

Data Protection: How should a Data Controller Respond to a Data Subject Access Request to Disclose an Email written by a Third Party that Refers to the Data Subject?

If you are a **data controller** and you have received a **Data Subject Access Request** to **disclose an email** with information sent to your organisation about the data subject by a third party, you should take legal advice, writes **Dr Rosanna Cooper**



A **data controller** must tread carefully. The main case dealing with this issue is the *Michael John Durant v Financial Services Authority* case and in this article you will find where appropriate, extracts from this case and legislation to clarify certain points.

The Scenario

A **contractor** has been working for your organisation in one of your offices in Europe for approximately 4 months primarily as a programme

director. She lives in the UK and there was a possibility of her returning to the UK to work for your London office.

In this role the contractor has to work at your **customer premises** to get the job done. This position requires the contractor to have certain skills, accreditations and experience which your organisation did not check as the contractor had all the right skills set and accreditations and experience in her CV when she was interviewed for the role, in particular, her technical capabilities.

The contractor had to visit one of your valued customer's premises and you sent her CV in advance of the visit. You received shortly after this feedback from a senior director of this customer who knows the contractor and had interviewed her for a role in their organisation and rejected her. **The senior director has informed you in an email that he would not accept the contractor working on their site or on any of their projects as the contractor has no technical qualifications.** To be fair to the contractor, she never said she had the particular qualification that this customer was looking for and had indicated during the interview that she was working towards this qualification. Your organisation had failed to check any qualifications or references before the contractor was appointed.

As soon as you received the email from the contractor you met with the contractor and informed her of the feedback from the customer and also that you had now informally contacted other people within the industry and received poor feedback on her technical capabilities. Shortly after the meeting the contractor sent a Data Subject Access Request requesting a copy of the email. Should you give the contractor a copy of the email?

The Law

Under the Data Protection Act 1998 ("DPA"), "**personal data**" relates to a living individual who can be identified from that data and other information which is in the possession of, or is likely to come into the possession of, the **data controller**.

Data means *information which is processed by computer or other automatic equipment, including word processors, databases and spreadsheet files, or information which is recorded on paper with the intention of being processed later by computer; or information which is recorded as part of a manual filing system, where the files are structured according to the names of individuals or other characteristics, such as payroll number, and where the files have*

sufficient internal structure so that specific information about a particular individual can be found easily. **Such data can include any expression of opinion** about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

In the Court of Appeal decision in *Michael John Durant v Financial Services Authority* [2003] EWCA Civ 1746, the Court of Appeal decided that a relevant filing system is limited to a system

“In which the files forming part of it are structured or referenced in such a way as clearly to indicate at the outset of the search whether specific information capable of amounting to personal data of an individual requesting it...is held within the system and, if so, in which file or files it is held; and which has, as part of its own structure or referencing mechanism, a sufficiently sophisticated and detailed means of readily indicating whether and where in an individual file or files specific criteria or information about the applicant can be readily located”

“...the purpose of section 7, in entitling an individual to have access to information in the form of his “personal data” is to enable him to check whether the data controller’s processing of it unlawfully infringes his privacy and, if so, to take such steps as the Act provides, for example in sections 10 to 14, to protect it. It is not an automatic key to any information, readily accessible or not, of matters in which he may be named or involved... Nor is to assist him, for example, to obtain discovery of documents that may assist him in litigation or complaints against third parties. As a matter of practicality and given the focus of the Act on ready accessibility of the information - whether from a computerised or comparably sophisticated non-computerised system - it is likely in most cases that only information that names or directly refers to him will qualify...”

“...It follows from what I have said that not all information retrieved from a computer search against an individual’s name or unique identifier is personal data within the Act. Mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data. Whether it does so in any particular instance depends on where it falls in a continuum of relevance or proximity to the data subject as distinct, say, from transactions or matters in which he may have been involved to a

greater or lesser degree. It seems to me that there are two notions that may be of assistance. The first is whether the information is biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised. The second is one of focus. The information should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest, for example, as in this case, an investigation into some other person's or body's conduct that he may have instigated. In short, it is information that affects his privacy, whether in his personal or family life, business or professional capacity. A recent example is that considered by the European Court in Criminal Proceedings against Lindquist, Case C-101/01 (6th November 2003), in which the Court held, at para. 27, that "personal data" covered the name of a person or identification of him by some other means, for instance by giving his telephone number or information regarding his working conditions or hobbies..."

