IN THE MATTER OF THE DATA PROTECTION ACT 1998

AND IN THE MATTER OF A PROPOSED CONTRACT

B E T W E E N:

Cambridge Analytica Inc

Claimant

- and -

United Kingdom Independence Party

Defendant

OPINION

1. We are instructed on the direct access basis to advise Cambridge Analytica Inc ("CA'"), a Delaware company, in relation to certain aspects of their data analysis system - more specifically, on their contract with the United Kingdom Independence Party ("**UKIP**") ("**the Contract**"). We are, in particular, asked to consider whether the processing proposed to be carried out under the Contract is lawful within the meaning of the *Data Protection Act 1998* ("**the DPA 1998**").

2. We have had the benefit of a conference with several staff members of CA and we have reviewed the *UKIP Data Protection Policy* and *Privacy Policy* which are freely available on the UKIP.org website.

3. Based on the information with which we have been provided, for the reasons and with the qualifications set out below, we are of the opinion that it would be lawful for CA to carry out the processing for UKIP proposed under the Contract.

Reasons

Introduction

4. The DPA 1998 provides a code setting out the manner and extent to which a person (whether an individual, corporate body, organisation or governmental agency) may use an individual's personal information. The terminology of the DPA 1998 is key to an understanding of its operation. The use of personal information controlled by the Act is called "processing"; the information whose use is controlled by the Act is called "personal data";[1] the controlling

[1] Section 1(1) of the DPA 1998 defines '"personal data" as data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller; and it includes any expression of

mechanism over the use of personal information is called the "data protection principles"; and the person subject to the main controls of the Act is called the "data controller."

5. The 1998 Act recognises that the person who carries out the task of saving, holding, retrieving etc (ie processing) personal information may be different from the person who decides what processing is to be carried out on that information. In other words, it recognises that sometimes there will be an arrangement where one person processes personal information by carrying out the instructions of someone else - ie a data controller. In that situation, the first person is called the "data processor." As just noted, the 1998 Act is mostly concerned to regulate the conduct of the data controller rather than the data processor.

6. The 1998 Act also recognises that the use of some sorts of personal information requires a closer degree of control than other personal information. The sort of information that is more closely controlled is called "sensitive personal information."[2]

7. The data protection principles are listed in Part 1 of Schedule 1 to the Act. Much of the detail of those principles is spelled out in Part II of Schedule 1 to the Act, as well as in Schedules 2, 3 and 4. The obligation to adhere to the data protection principles is imposed by s 4(4).

8. A suite of exemptions is set out in Part IV of the Act (ss 27-38). There are further exemptions in Sch 7 to the Act and in regulations made under the Act. Where an exemption applies, it serves to relieve the data controller from some, but not all, of the data protection principles: see s 27.

9. Non-compliance with the s 4(4) obligation exposes the data controller to a court claim for compensation. Where such a claim is made, the individual affected may seek recompense for pecuniary loss, as well as for distress, suffered as a result of the breach of the principles. Where such a claim is made, a court may also make coercive orders requiring the data controller to destroy, amend, erase etc that individual's information.

10. Quite separately from any court claim, the Information Commissioner can investigate the data processing procedures of a data controller by issuing various notices (assessment, enforcement and so forth) with which a data controller must comply.

---

opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

[2] Section 2 of DPA 1998 defines "sensitive personal data" as personal data consisting of information relating to the data subject with regard to racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health or condition; sexual life; the commission or alleged commission by the data subject of any offence; or any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

11. In short, a data controller is well advised to know and abide by the requirements of the Act when handling personal information.

Which (if any) of CA's processing will be regulated by the DPA 1998?

12. As we are instructed, the system used by CA is one that it has successfully used in the USA and elsewhere. It relies upon detailed analysis of data using a method that has not previously been used in the UK. The design of that analysis and the means of effecting it are all within the exclusive domain of CA. While CA's clients will typically supply some of the raw data used in the system, CA adds further data to that client-sourced data, which it analyses in order to yield an output. CA is solely responsible for deciding what analysis will be carried out in order to supply the client with the output. The output does not identify specific individuals, but is an abstraction of attributes arranged in way that is informative to the client.

13. It is proposed by CA to enter in to a contract with UKIP to provide data analysis and profiling for the party to as part of UKIP's research into its membership. This research includes trying to ascertain the profile of a typical and likely UKIP member. UKIP intends to share the results of this research with Leave.EU, a campaign group with similar aims to UKIP.

