Information Commissioner's Office

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Bounty (UK) Limited

Of: 29 Broadwater Road, Welwyn Garden City, Hertfordshire, AL7 3BQ

1. The Information Commissioner ("Commissioner") has decided to issue Bounty (UK) Limited ("Bounty") 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 first data protection principle ("DPP1") from Schedule 1 to the DPA.

2. Bounty contravened DPP1 by sharing the personal data of over 14 million individuals to a number of organisations including credit reference and marketing agencies without informing those individuals that it might do so. As a result Bounty processed that personal data unfairly and without satisfying any processing condition under Schedule 2 to the DPA.

3. The amount of the monetary penalty which the Commissioner has decided to issue is £400,000.

4. This Notice is served under section 55B of the DPA. It explains the grounds on which the Commissioner has decided to issue the monetary penalty. The Commissioner has considered written representations

from Bounty dated 19 February 2019 and 8 March 2019 in response to the Notice of Intent before reaching a final decision on this matter.

Legal framework

5. The DPA implemented 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. Both the DPA and the Directive have since been repealed, but the contravention at issue in this case took place while they were still in force.

6. Bounty 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.

7. The relevant provision of the DPA is DPP1 which provides that:

> *Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -*
> *(a) at least one of the conditions in Schedule 2 is met, and*
> *(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*

8. Interpretative provisions in Part II of Schedule 1 to the DPA provide in relevant part that:

> *1.- (1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be*

processed.

(2)....

2. – (1) Subject to paragraph 3, for the purposes of the first principle personal data are not to be treated as processed fairly unless -

(a) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3), and

(b) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3).

(2) In sub-paragraph (1)(b) "the relevant time" means -
(a) the time when the data controller first process the data, or

(b) in a case where at that time disclosure to a third party within a reasonable period is envisaged -

(i) if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed,
(ii) if within that period the data controller becomes, or ought to become, aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware, or
(iii) in any other case, the end of that period.

(3) The information referred to in sub-paragraph (1) is as follows, namely-
(a) the identity of the data controller,
(b) if he has nominated a representative for the purposes of this Act, the identity of that representative,
(c) the purpose or purposes for which the data are intended to be processed, and
(d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

3. – (1) Paragraph 2(1)(b) does not apply where either of the

primary conditions in sub-paragraph (2), together with such further conditions as may be prescribed by the Secretary of State by order, are met.

(2) The primary conditions referred to in sub-paragraph (1) are -
(a) that the provision of that information would involve disproportionate effort, or
(b) that the recording of the information contained in the data by, or the disclosure of the data by, the data controller is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

9. It appears to the Commissioner that two processing conditions from Schedule 2 to the DPA are potentially relevant in cases such as this:

1. The data subject has given his consent to the processing.

...

6.—(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

10. Article 2(h) of the Directive provided that:

'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

11. 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 a monetary penalty notice of the Commissioner considers 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.

12. 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.

13. 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.

Background to the case

14. Bounty has traded since 1959, and describes itself as a pregnancy and parenting support club which provides information and markets offers and services to parents at different stages of a family's life from pre-conception to pre-school. Bounty's key service is the provision of 'Bounty Packs' (sample packs for different stages of pregnancy and after birth), distributed to new parents. Bounty also provides a mobile App which allows expectant mothers to track their pregnancies, a new-born portrait service and access to competitions and offers throughout pregnancy and beyond. In addition to its primary function described above, Bounty operates a data broking service, providing hosted marketing on behalf of third parties and, until 30 April 2018, it supplied data to third parties for the purpose of electronic direct marketing.

15. Bounty first came to the attention of the Commissioner during the course of a general investigation into non-compliant practices of the data brokerage industry, in which Bounty were identified as a significant supplier of personal data to third parties for direct marketing purposes.

16. Accordingly the Commissioner launched an investigation into Bounty's own practices, in which Bounty advised that it collected personal data for the purpose of membership registration across a variety of channels: its website, mobile App, 'Mother-to-be pack' offline claim cards and directly from new mothers at hospital bedsides. [redacted]

17. Bounty informed the Commissioner that each unique record comprised the following personal data: Full name, parents date of birth, Email address, postal address, postcode, pregnancy status, first time mum, name, gender and date of birth of children (and by extension, address of child). The mobile App also collected location data [redacted]

18. In accordance with its retention policy at the relevant time, digital records were held 'indefinitely' unless a data subject made a written request for their details to be removed from the database. Children's data was retained for the duration of the parent's membership.

