

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Uber B.V.

Of: Mr. Treublaan 7, 1097 DP, Amsterdam, The Netherlands.

And: Uber London Limited

Of: Aldgate Tower, First Floor, 2 Leman Street, London E1 8FA.

And: Uber Britannia Limited

Of: Aldgate Tower, First Floor, 2 Leman Street, London E1 8FA.

And: Uber Scot Limited

Of: 93 George Street, Edinburgh, Scotland, EH2 3ES.

And: Uber NIR Limited

Of: Aldgate Tower, First Floor, 2 Leman Street, London E1 8FA.

Introduction

1. The Information Commissioner ("the Commissioner") has decided to issue Uber B.V. ("Uber BV"); and Uber London Limited; Uber Britannia Limited; Uber Scot Limited; and Uber NIR Limited (collectively "Uber UK") (Uber BV and Uber UK together, "Uber"), with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA") because of a serious contravention of the seventh data protection principle ("DPP7") from Schedule 1 DPA.

2. The amount of the monetary penalty which the Commissioner intends to issue is £385,000.

Legal framework

3. 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.
4. The DPA applies to data controllers. Section 1 of the DPA provides that:

(1) 'data controller' means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

...

5. Section 5 of the DPA provides that:

(1) Except as otherwise provided by or under section 54, this Act applies to a data controller in respect of any data only if—
(a) the data controller is established in the United Kingdom and the data are processed in the context of that establishment,

...

(3) For the purposes of subsections (1) and (2), each of the following is to be treated as established in the United Kingdom—

...

(d) any person who does not fall within paragraph (a), (b) or (c) but maintains in the United Kingdom—
(i) an office, branch or agency through which he carries on any activity, or
(ii) a regular practice;
and the reference to establishment in any other EEA State has a corresponding meaning.

6. The Commissioner's view is that Uber BV is a joint data controller within the EU, together with at least Uber UK, of the personal data of at least the users of Uber's services in the UK, and that it is established in the United Kingdom, pursuant to section 5(3)(d) of the DPA:
- (1) Its four affiliates, Uber London Limited, Uber Britannia Limited, Uber Scot Limited and Uber NIR Limited, are located in the United Kingdom;
 - (2) Uber UK carries out activities in the United Kingdom, including sales and marketing activities to UK customers, and data processing activities which are jointly determined by Uber UK and Uber BV. The Commissioner considers they are data controllers, and refers in this regard to the findings of the Court of Justice of the European Union ("CJEU") in Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* EU:C:2018:388, paragraph 64; and
 - (3) Uber BV exercises real and effective activities in the United Kingdom with and through Uber UK, under stable arrangements, and data is processed in the context of those activities and those arrangements. The Commissioner refers, in this regard, to the findings of the CJEU in Case C-131/12 *Google Spain v AEPD* EU:C:2014:317, paragraphs 55 et seq.
7. 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.

8. 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.

9. 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.*

(10) The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

(11) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle—

- (a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and*
- (b) take reasonable steps to ensure compliance with those measures.*

(12) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless—

- (a) the processing is carried out under a contract—
 - (i) which is made or evidenced in writing, and*
 - (ii) under which the data processor is to act only on instructions from the data controller, and**

(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

10. 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.

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. Uber is a global transport network company. It operates through a mobile telephone application ("the App"), which permits registered users to make requests for trips which are matched to nearby drivers

on the App. The relevant companies within the group for the purposes of this Notice are:

- (1) The ultimate parent company, Uber Technologies Inc. ("Uber US"), is based in California, USA;
 - (2) The four Uber UK affiliate companies listed in paragraph 7(1) above, through which Uber BV is established in the United Kingdom;
 - (3) Uber BV, which is based in the Netherlands. Uber BV is wholly owned by Uber International BV, which in turn is wholly owned by Uber International CV and the latter is owned by Uber US (99%) and Neben LLC (1%), with Neben LLC being wholly owned by Uber US.
14. This Notice concerns the cloud-based storage service, Amazon Web Service's Simple Storage Service ("S3"). S3 enables businesses to store large quantities of data in a collection of cloud-based 'buckets'.
15. Personal data belonging to individuals in the UK was transferred to Uber US by Uber BV pursuant to a Data Processing Agreement dated 31 March 2016 and a Support Services Agreement between Uber US and Uber BV dated 1 January 2014. Uber US, which serves as a processor to Uber BV and Uber UK with respect to the data of UK riders and drivers, then used S3, as well as other systems, to store that data.
16. Over the period 13 October - 15 November 2016, Uber US's stored data in a set of Uber US's buckets on S3 was subject to an external cyberattack. The attackers obtained Amazon IAM credentials for an Uber US service account known as [REDACTED], through which they were able to access files in Uber US's S3 datastore.