14. UKIP's data are split in to two types: data gathered from the membership information of members ("**Membership Data**"), and data gathered from the operation of the UKIP website ("**Website Data**"). The Membership Data are covered by the *UKIP Data Protection Policy*. The Website Data are covered by UKIP's *Privacy Policy*.

15. The document entitled *UKIP Data Protection Policy* recites that UKIP:

    "needs to gather and use certain information about individuals"

    and that these individuals can include:

    "members, supporters, enquirers, business contacts, employees and other people the organisation has a relationship with or may need to contact."

    The policy is stated to

    "describe how this personal data must be collected, handled and store to meet the party's data protection standards - and to comply with the law."

    The document spells out which people within UKIP may access the information covered by the policy and the purpose for which they may access. It spells out that data should not be shared informally and that

    "personal data should not be disclosed to unauthorised people, either within the party or externally."

    There are paragraphs relating to the deletion of out-of-date information and storage of personal information. In summary, the policy is more concerned with telling UKIP staff and workers how the party wants them to handle personal information than it is with the party's advising individuals about whom the party holds information how the party may make use of that information. However, the document concludes:

    "UKIP aims to ensure that individuals are aware that their data is being processed,

and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the party has a privacy statement, setting out how data relating to individuals is used by the company.

This is available on request. A version of this statement is also available on the party's website."

16. The UKIP web home page (http://www.ukip.org/) has at its foot a hyperlink to "PRIVACY POLICY." Clicking on that brings up a page headed "PRIVACY POLICY", which is what it says it is. The page has four headings: "Information We Collect"; "Third Party Services"; "How We Use Your Information"; and "Queries". The *Privacy Policy* opens:

> "The UK Independence Party knows that you care how information about you is used and shared. This Privacy Policy explains what information of yours will be collected by us when you use our online services, how the information will be used, and how you can control the collection, correction and/or deletion of information. We will not use or share your information with anyone except as described in this Privacy Policy. This Privacy Policy does not apply to information we collect by other means (including offline) or from other sources."

As we understand it, apart from the website *Privacy Policy* UKIP has no other privacy policy. In other words, the website *Privacy Policy* is the "privacy statement" referred to in *UKIP Data Protection Policy*, despite what appears in the opening paragraph of the website *Privacy Policy*. We consider that it would be sensible for this to be checked with UKIP, but we have proceeded on the assumption that it is correct.[3]

17. The website *Privacy Policy* provides that:

> "Any information you provide, including your email address, will not be passed onto any third party (other than firms working on our behalf), except where you have signed a petition or similar, where the petition will be presented to a third party."

It also provides that:

> "How We Use Your Information
>
> We use the personal information you submit to operate, maintain, and provide to you the features and functionality of http://ukip.org."

18. UKIP intend to provide CA with all of their Membership Data and Website Data, as well as some anonymous membership questionnaires.

19. In relation to the Contract, the system will plainly involve the utilisation of personal data and sensitive personal data supplied to CA by UKIP. In addition, CA will use other types of data available to it such as mosaic data, credit data and demographic data, some of which may be

[3] Plainly, if it is not correct then we would need to re-visit our conclusions.

personal data or sensitive personal data. CA will then analyse all this data using its proprietary method. For the purpose of carrying out its analysis, CA may further augment this data with data from surveys conducted by CA. All of the CA data, including personal data and sensitive personal data, are or will be held and otherwise processed at their secure data centre in Scotland.

20. As we understand the operation of CA's proposed system, CA will be a "data controller" and not simply a "data processor."

21. Given that in the performance of the Contract the CA system will be analysing political opinions it will inevitably be processing both personal data and sensitive personal data.

22. The output (called "the Analysed Dataset" in the Contract) will be a psychological profile of classes of elector and an assessment of the likelihood of each such class of elector to be convinced of particular ideas and, most importantly, the messaging that would be most effective in convincing that class of elector ("**the Output**").

23. The Output will not itself contain any personal data or sensitive personal data. Rather, the Output will be generic information based upon an analysis of the personal data described above. Whilst a person could conjecture the identity of individuals from the Output, that conjecture would require an evaluative process separate from that provided by the CA service and the outcome of that evaluative process would remain conjectural.

