

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: TalkTalk Telecom Group PLC

Of: 11, Evesham Street, London W11 4AR

1. The Information Commissioner ("the Commissioner") has decided to issue TalkTalk Telecom Group PLC ("TalkTalk") with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA").
2. This amount of the monetary penalty which the Commissioner has decided to issue is £100,000.
3. The monetary penalty concerns customer personal data that could be accessed through a web-based platform ("portal").
4. In 2004, TalkTalk provided Wipro Limited ("Wipro"), a multinational IT services company, with access to that portal. In late-2014, three of Wipro's employees misused their access to the portal.
5. For the reasons set out below, the Commissioner considers that TalkTalk failed to take appropriate technical and organisational measures against unauthorised and unlawful processing of the personal data which could be accessed through the portal.

6. The Commissioner's view is that, in all the circumstances, this failure constituted a serious contravention by TalkTalk 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 £100,000 is reasonable and proportionate.

Legal framework

7. 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.
8. TalkTalk 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.
9. Schedule 1 to the DPA contains the eight data protection principles. In the present case, the relevant principle is DPP7, which stipulates as follows:

"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".

As regards DPP7, the interpretative provisions in paragraph 9 at Part II of Schedule 1 to the DPA provide 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".

10. Section 55A (1) of the DPA empowers the Commissioner to issue monetary penalties. The Commissioner may serve a data controller with a monetary penalty notice if she 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.

11. 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.
12. 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

13. TalkTalk's portal was designed and implemented in 2002. Wipro was provided with access to the portal, acting as a data processor to resolve high level complaints and monitor and address network connectivity problems on TalkTalk's behalf. This service fulfilled both a business and a regulatory need for Talktalk (the later comprising obligations under the Communications Act 2003, as enforced by Ofcom).
14. The portal was accessed by entering valid user names and passwords into a website with a publicly available URL. This was to ensure that Wipro could address network coverage problems quickly. 40 individual users employed in Wipro's High Repeat Team had access to the personal data of between 25,000 to 50,000 TalkTalk customers at any

point in time. TalkTalk retained administrative control over those user accounts.

15. For the purposes of this Monetary Penalty Notice, the affected personal data comprised, for each customer: name; address; telephone number and TalkTalk account number. This is referred to below as “the relevant personal data”.
16. Wipro employees with access to the portal were able to: log in to the portal from any computer (i.e. not only from work devices); to carry out “wildcard” searches (for example, by entering “A*” into the surname field, which would then return all surnames beginning with A); view up to 500 customer records at a time, and export data to separate applications and files so that regulatory reports could be produced.
17. In September 2014, TalkTalk began receiving complaints from customers regarding scam calls purportedly from TalkTalk. Typically, the callers purported to be providing support for technical problems which had been detected. They were able to quote customers’ addresses and TalkTalk account numbers.
18. TalkTalk commenced an initial security investigation and reported the matter to the Commissioner on 11 September 2014.
19. In October 2014, TalkTalk commissioned a specialist investigation which identified three Wipro user accounts that had been used to gain unauthorised and unlawful access to the relevant personal data of up to 21,000 customers.

20. However, there was no evidence of a causal link between the complaints referred to in paragraph 17 above and these incidents.
21. In November 2014, and in February, October and November of 2015, TalkTalk wrote to all of its customers warning them of potential scam calls and how to deal with them.
22. TalkTalk provided the Commissioner with more detailed notifications about this matter on 20 February, 10 March and 15 July 2015. The Commissioner investigated. The outcome of this investigation is as follows.

The contravention

23. Based on the factual matters set out above, the Commissioner's view is that TalkTalk contravened DPP7 in respect of the portal. In short, unjustifiably wide-ranging access to the relevant personal data by external agents put that data at risk. In particular:
 - (1) As described above, TalkTalk provided 40 Wipro employees with access to the relevant personal data of between 25,000 to 50,000 through the portal. No controls were put in place to limit access to the customers whose accounts were being worked on to resolve network problems, or to allow for the exporting of the fields that were actually needed for Ofcom reporting.
 - (2) The Wipro employees were able to access the portal from any internet-enabled device. No controls were put in place to restrict such access to devices linked to Wipro.