17. The [REDACTED] credential was contained in a piece of code located in Uber US's private repository on GitHub. The attackers told Uber US that they accessed the GitHub repository using username and password pairs from other accounts (not on the Uber network) which had previously been breached. The Commissioner's view, based on her analysis of information provided by Uber and other sources, is that the attackers did this by 'credential stuffing': a process by which the compromised username and password pairs are injected into websites until they are matched to an existing account, which is then hijacked for fraudulent purposes. The attackers told Uber that they had identified the passwords for the GitHub accounts belonging to 12 of Uber US' employees.

18. Having accessed parts of Uber US's S3 datastore, the attackers downloaded the contents of 16 files. Outside counsel for Uber US has commissioned a report by a forensic IT consultant, Mandiant, which identifies the following personal data belonging to individuals in the UK as having been contained in those files:
 - (1) Records for approximately 32 million non-US users, of whom some 2.7 million users were based in the UK. These included: full name, mobile phone number, email address, and 'initial sign-up location' data for those users who had switched on the location data functionality, as reflected in Uber's files on 24 June 2015. They also included salted and hashed versions of some then-current, and some previous, user passwords, in a file last updated on 20 August 2015.

 - (2) Records for approximately 3.7 million non-US drivers, of whom approximately 82,000 were based in the UK. These included, in some instances, drivers licence numbers, although Uber BV has

confirmed that only 2 records pertaining to UK drivers contained an entry in this field. They also included summaries of the rides provided by the drivers, such as how much drivers were paid over a week, a summary on a trip by trip basis, the type of ride, and when the invoice was created.

19. S3 was used at the relevant time to store more data than described in paragraph 19 above, including, potentially, additional personal data. The [REDACTED] credential could access over 100 buckets within S3. Some of the information in these buckets was accessible to the attackers during the attack. Although there is no evidence that any information which was accessible through the [REDACTED] credential was in fact accessed other than the 16 downloaded files, Uber BV has not identified for the Commissioner the information which was accessible in those buckets but not in fact accessed (ie the contents of any file other than the 16 which were in fact accessed) because (1) given the passage of time, it is not possible now to identify definitively the contents of files that may have been accessible at the time of the incident and (2) Uber's view is that reviewing the current files in those buckets is practically infeasible. Uber does not hold a record of all information it stored on the S3 system at every point in time. The Commissioner notes that it is poor data protection practice to be unable or unwilling to identify whether and what personal data is contained in those buckets. Given the huge volume of data contained in those buckets it is highly likely that they contained some personal data.
20. The attackers alerted Uber US on 14 November 2016 to the breach. They demanded a payment of at least \$100,000 to reveal how they had accessed the S3 accounts (although they later revealed this information in advance of any payment), and also implied that they

would not destroy the data they had downloaded until the monies were received.

21. In response to the attackers' communications, Uber US:

(1) took steps to put an end to the attack by rotating the compromised key found in GitHub that provided access to S3, including the compromised [REDACTED] service account, and requiring two-factor authentication for access to its private GitHub repositories;

(2) paid the attackers the sum of \$100,000, through the third party that administers Uber's "bug bounty" programme. This programme invites outside information security experts to search for vulnerabilities in Uber's systems and disclose the method of compromise to Uber, in exchange for a reward; and

(3) obtained assurances from the attackers that the downloaded data had been destroyed.

22. Since the attack, a number of additional security measures have been completed, including the introduction of a new key management system for credentials that access S3; the migration of source code from GitHub to internal code repositories (with limited exceptions for things like open source code); the adoption of multi-factor authentication for programmatic service account access to the S3 datastore to augment the previously existing multi-factor authentication for individual account access to the S3 datastore; and ongoing work to implement two-factor authentication on [REDACTED].

