraud.

31. On 12 July 2017, the data controller began a communication programme to alert all of its customers to the potential for scam messages and calls. A customer information page on the data controller's website went live. The data controller received approximately 191 complaints from Bupa Global customers about this incident.
32. The Commissioner's office has also received seven complaints from Bupa Global customers.
33. On 20 July 2017, AlphaBay Market was shut down by US authorities.
34. In August 2017, the data controller appointed a professional services firm to carry out an independent, external review of this incident. The review found that at the time of the incident, the data controller's security controls to protect customer data against the threat of a rogue employee were weak.
35. The Commissioner investigated this incident. The outcome of this investigation is as follows.

### **The contravention**

36. Based on the factual matters set out above, the Commissioner's view is that, at the relevant time (i.e. at least 19 December 2013 to 18 June 2017), the data controller contravened DPP7 in respect of SWAN, in that:

- (1) As described above, the data controller provided 20 PAT members and 1,351 other users with access to large volumes of its customers' personal data through SWAN. It did not undertake any adequate risk assessment of those features of SWAN. That was a material organisational inadequacy, given the volume of personal data accessible through SWAN, the number of data subjects involved, the number of individuals with access to SWAN, and the ease with which they could access it.
  - (2) 20 PAT members were also able to make searches, view large numbers of customer records at a time and export data to separate applications and files including file sharing platforms and social media. Those capabilities facilitated potential large-scale misuse of the relevant personal data over a short period of time. There was no adequate justification for those capabilities.
  - (3) The data controller failed to monitor its activity log (which was defective) in order to check for activity of concern, such as bulk extractions of data.
37. Having regard to the state of technological development, the cost of implementing any measures, the nature of the relevant personal data and the harm that might ensue from its misuse, the Commissioner's view is that the data controller contravened DPP7 in respect of the arrangements applicable to SWAN at the relevant time.

### The issuing of a monetary penalty



38. The Commissioner's view is that the conditions for issuing a monetary penalty under section 55A have been met in this case.
39. The Commissioner considers that this contravention was serious, in that:
- (1) The contravention comprised a number of material inadequacies in the data controller's technical and organisational measures for the safeguarding of the relevant personal data: see paragraph 18 above.
  - (2) The Commissioner has seen no satisfactory explanation for those inadequacies.
  - (3) Those inadequacies were systemic, rather than arising from any specific incident or incidents.
  - (4) Those systemic inadequacies appear to have been in place for a long period of time without being discovered or addressed.
  - (5) Those inadequacies put the personal data of up to 1.5 million data subjects at risk.
  - (6) 1,371 SWAN users had access to the relevant personal data. There were thus a great number of opportunities for those inadequacies to be exploited and the relevant personal data to be misused.
  - (7) Large volumes of personal data were accessed and could be exported swiftly by 20 PAT members, from the SWAN system to any device.

- (8) The relevant personal data was of a type that can be useful to scammers and fraudsters.

40. The Commissioner considers that this contravention was of a kind likely to cause substantial damage or substantial distress, in that:

- (1) In light of the inadequacies outlined above, some of the relevant personal data was a type of information that could be used in furtherance of fraud and/or other criminal activity. The relevant personal data was likely to help scammers (a) identify and contact target individuals and (b) pass themselves off as representatives of the data controller.
- (2) Any such communications that were made would be likely to result in at least some recipients providing their bank details to scammers and/or being defrauded and/or having their bank accounts used for money laundering. Those consequences would constitute substantial damage if they arose.
- (3) Any such communications that were made would also be likely to cause substantial distress to at least some recipients, whether individually or cumulatively. Recipients would know that their personal data may have been stolen or misused and would be aware of how this may have happened due to the information contained in the data controller's communications to its customers about the incident. They would be uncertain about how it might adversely affect them, particularly in the context of the dark web which can facilitate anonymous communications and disguise criminal activity. Substantial distress was very likely in these circumstances.