24. On the basis that an individual will not be able to be identified from the Output and that even with the raw data UKIP supplied to CA UKIP would not be able to identify individuals from the Output, we are of the opinion that the Output itself would be not constitute personal data within the meaning of the DPA: see the definition of "personal data." Thus, neither the sending by CA nor the receipt by UKIP of the Output would constitute processing of personal data. As such, those forms of processing of the Output would not have to comply with the data protection principles.

25. On the other hand, the receipt by CA from UKIP of the information described above will constitute processing by CA of personal information. Indeed, given that it links each individual to a political opinion (because it has been collected by a political party and the quantity and content of that information will associate that individual with support for the party and its ideas), it will constitute the processing of sensitive personal information. Similarly, the subsequent holding of that information by CA, its analysis (including its combination with other information) and all the steps leading up to the production of the Output will each constitute processing of personal information/sensitive personal information by CA. As such, in so processing that information, CA must comply with the requirements of the DPA 1998.

26. We therefore now turn to consider whether what CA proposes to do with this information will

be compliant with the requirements of the DPA 1998, i.e. whether the processing would comply with each of the eight data protection principles.

To the extent that CA's processing is subject to the DPA 1998, is it lawful?

27. Part 1 of Schedule 1 to the DPA 1998 contains the "data protection principles." Under s 4(4) of the DPA 1998, a data controller (such as CA) must adhere to these data protection principles whenever processing personal data.

First data protection principle

28. The first data protection principle is:

> "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."

29. It will be seen that there are three requirements that must be met in order for the processing of ordinary (ie non-sensitive) personal data to comply with the first data protection principle: the data must be processed "fairly"; it must be processed "lawfully"; and at least one of the conditions in Schedule 2 must be met. In the case of sensitive personal data, there is a fourth requirement: namely, that at least one of the conditions in Schedule 3 must be met.

30. In determining whether personal data are processed "fairly," paragraphs 1-3 of Part II of Schedule 1 prescribe situations where the fairness will necessarily be met, situations where it will not be met and, in relation to the remaining situations, certain matters to which regard is to be had in evaluating whether the data is being processed fairly.

31. Put very generally, whether data is or is not being processed fairly revolves around how the data controller obtained the personal information being processed: in particular, it is concerned with whether the individual gave consent to the processing or was notified of it.

32. Paragraph 2 of Part II of Schedule 1 (which sets out required but not necessarily sufficient procedures for "fairness") provides, so far as relevant:

> "(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 processes 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."

33. In the present case, CA is not obtaining the personal data from the data subject: it is obtaining it from UKIP. Accordingly, sub-sub-paragraph 2(1)(b) (rather than sub-sub-paragraph 2(1)(a)) which is applicable. As we understand it, CA has not started processing the data yet, so the "relevant time" has not been reached: but it is imminent. Putting it at its lowest, the requirement is for CA to make readily available to the data subject the information specified in sub-paragraph 2(3). We consider that in order to satisfy this requirement CA should make available on its website a general statement of the information in (3). This should be done at the outset of processing. This will ensure that the processing is not deemed to offend the fairness requirement. But it does not follow that the processing is necessarily fair.

34. So far as is relevant, the only other statutory assistance given by Part II of Schedule 1 is in sub-paragraph 1(1) which states:

> "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."

35. We have seen nothing to suggest that any of the personal data that UKIP is proposing to pass over to CA for the purpose of carrying out the contract was obtained by deception or in a misleading way. Again, while of some assistance, satisfaction of sub-paragraph 1(1) does not necessarily make the processing fair.

36. The Information Commission has a statutory duty (s 51(1)) to:

> "promote the following of good practice by data controllers and, in particular, so to perform his functions under this Act as to promote the observance of the requirements of this Act by data controllers."

One of his functions (s 51(2)) is to:

> "...arrange for the dissemination in such form and manner as he considers appropriate of such information as it may appear to him expedient to give to the public about the operation of this Act, about good practice....and may give advice to any person as to any of those matters."

Thus, although statements of good practice from the Information Commissioner do not have the status of a statute, where a data controller follows such statements in the processing of personal data it is extremely unlikely that such processing will result in adverse determinations by the Commissioner.

37. In dealing with the fairness requirement in the first data protection principle, and specifically where the data controller acquires the personal information from another data controller, the Commissioner's current statement is as follows:

> "Some organisations share personal data with other organisations. For example, charities working in the same field may wish to use or share supporters' information to allow reciprocal mailings. Some companies even trade in personal data, selling or renting the information. The individuals concerned must still be treated fairly. They should be told that their information may be shared, so they can choose whether or not to enter into a relationship with the organisation sharing it."