19. Bounty informed the Commissioner that during the period 1 June 2017 to 30 April 2018, based upon consent received during the member registration process, it shared a total of 35,027,373 personal data records with Acxiom (a marketing and profiling agency), Equifax (a

credit reference agency), Indicia (a marketing agency) and Sky (a telecommunications company) for the purposes of direct electronic marketing. These organisations represented the four largest recipients out of a total of 39 organisations with which Bounty confirmed it shared personal data, with each record shared representing the personal data of an individual person. Whilst the data shared with each organisation varied slightly, in each case it comprised the majority, if not all of the data collected in respect of each individual.

20. In representations made to the Commissioner in response to the Notice of Intent, Bounty went on to confirm that during the period 1 June 2017 to 9 January 2018, the number of individual records shared was 34,267,889 (this is of particular relevance to paragraphs 25 and 39 below).

21. At the time of disclosure Bounty held over 17 million unique individual's records on its database. Bounty stated that it did not share all records held, but informed the Commissioner that the number of records shared in the circumstances described in paragraphs 19 & 20 above, represented the data of 14,315,438 unique individuals. Bounty also confirmed that each data record could be shared on multiple occasions, in some cases up to 17 times in a 12 month period.

22. In response to the Commissioner's enquiries Bounty provided an explanation of its data collection processes, as well as providing copies of its Privacy, Data Protection and Retention policies in place at the point of registration.

23. Bounty's Data Protection Policy states that data is not collected excessively, and only for the specific purposes as explained to the individual. It states that Bounty may share data with 'selected third parties'.

24. Bounty's Privacy Policy appearing on its website (dated 2017) states that Bounty collected personal data for the purposes of 'marketing' and 'tailoring the service'. In relation to data collected about children specifically, Bounty advised the Commissioner that it used the knowledge of due dates and children's birth dates to offer 'tailored communications'. The policy goes on to say that users may receive communications from Bounty or 'a third party', and that information may be sent based on a user's location. The policy then categorises general types of 'selected third parties', together with a link to specific companies, who may send marketing [redacted] Up to 9 January 2018 (see below) none of the organisations with whom data was shared (as per paragraph 19 above) were named in the Policy.

25. In representations made to the Commissioner on 8 March 2019, Bounty explained that in late 2017, a decision was made to supplement the terms of its Privacy Policy by supplying a 'named list' of third-party partners. The list, which included the four named parties detailed in paragraph 19 of this Notice, went live on the website and the mobile App on 9 January 2018.

26. Individuals using Bounty's App are offered an opt-in to marketing with a 'yes' or 'no' response option to the question *"would you like to receive free samples, offers and promotions by post and email from carefully selected third parties (see privacy policy for full details)".* The website operates using a similar notice, offering a tick box for users to opt-in to receiving promotions by post and email from *"carefully selected third parties"*.

27. Bounty advised the Commissioner during her investigation that the business is moving towards a digital only data capture platform, but

provided examples of hard copy claim cards still in use at the relevant time, and a copy card left at hospitals for new mothers who do not see a Bounty representative during their stay. Whilst hard copy claim cards are not currently in use, the data previously collected in this manner continues to be held by Bounty.

28. None of the claim cards have an opt-in to marketing option, instead, a small piece of text at the bottom of the card explains: *"By providing your email address and/or telephone number (optional) you consent to be contacted by these channels as well as post. We will take great care of the information you have provided and will use it to fulfil your membership of Bounty. While you are a member, we may share your information with a selected group of companies who also have services, free samples, offers and product information that may be of interest to you."* Name and postal address are mandatory data fields on each claim card, so individuals wishing to register for Bounty's services 'offline' had no choice but to agree to their personal data being shared with third parties for marketing purposes. Given that 'offline' registrants did not have access to Bounty's Privacy Policy at the point of registration, the supplementary list referred to in paragraph 25 of this Notice likewise would not have been available to individuals registering 'offline' via hard copy claim cards or bedside contracts.

29. [redacted]

30. Bounty informed the Commissioner that in respect of its current database, 69% of the records held represent data acquired through 'offline' registrations, and therefore it follows that 31% of records represent data acquired through 'online' registrations.