23. The Commissioner has based her synopsis of this cyberattack on the account provided by Uber, and on the report of Mandiant prepared on

behalf of Uber US, as well as her independent knowledge of 'credential stuffing' attacks.

The contravention: DPP7

24. The material submitted by Uber, including the Mandiant report and the testimony of Uber US' Chief Information Security Officer to the US Senate's Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, has informed the Commissioner's assessment of the technical and organisational measures in place for the S3 and GitHub repositories up to 15 November 2016.
25. Based on the factual matters set out above, the Commissioner's view is that, at the relevant time, Uber contravened DPP7 in relation to its personal data storage arrangements in that:
 - (1) The security arrangements adopted by Uber US were in fact inadequate.
 - a. Uber US's policies and practices did not adequately cover the risks presented by the use of third party platforms such as GitHub without multifactor authentication where the repository includes an access key in plain text. GitHub recommends that developers use one account within their platform. This means that developers often used personal email addresses as user names. The GitHub platform does allow additional security features, such as two factor authentication. At that time, Uber US did not mandate the use of two factor authentication to access Uber's private GitHub repositories. While its Information Security Awareness Policy referred to not reusing Uber's Onelogin password (evidencing its appreciation of the risk of credential stuffing) at the relevant time, Uber US did not expressly prohibit personnel from re-using credentials for third party

platforms, including GitHub, used to conduct Uber business. At the relevant time, the outside actors were able to obtain access to the GitHub accounts for 12 employees, reportedly because those employees had re-used their GitHub credentials on other platforms.

b. The [REDACTED] account credential was contained in plain text in a piece of code that was stored in GitHub. Uber US has confirmed that, while it did not have a formal written policy in this regard, its policy nonetheless was that engineers should not have hard coded credentials in plain text. Uber and Uber US should have appreciated the serious risk of cyber attack, of the sort which in fact occurred, from developers' use of personal email addresses without multifactor authentication to get access to a third party service where an access code was stored in plain text.

c. Uber US had adopted a tool for managing 'secrets' (a technical term of art), known as [REDACTED], to generate and manage S3 service account credentials and other secrets. Although [REDACTED] enabled engineers to rotate or configure rotation of S3 service account credentials, the [REDACTED] credential had not been rotated. Uber has been unable to explain why this credential was not rotated, although it believes that this was attributable to a human error rather than to any flaw in [REDACTED] or any failure adequately to test it.

(2) Moreover, Uber US's decision to treat the incident as a bug bounty rather than a security breach demonstrates an inadequacy in its decision making when contacted by the attackers in November 2016. The Commissioner recognises that a bug bounty programme, such as that which Uber US operated at the relevant time, may be a legitimate practice for paying financial rewards in exchange for the responsible

disclosure of security vulnerabilities. In this case, however, Uber US did not follow the normal operation of its bug bounty programme. In this incident Uber US paid outside attackers who were fundamentally different from legitimate bug bounty recipients: instead of merely identifying a vulnerability and disclosing it responsibly, they maliciously exploited the vulnerability and intentionally acquired personal information relating to Uber users.

26. 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 above-described practices constitute inadequacies in Uber US' arrangements for ensuring the security of personal data on the S3 system. Assessing the arrangements in the round, the Commissioner's view is that there was plainly a contravention of DPP7 in this case.

The issuing of a monetary penalty

27. The Commissioner's view is that the conditions for issuing a monetary penalty under section 55A have been met in this case.
28. The Commissioner considers that these contraventions were serious, in that:
- (1) The set of S3 buckets accessible through the [REDACTED] credential contained a substantial quantity of data, which may have included additional personal data. While (i) these buckets were not used to store [REDACTED] information [REDACTED] [REDACTED] from data subjects in the UK; (ii) Uber does not typically collect sensitive personal data from UK

data subjects or store it in these S3 buckets; and (iii) there is no evidence that any information was in fact accessed other than the 16 downloaded files, any additional personal data that was accessible was put at risk by this breach;

- (2) The breach involved a very large amount of personal data, affecting approximately 2.7 million individuals in the UK. This increases the seriousness of the data security inadequacies;
- (3) The attack was not notified to the Commissioner (or any other relevant regulator) at the time;
- (4) None of the individuals whose personal data had been compromised were notified of the breach at the time. Nor were steps taken to monitor affected users' accounts, or to flag them for additional fraud protection at the time. While Uber has instituted additional fraud monitoring for all accounts affected by the breach, and has reviewed all such accounts for activity occurring since the time of the breach, these steps were only taken some 12 months after the attack took place.