In other words, in this situation the Information Commissioner looks to the conduct of the original acquirer of the personal information — in this case UKIP.

38. We have set out above the relevant parts of the *UKIP Data Protection Policy* and UKIP's *Privacy Policy*. In processing the personal data supplied by UKIP to it, CA is working on behalf of UKIP. The *Privacy Policy* expressly contemplates that UKIP may pass personal information it holds to others working on its behalf. UKIP has acted in accordance with the Commissioner's guidance. In short, provided that the requirements of para 2(3) are met, we consider that CA's processing will meet the fairness requirement of the first data protection principle.

39. In relation to the second requirement of the first data protection principle — that the processing be lawful — this essentially means that the processing does not otherwise offend any statutory provision. We have seen nothing to suggest any unlawfulness in the proposed processing of the personal data. The lawfulness requirement is thus satisfied.

40. We turn next to the third requirement of the first data protection principle, the requirement that at least one of the conditions in schedule 2 is met. Schedule 2 comprises six paragraphs. The first five are not relevant. The sixth is relevant. So far as relevant, it provides:

> "(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."

41. Paragraph 6(1) contemplates a balancing exercise. On one side are the processing which is necessary for the purposes of "the legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed." On the other side of the balance is the prejudice which the processing would cause to "the rights and freedoms or legitimate interests of the data subject."

42. Based on the information with which we have been provided, it is clear to us that the processing of personal information under the Contract is necessary for the legitimate interests both of CA (to carry on its business) and of UKIP (to understand its constituents). On the other side of the balance, the processing is not going to impede the rights and freedoms or legitimate interests of any data subject. The Contract will not involve an invasion of anyone's privacy; there is no profiling of specific individuals. The Output will not contain any personal data or sensitive personal data. We are firmly of the view that paragraph 6(1) is satisfied.

43. Thus, in relation to personal data that is not sensitive personal data, the processing contemplated by the Contract complies with the first data protection principle.

44. In relation to sensitive personal data, the processing will also have to meet a paragraph in Schedule 3 to the DPA 1998. That Schedule has seven paragraphs. Paragraphs 2-3 and 5-7 are inapplicable. Paragraphs 1 and 4 provide:

> "1. The data subject has given his explicit consent to the processing of the personal data.
>
> .....
>
> 4. The processing—
>
> (a) is carried out in the course of its legitimate activities by any body or association which—
>
> (i) is not established or conducted for profit, and
>
> (ii) exists for political, philosophical, religious or trade-union purposes,
>
> (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
>
> (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
>
> (d) does not involve disclosure of the personal data to a third party without the consent of the data subject."

45. Although it is not as clear as it might have been, the *Privacy Policy* does state that by providing an email address, a person does consent to a certain amount of processing of his/her personal

information. It is worth setting out the whole of this part of the *Privacy Policy*:

> "By providing http://ukip.org your email address (including by 'following,' 'liking,' linking your account to http://ukip.org, etc., on a third party website or network), you ***consent*** to our using the email address to send you http://ukip.org related notices, including any notices required by law, in lieu of communication by postal mail. You also agree that we may send you notifications of activity on http://ukip.org to the email address you give us, in accordance with any applicable privacy settings. We may use your email address to send you other messages, such as newsletters, changes to features of http://ukip.org, or other information. If you do not want to receive such email messages, you may opt out using the unsubscribe button at the bottom of any email.
>
> Following termination or deactivation of your http://ukip.org account, http://ukip.org may retain your profile information and user content for a reasonable time for archival purposes. Furthermore, http://ukip.org may retain and continue to use indefinitely all information (including user content) contained in your communications to other users or posted to public or semi-public areas of http://ukip.org after termination or deactivation of your account.
>
> http://ukip.org reserves the right, but has no obligation, to monitor the user content you post on http://ukip.org. We reserve the right to remove any such information or material for any reason or no reason, including without limitation if in our sole opinion such information or material violates, or may violate, any applicable law or to protect or defend our rights or property or those of any third party. http://ukip.org also reserves the right to remove information upon the request of any third party.
>
> Any information you provide, including your email address, will not be passed onto any third party (other than firms working on our behalf), except where you have signed a petition or similar, where the petition will be presented to a third party." (emphasis added)

46. Although there is only one reference using the word "consent", the next sentence refers to "agree" which we consider is in this context indistinguishable. More significantly, it is necessary to read the whole quoted passage as one. While the later paragraphs do not refer to consent being deemed to be given to the passing on of personal information to third parties working on UKIP's behalf by the provision of an email address, that is the sense of the passage. If a person does not want this to happen, they are given the choice of opting out. But otherwise, by providing their email address to UKIP they are consenting to it. Although not as clearcut as it might be, we consider that paragraph 1 of Schedule 3 is satisfied.