31. In further representations to the Commissioner dated 8 March 2019, Bounty stated that in relation to its current records data base, 66% of 'offline' registrants provided an email address as part of the registration process. As a matter of course, Bounty states it sent an email to those registrants shortly after registration, which included in the footer a direct link to its Privacy Policy and an 'unsubscribe' link, and so 'offline' registrants would have been given the opportunity to view Bounty's Privacy Policy 'within a very short period of registration'. The Commissioners position is that fair processing information should be provided at the point of data collection and not within a 'very short period' thereafter, and so finds that Bounty's practice as described above did not comply with DPP1.

32. On 30 April 2018 Bounty ceased its practice of sharing data with third parties for direct marketing purposes, and removed from the 'named list' referred to in paragraph 25 of this Notice the four organisations named in paragraph 19.

33. Up to the relevant time (i.e. up to 30 April 2018 in respect of 'offline' registrations and 9 January 2018 in respect of 'online' registrations), Bounty's fair processing notices gave no indication that personal data may be shared with any of the organisations detailed in paragraph 19 of this notice. Based upon the information Bounty provided, it is the Commissioner's considered view that any 'consent' provided by data subjects was not informed, nor could data subjects have foreseen that their data would be shared with those organisations.

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

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

The contravention

36. As set out above, the "fairness" requirement under DPP1 included a transparency duty: data controllers were required to provide or make available to data subjects information about (inter alia) the purposes for which their personal data will be used. Bounty failed to comply with that transparency duty in this case. It did not provide or make available to the affected data subjects information about the potential disclosure of their personal data to Acxiom, Equifax, Indicia or Sky.

37. The "fairness" requirement under DPP1 also included a substantive duty to treat individuals fairly when using their personal data. In particular, fairness involves adhering to individual's reasonable expectations of how their data will be used and not using their data in ways that risk causing them damage or distress, unless there is some sufficiently weighty justification for doing so. Bounty failed to use the personal data of the affected data subjects fairly in this case. As indicated above, data subjects registering with a pregnancy and parenting club would not reasonably have expected their personal data to be disclosed to the likes of credit reference, marketing and profiling agencies. Bounty had no adequate justification for acting as it did. Its actions appear to have been motivated by financial gain, given that data sharing was an integral part of Bounty's business model, and as confirmed by Bounty, cessation of its data sharing practice on 30 April 2018 resulted in significant commercial impact.

38. The extracts from Bounty's fair processing information set out above suggest that Bounty sought to justify its disclosure of data to third parties for marketing purposes by reference to condition 1 of Schedule 2, namely the consent of data subjects. Indeed, Bounty confirmed to the Commissioner during her investigation that the sharing of the personal data as described in this notice was based on consent received from data subjects during the registration process. The Commissioner's assessment is that this condition was not met here. These 'consents' were not specific or informed, given that data subjects were not told that that their data may be shared for the purposes of marketing with Acxiom, Equifax, Indicia or Sky, or with any organisations of a similar nature. Nor, in the case of 'offline' claim cards, were these 'consents' freely given, given that, at the point of registration, the data subjects had no choice but to agree to disclosure of their personal data for marketing purposes.

39. The only other potentially applicable condition from Schedule 2 in such cases is condition 6(1) (legitimate interest). Bounty has not indicated to the Commissioner that it relies upon this condition, however the Commissioner's assessment is that this condition would not have been met here either. Given its failure to inform data subjects that their personal data may be shared with the organisations listed in paragraph 19 or indeed any organisations of a similar nature, the balance of interests entailed by condition 6(1) tipped against Bounty.

40. The Commissioner's assessment is thus that no condition from Schedule 2 to the DPA was satisfied in this case.

41. For those reasons, the Commissioner's assessment is that Bounty's disclosure of the personal data contained in approximately 34,436,776 records comprising:

a) 24,168,887 records provided to Acxiom, Equifax, Indicia and Sky between 1 June 2017 and 30 April 2018 in respect of data acquired through 'offline' member registrations (representing 69% of 35,027,373 records shared during this period - see paragraphs 19 & 30 above), and

b) 10,267,889 records provided to Acxiom, Equifax, Indicia and Sky between 1 June 2017 and 9 January 2018 in respect of data acquired though 'online' member registrations (representing 31% of 34,267,889 records shared during this period - see paragraphs 20 & 30 above)

contravened DPP1 in that:

(1) The disclosure was unfair, in that the data subjects were not provided with information about the potential disclosure of their personal data to those organisations, or to any organisations of a similar nature who may use that data for the purposes of marketing.

(2) The disclosure was also unfair in that it contravened the reasonable expectations of the data subjects and exposed at least some of them to potential distress without reasonable justification.