- (3) The Wipro employees were able to make “wildcard” searches, view large numbers of customer records at a time and to export data to separate applications and files (although there is no evidence of any bulk download of this data). Those capabilities exacerbated opportunities for the misuse of the relevant personal data. There was no adequate justification for those capabilities.
24. 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 TalkTalk contravened DPP7 in respect of the arrangements applicable to the portal.
25. This was an ongoing contravention from 2004 when Wipro was provided with access to the portal, until 2014 when remedial action was taken by TalkTalk following these incidents.

The issuing of a monetary penalty

26. The Commissioner’s view is that the conditions for issuing a monetary penalty under section 55A have been met in this case.
27. The Commissioner considers that this contravention was serious, in that:
- (1) The contravention comprised a number of material inadequacies in TalkTalk’s technical and organisational measures for the safeguarding of the relevant personal data: see paragraph 23 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 relevant personal data of between 25,000 to 50,000 customers at risk.
 - (6) 40 Wipro employees 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) The relevant personal data of up to 21,000 customers was accessed and could be exported swiftly, from and to any device (although there is no evidence of any bulk download of this data).
 - (8) The relevant personal data was useful to scammers and fraudsters (although there is no evidence that any data was passed to fraudsters or any other third parties as a result of these incidents).
28. 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 likely to be misused 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 TalkTalk.
 - (2) Such communications were 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.
 - (3) Such communications were also likely to cause substantial distress to at least some recipients, whether individually or cumulatively. At least some recipients would realise that their personal data had been stolen or misused. They would be uncertain about how that had occurred and how it might adversely affect them. Substantial distress was very likely in these circumstances.
29. The Commissioner considers that TalkTalk 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 TalkTalk failed to take reasonable steps to prevent such a contravention, in that:
- (1) TalkTalk is a large, well-resourced and experienced data controller. It should have been aware of the risks entailed by the use of its portal as outlined above. It should have

appreciated that misuse of the relevant personal data was likely to cause substantial damage or distress.

- (2) The specific internal security risk in respect of the portal should have been obvious to TalkTalk given that the portal's functionality allowed Wipro's employees to search any of its customers' relevant personal data, including via wildcard searches and export the data in bulk.
- (3) TalkTalk 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. TalkTalk should have assessed the technical and organisational measures pertaining to the portal in light of those increased risks.
- (4) TalkTalk had ample opportunity over a long period of time to implement appropriate technical and organisational measures in respect of the portal, but it failed to do so. For example, it failed to ensure that the portal could only be accessed from authorised devices (whether on or off site); and failed to take steps to prevent large-scale accessing and exporting of the relevant personal data through the portal.

The Commissioner's decision to impose a monetary penalty

- 30. The Commissioner's view is therefore that the statutory conditions for issuing a monetary penalty have been met in this case. She has considered all the circumstances and has reached the view that it is appropriate to issue a monetary penalty in this case.

31. That view is based on the multiple, systemic and serious inadequacies identified above. The Commissioner has also considered the importance of deterring future contraventions of this kind, both by TalkTalk and by others. The Commissioner considers that the latter objective would be furthered by the issuing of a monetary penalty in this case.
32. The Commissioner has taken into account the following **mitigating features** of this case:
- TalkTalk has been the victim of the malicious actions of a small number of individuals;
 - TalkTalk proactively reported this matter to the Commissioner;
 - TalkTalk took steps to minimise potentially harmful consequences, for example by immediately removing the offending Wipro employees' access to the portal and alerting all of its customers to the potential for scam calls;
 - There is no evidence that the affected customers (up to 21,000) suffered any damage or distress as a result of these incidents;
 - TalkTalk has implemented certain measures to prevent the recurrence of such incidents.
33. The Commissioner has considered evidence of TalkTalk's financial position. She does not consider that the payment of a penalty of the above amount would cause TalkTalk undue hardship.
34. 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 reinforce the need for data


controllers to ensure that appropriate and effective security measures are applied to personal data.

Conclusion and amount of penalty

35. The Commissioner confirms that she has taken account of TalkTalk's written and oral submissions in response to her Notice of Intent.
36. Notwithstanding those submissions, the Commissioner has decided that she can and should issue a monetary penalty in this case, for the reasons explained above.
37. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of **£100,000 (One hundred thousand pounds)** is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.
38. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **7 September 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.
39. If the Commissioner receives full payment of the monetary penalty by **6 September 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.
40. 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.
41. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.
42. Information about appeals is set out in Annex 1.
43. 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.
44. 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 7th day of August 2017

Signed 

Elizabeth Denham
Information Commissioner
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)).