41. The Commissioner considers that the data controller knew or ought reasonably to have known that there was a risk that the contravention would (a) occur, and (b) be of a kind likely to cause substantial damage or substantial distress. She further considers that the data controller failed to take reasonable steps to prevent such a contravention, in that:

- (1) Bupa Insurance Services Limited is a large, well-resourced and experienced data controller. It should have been aware of the risks entailed by the use of SWAN as outlined above. It should have appreciated that misuse of the relevant personal data was likely to cause substantial damage or distress.
- (2) The data controller was also aware of internal security risks to SWAN i.e. unauthorised use of customer data accessed through SWAN. The threat of a rogue employee is widely recognised in industry. This is also evident, for example, from aspects of the data controller's domestic customer relationship management system ("SWIFT ") which contains 2.3 million customer records. SWIFT does not permit the generation of reports directly from the system by Intermediary Team members. It also had a functioning system for recording accurate activity logs of the reports generated from a separate system called Cognos. Those aspects show that the data controller was mindful of the need to prevent unauthorised use.
- (3) The data controller should have been aware of the increasing prevalence of scams and attempted frauds, as reported in the media and by bodies such as Financial Fraud Action UK. The

data controller should have assessed the technical and organisational measures pertaining to SWAN in light of those increased risks.

- (4) The data controller had ample opportunity over a long period of time to implement appropriate technical and organisational measures in respect of SWAN, but it failed to do so. For example, it failed to take steps to prevent the large-scale accessing and exporting of the relevant personal data from SWAN.
- (5) The data controller failed to undertake an adequate risk assessment of the use of SWAN: see paragraph 36(1) above.
- (6) The data controller failed to monitor its activity log (which was defective) in order to check for activity of concern, such as bulk extractions of data.

#### **The Commissioner's decision to impose a monetary penalty**

42. The Commissioner has concluded that the conditions for issuing a monetary penalty are in place. She has considered whether it is appropriate for her to exercise her discretion in favour of issuing a monetary penalty in this case. Her conclusion is that it is appropriate to do so in all the circumstances. That view is based on the multiple, systemic and serious inadequacies identified above, and on the data controller's inadequate response to the resultant risks prior to June 2017 (see for example paragraph 45 below).
43. The issuing of a monetary penalty in this case would be fair and just and 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.

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

- The relevant personal data was not of itself highly sensitive in terms of its impact on data subjects' privacy;
- The affected data subjects, as well as the data controller, have been the victim of the malicious actions of one individual acting in contravention of the data controller's policies;
- The rogue employee was dismissed, and Sussex police has issued a warrant for his arrest regarding an offence under section 55 DPA, although his current whereabouts are unknown;
- The data controller proactively reported this matter to the Commissioner and other relevant regulators;
- The data controller took steps to minimise potentially harmful consequences and has treated this incident very seriously;
- There is no evidence that the relevant personal data was in fact used for successful fraud activities;
- There is no evidence that the relevant personal data was sold to any unknown third party;
- This incident has been widely publicised in the media;
- Bupa has agreed to participate in the ICO's annual audit program;
- The data controller has now implemented certain measures to prevent the recurrence of such incidents. These measures in part reflected the

recommendations made following the external investigation commissioned by the data controller.

45. The Commission has also taken into account the following aggravating features of this case:

- Up to 1.5 million data subjects' personal data was put at risk;
- Those risks appear to have persisted for a long period of time;
- While additional controls were promptly put in place by the data controller which would prevent a reoccurrence of the data breach caused by AA, 100 days after the incident it was still possible for a rogue employee to exfiltrate personal data from the data controller's systems through other means.

### **Conclusion and amount of penalty**

46. The Commissioner confirms that she has taken account of the data controller's written submissions in response to her Notice of Intent.

47. Notwithstanding those submissions, the Commissioner has decided that she can and should issue a monetary penalty in this case, for the reasons explained above.


48. The Commissioner has also taken into account her underlying objective in imposing a monetary penalty notice, namely 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.

49. She considers that, given the nature, seriousness and potential consequences of the contravention arising in this case, that objective would not be adequately served by an unduly lenient penalty.
50. The Commissioner has considered evidence of the data controller's financial position. She does not consider that the payment of a penalty of the above amount would cause the data controller undue hardship.
51. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of **£175,000 (One hundred and seventy five thousand pounds)** is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.
52. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **29 October 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.
53. If the Commissioner receives full payment of the monetary penalty by **26 October 2018** the Commissioner will reduce the monetary penalty by 20% to **£140,000 (One hundred and forty thousand pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.
54. 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.
55. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.
56. Information about appeals is set out in Annex 1.
57. 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.
58. 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 26<sup>th</sup> day of September 2018



Stephen Eckersley  
Director of Investigations  
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)).