(3) Neither the consent condition, nor the legitimate interests condition, nor any other condition from Schedule 2 to the DPA was met.

42. In respect of 'online' member registrations this was an ongoing contravention until 9 January 2018 when Bounty supplemented its Privacy Policy with a 'named list' of third-party partners, which

included those organisations detailed in paragraph 19 of this Notice. In respect of 'offline' member registrations this was an ongoing contravention until 30 April 2018 when Bounty ceased its practice of trading and sharing personal data with third parties.

43. The Commissioner is satisfied that Bounty was responsible for this contravention.

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

The issuing of a monetary penalty

45. The Commissioner's preliminary view is that the conditions for issuing a monetary penalty under section 55A have been met in this case.

Seriousness of the contravention

46. The Commissioner is satisfied that the contravention identified above was serious, in that:

(1) The number of affected data subjects was extraordinarily high - in excess of 34 million records having been disclosed, comprising the personal data of over 14 million individuals. This represents an unprecedented number of affected data subjects in the history of the Commissioner's investigations into data broking organisations. As her investigation focussed on only four 4 out of 39 organisations with which Bounty shared data, it is reasonable to suppose that the number of records disclosed could have been significantly higher.

(2) In addition, some of the affected individual's data was shared on multiple occasions and with multiple organisations, further impacting on their data rights. Whilst Bounty stated it tracked the data it shared, trading data up to 17 times in a 12 month period is arguably disproportionate, and opened the affected individuals to excessive processing that they did not consent to.

(3) The sustained and prolonged duration of the contravention – approximately 7 months in respect of 'online' member registrations, and 11 months in respect of 'offline' member registrations.

(4) The data subjects were not only potentially vulnerable new mothers/mothers-to-be, but also very young children. Furthermore, whilst Bounty advised that its 'philosophy and policy' is never to market children, and it did not share children's names with third parties, the Commissioner considers that sharing the birth date and gender of a child along with information about its parent, creates the potential this data to be appended to create a fuller profile of the child, which may then be used for future targeted marketing. In these circumstances a loss of control of data has already taken place before the child has capacity to consent for its data to be used for marketing purposes.

(5) In the Commissioner's assessment, this disclosure went clearly against the terms of the privacy notices in place at the time. As subjects signed up to a parenting club it is considered highly unlikely that individuals would reasonably expect their personal data to be shared with credit referencing, marketing and profiling agencies, unless explicitly informed that it would be.

(6) The nature of the data involved - this included information relating to number, age and gender of children, and [redacted] pregnancy status. Disclosure of such information in this context created a real risk of distress (see further below).

(7) Individuals were exposed to a significant loss of control over their data, exacerbated by the fact that Bounty did not inform them about this disclosure either before or after it had taken place.

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

Contraventions of a kind likely to cause substantial damage or substantial distress

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

(1) For those data subjects registering online, Bounty's privacy notices contained reasonably clear descriptions of the kinds of third parties who might receive personal data from Bounty. However, none of the four most supplied organisations were listed, and the broad category types did not clearly indicate the types of organisations with which the data the subject of the Notice was shared. At least some of the affected data subjects are likely to have been distressed by this failure to adhere to their expectations about how their data would have been used. At least some of these data subjects would reasonably feel misled.

(2) In addition, given that Bounty failed to be transparent with the data subjects about this disclosure, the data subjects may well have been distressed by uncertainty as to how the organisations in this case obtained information with which to target them based on their personal circumstances.

(3) This sense of distress is likely to have been exacerbated by the fact that it focussed on the affected data subjects' status as new or expectant mothers, as well as on their young children. It is highly likely that at least some data subjects who may not be concerned about their name or email address being shared with a marketing company, would have been distressed by the inclusion of information about their pregnancy status and children without their explicit consent.

(4) At least some of the affected data subjects are likely to be distressed by the perceived loss of control over their data when it was shared without their knowledge with large marketing organisations.

(5) At least some of the affected data subjects are likely to be distressed by the fact that their personal data has been shared on numerous occasions with multiple organisations. Some data records were shared up to 17 times over a 12 month period. This, in the Commissioner's view, would exacerbate the level of any distress caused.

(6) The Commissioner has also given weight to the number of affected data subjects: in excess of 14 million. The Commissioner considers that even if the damage or distress likely to have been suffered by each affected individual was less than substantial,

the cumulative impact would clearly pass the threshold of "substantial".