29. The Commissioner considers that these contraventions were of a kind likely to cause substantial distress, in that:

- (1) The personal data that was put at risk as a result of these contraventions is described at paragraph 19 above. The expectation of individuals is likely to be that a contravention involving personal data of those kinds will be useful in terms of increasing the likelihood of social engineering via phishing or smishing attempts, causing substantial distress;

- (2) This contravention was of a kind that exposed personal data to the risk of cyberattack - as opposed, for example, to the accidental loss of data. Cyberattack invariably involves nefarious and criminal purposes. A contravention that exposed individuals to such consequences was of a kind likely to cause substantial distress;
- (3) The delay in reporting the breach is likely to have compounded the distress that affected individuals suffered.
30. The Commissioner considers that Uber knew or ought reasonably to have known that there was a risk that the contraventions would (a) occur, and (b) be of a kind likely to cause substantial distress. She further considers that Uber failed to take reasonable steps to prevent such a contravention.
31. 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.
32. That view is based on the inadequacies identified above, the likely consequences of such a contravention and Uber's culpability for it. The Commissioner has also considered the importance of deterring future contraventions of this kind, both by Uber and by others. The Commissioner considers that the latter objective would be furthered by the issuing of a monetary penalty in this case.

The Commissioner's decision to issue a monetary penalty

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

- (1) Uber (being Uber BV and Uber UK) was not aware that the security breach had occurred at the time that it took place. It was therefore not itself in a position to report it to the Commissioner, nor to notify the relevant data subjects that their data had been compromised;
 - (2) There is no evidence that the compromised personal data was in fact used for successful identity theft or fraud activities;
 - (3) In the course of its review, Mandiant did not identify trip location history, location over time, payment card numbers, bank account numbers, date of birth, or government or tax identifiers in the compromised data;
 - (4) Uber has taken substantial and prompt remedial action to prevent a reoccurrence of this type of incident;
 - (5) The incident giving rise to the breach was a cyberattack on a third party's system and the integrity of Uber's internal systems was not compromised.
34. The Commissioner has also taken into account the following aggravating features of this case:
- (1) Uber (being Uber BV and Uber UK) did not notify the Commissioner of the breach upon learning of it; rather, the Commissioner became aware that it had taken place via reports in the media;

- (2) None of the data subjects were notified that their personal data had been compromised at the time of the breach;
- (3) In consequence, there was a significant delay in the Commissioner, and the data subjects, being notified of what had occurred.
35. 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 the procedural rights under section 55B have been complied with.
36. The latter has included the issuing of a Notice of Intent, in which the Commissioner set out her preliminary thinking. In reaching her final view, the Commissioner has taken into account the representations made by Uber on this matter.
37. The Commissioner is accordingly entitled to issue a monetary penalty in this case.
38. The Commissioner has considered whether, in the circumstances, she should exercise her discretion so as to issue a monetary penalty.
39. The Commissioner has also taken into account her underlying objective in imposing a monetary penalty notice, namely to promote compliance with the DPA. 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.
40. Further, she has considered Uber's financial position, as evidenced, for example, by the published annual accounts of Uber.

The amount of the penalty

41. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of **£385,000 (three hundred and eighty five thousand pounds)** is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.


Conclusion

42. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **3 January 2019** 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.
43. If the Commissioner receives full payment of the monetary penalty by **2 January 2019** the Commissioner will reduce the monetary penalty by 20% to **£308,000 (three hundred and eight thousand pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.
44. 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.

45. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.
46. Information about appeals is set out in Annex 1.
47. 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.
48. 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 November 2018

Signed .. 

Elizabeth Denham
Information Commissioner
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 55B(5) of the Data Protection Act 1998 gives any person upon whom a monetary penalty 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:

General Regulatory Chamber
HM Courts & Tribunals Service
PO Box 9300
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 section 55B(5) 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)).