47. Although it is not necessary to consider whether paragraph 4 is also met, on balance we incline to the view that it probably is. Our doubt revolves around an ambiguity in paragraph 4 which is not resolved by any guidance from the courts or the Commissioner. The doubt is whether the processing must be carried out by the body or association or whether it can also cover processing carried out by a data controller in fulfilment of a contract with such a body or association. On the footing that it extends to the latter, paragraph 4 of Schedule 3 would also

be met.

48. In any event, because paragraph 1 of Schedule 3 is met, the processing by CA of sensitive personal data in the performance of the Contract will comply with the first data protection principle.

Second data protection principle

49. The second data protection principle is:

> "Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes."

50. CA must take care to ensure that their processing is not against the processes for which the data was collected. Paragraph 6 of Part II of Schedule 1 to the DPA explains:

> "In determining whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, regard is to be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed."

51. Given the nature of the datasets with which CA work it is unlikely that they will have been collected for a purpose that is incompatible with CA's processing.

52. In any event, we consider that all forms of the processing contemplated to be carried out under the Contract would be exempted from the second data protection principle by s 33 of the DPA 1998. That provides, so far as relevant:

> "(1) In this section- "research purposes" includes statistical or historical purposes; "the relevant conditions", in relation to any processing of personal data, means the conditions-
>
> (a) that the data are not processed to support measures or decisions with respect to particular individuals, and
>
> (b) that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.
>
> (2) For the purposes of the second data protection principle, the further processing of personal data only for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.
>
> (3)-(4) ...
>
> (5) For the purposes of subsections (2) to (4) personal data are not to be treated as processed otherwise than for research purposes merely because the data are disclosed-
>
> (a) to any person, for research purposes only,
>
> (b) to the data subject or a person acting on his behalf,
>
> (c) at the request, or with the consent, of the data subject or a person

acting on his behalf, or

(d) in circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within paragraph (a), (b) or (c)."

53. In short, there is unlikely to be any issue with the second data protection principle

Third data protection principle

54. The third data protection principle is:

"Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed."

55. Given the nature of the analysis performed by CA it is very unlikely that the third data protection principle will be contravened by the processing contemplated by the Contract.

Fourth data protection principle

56. The fourth data protection principle is:

"Personal data shall be accurate and, where necessary, kept up to date."

57. Paragraph 7 of Part II of Schedule 1 to the DPA explains:

"The fourth principle is not to be regarded as being contravened by reason of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in a case where-

(a) having regard to the purpose or purposes for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data, and

(b) if the data subject has notified the data controller of the data subject's view that the data are inaccurate, the data indicate that fact."

58. In these circumstances it is exceptionally unlikely that the fourth data protection principle will be breached by the processing contemplated by the Contract.

Fifth to eighth data protection principles

59. The remaining four data protection principles are:

"5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

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.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate

level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

60. These four principles can be dispensed with shortly.

61. So far as the fifth principle is concerned, CA must ensure that all personal data is destroyed once it has been processed and the Output has been produced. This should be recorded in the Contract.

62. The sixth principle is generally understood to mean that if a data subject makes a request under s 7 of the DPA (ie a "subject access request"), the data controller must comply with the requirements of ss 7-8.

63. Given the experience and expertise of CA, it is to be expected that it will be able to adhere to the seventh data protection principle. We note in this regard that all the data will be stored in secure premises and on secure systems.

64. In relation to the eighth data protection principle, CA will not be transferring any data outside the United Kingdom. Accordingly, that principle will not breached. Given that CA is foreign company, we consider it prudent that this be recorded in the Contract.

65. We therefore conclude, with the above caveats in mind that the CA system is lawful and its operation in general does not breach the DPA.

MATTHEW RICHARDSON
HENDERSON CHAMBERS
THE TEMPLE

PHILIP COPPEL QC
CORNERSTONE CHAMBERS
2-3 GRAY'S INN SQUARE

17 November 2015