(7) In representations made to the Commissioner, Bounty pointed to a lack of complaints about Bounty's processing of data in the circumstances described. Bounty also stated that only a tiny proportion of those registering 'online' went on to view the supplementary list linked to the Privacy Policy, suggesting that very few data subjects were concerned about the 'named list' and so (if any) detriment to those individuals would be minimal. Bounty relies upon a lack of any evidence of actual distress, stating this case is based more upon an assumption of 'risk'. The Commissioner's view is that the above is demonstrative of the 'invisible' nature of the processing whereby individuals are unaware, either before or after, of the processing of their data in these circumstances. She considers that if individuals were aware of the processing of their personal data in these circumstances there would be a real likelihood of substantial damage or distress of the nature described above.

49. Given the considerations outlined above and the number of affected data subjects, it is likely that the "substantial distress" threshold was crossed here. In other words, the Commissioner's view is that there was a significant and weighty chance that a contravention of the kind described would have such consequences.

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

Deliberate or negligent contraventions

51. While it may not have set out to contravene the DPA, Bounty's actions in sharing the data were plainly deliberate. In any event, the Commissioner considers that Bounty 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 Bounty failed to take reasonable steps to prevent such a contravention in that:

(1) Bounty was aware of the terms of its own privacy notices. It should have been readily aware that those terms were inadequate for disclosure for these purposes.

(2) Bounty knew its customer base. It knew why they registered with Bounty and what kind of marketing communications they would expect to receive. It should have been very clear to Bounty that this disclosure contravened those expectations.

(3) Given its own knowledge of its customer base and the common sense considerations summarised at paragraph 48 above, it should have been readily apparent to Bounty that this disclosure was likely to cause substantial distress to at least some of the affected data subjects.

(4) The ICO has published extensive guidance on the importance of valid consent and how to obtain it, and a long established organisation of Bounty's size should have been well aware of the steps it needed to take to ensure its data subjects had all the relevant information at the point of data collection.

(5) [redacted]

(6) At the commencement of the Commissioner's investigation in early 2018, Bounty informed the Commissioner that it planned detailed changes to ensure that its marketing practices were compliant with the (then) forthcoming GDPR, including cessation of trading and sharing personal data with third party organisations, updating fair processing notices to ensure data obtained for marketing is fully opted-in, changes to its retention policy, cessation of hard copy claim cards, training of staff and purging its database to reduce the number of records held. Bounty knew that its data sharing practices would likely not be compliant with GDPR and confirmed that it had not carried out impact assessments prior to GDPR. If these appropriate checks had been carried out beforehand then Bounty should have known that its data sharing practices would contravene the DPA.

(7) As referred to above, the steps it took to prevent further breaches and minimise detriment to data subjects shows that Bounty was alive to the kinds of steps that would be needed to avoid contraventions of the DPA in the circumstances, but it failed to take any such steps. The Commissioner considers there was no good reason for this failure.

52. The Commissioner's view is therefore that condition (c) from section 55A (1) DPA is met. That view is based on the size and scale of the contravention, given the number of affected data subjects, the likely consequences of such a contravention and Bounty's culpability for it.

The Commissioner's decision to impose a monetary penalty

53. 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 section 55A(3) and the procedural rights under section 55B have been complied with.

54. The latter has included the issuing of a Notice of Intent dated 21 January 2019 in which the Commissioner set out her preliminary thinking. Bounty received the Notice of Intent on 22 January 2019.

55. The Commissioner received initial representations from Bounty on 19 February 2019, together with additional representations and information on 8 March 2019 which she has taken into consideration when reaching her decision. She has also considered Bounty's financial position, as evidenced by its published annual accounts, more recent unaudited accounts and bank statements.

56. The Commissioner is accordingly entitled to issue a monetary penalty in this case.

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

- Bounty voluntarily ceased its practice of trading and sharing personal date with third party organisations on 30 April 2018.

- Bounty has since made significant changes to its data practices to ensure compliance with GDPR and PECR (as detailed in paragraph 51(6) above).

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

The amount of the monetary penalty

59. Taking into account all of the above, the Commissioner has decided that the amount of the penalty is **£400,000 (four hundred thousand pounds).**

Conclusion

60. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **16 May 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.

61. If the Commissioner receives full payment of the monetary penalty by **15 May 2019** the Commissioner will reduce the monetary penalty by 20% to **£320,000 (three hundred and twenty thousand pounds).** However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

62. 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.

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

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

65. 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.

66. 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 9th day of April 2019

Signed .....

Stephen Eckersley
Director of Investigations
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)).