Under the Data Protection Directive it further states that any information which relates to an identified or identifiable natural person (namely the contractor, the data subject) is personal data. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Key Definitions

- A **data controller** is any person who (alone or jointly with others) decides the purposes for which, and the manner in which, the personal data are **processed**. The definition of **processing** is very broad. It covers any operation carried out on the data and includes, obtaining or recording data, the retrieval, consultation or use of data, the disclosure or otherwise making available of data (see below).
- A **data subject** is any living individual who is the subject of personal data. There are no age restrictions on who qualifies as a data subject, but the definition does not extend to individuals

who are deceased.

As stated above, it is understood that the content of the email contained information pertaining to the contractor. The email contained information specific to the contractor and accordingly The contractor can be *identified* and/or is *identifiable* directly from the information.

According to the Information Commissioners Office (“ICO”), information can be considered to be **personal data** if **any** of the following questions can be answered in the affirmative:

- Does the data have any biographical significance in relation to the individual- that is, going beyond the recording of the putative data subject’s involvement in a matter or event that has no personal connotations...? “...information should have the putative data subject as its focus rather than some other person with whom he/she may have been involved or some transaction event...”
- Does the data ‘relate to’ the identifiable living individual, whether in personal or family life, business or profession?
- Is the data ‘obviously about’ a particular individual?
- Is the data ‘linked to’ an individual so that it provides particular information about that individual?
- Is the data used, or to be used, to inform or influence action or decisions affecting an identifiable individual?
- Does the data focus or concentrate on the individual as its central theme rather than on some other person or some object, transaction or event?
- Does the data impact or have the potential to impact on an individual, whether in a personal, family, business or professional capacity?

The Court issued a clear warning in *Michael John Durant v Financial Services Authority* to litigants that the DPA: “...is not an automatic key to any information, readily accessible or not, of matters of matters in which he may be named or involved. ... Nor is to assist him...to obtain discovery of documents that may assist him in litigation or complaints against third parties...”

Therefore, the information contained in the **email** would amount to **personal data** for the purposes of the **DPA** if **you were able to answer any of the above questions in the affirmative**. As data controller you would therefore have certain **responsibilities** in relation to the processing of any **personal data that was obtained, stored or used**.

Data Controller's Responsibility

As **Data Controller** you must comply with all **eight data protection principles** when **processing personal data**. In this regard, as **Data Controller** you should pay particular attention to the **first principle as detailed in the DPA**.

First Principle

Under the first data protection principle: **personal data must be processed fairly and lawfully** and, in particular, must not be processed unless at least one of the specified conditions which apply to all personal data is met. In determining for the purposes of the first data protection principle whether personal **data is processed fairly**, regard is to be had to the method by which the data was obtained, which **in the contractor's case was lawful** (an email was sent to you and you informed her of the content plus you were interviewing her for the purposes of hiring her). **The contractor was not deceived or misled as to the purpose or purposes for which the data was collected and/or to be processed**.

'Processing' covers the majority of operations that can be carried out in respect of data, and includes **printing, publishing, viewing on a computer screen, as well as a wide variety of other operations**.

The conditions are as follows:-

- (1) *'The data subject has given his consent to the processing.'*
- (2) *'The processing is necessary:*
 - (a) *for the performance of a contract to which the data subject is a party, or*
 - (b) *for the taking of steps at the request of the data subject with a view to entering into a contract.'*

- (3) *The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.*
- (4) *The processing is necessary in order to protect the vital interests of the data subject.*
- (5) *The processing is necessary:*
- (a) *for the administration of justice,*
- (b) *for the exercise of any functions conferred on any person by or under any enactment ...*
- (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.*

Therefore, the **reviewing, storing, printing and/or disseminating of the email containing the contractor's personal data would amount to the processing of that data and therefore must be processed in accordance with one of the conditions above.**

What has to be deduced?

Generally, an individual needs to know **what information is held about that individual** in order to have an opportunity of remedying an error or false information. **A Data Subject Access Request is made under section 7 of the DPA.**

Section 7(4) to (6) and 8(7) of the DPA provide:

- "7(4) Where a data controller cannot comply with the request [i.e. for information under section 7(1)] without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request unless -*
- (a) the other individual **has consented to the disclosure of the information to the person making the request, or***
- (b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual, or*

(c) the information is contained in a health record and the other individual is a health professional who has compiled or contributed to the health record or has been involved in the care of the data subject in his capacity as a health professional [added by the Data Protection (Subject Access Modification) (Health) Order 2000, SI 2000/413].

(5) In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request; and that subsection is not to be construed as excusing a data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise.

(6) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to -

*(a) **any duty of confidentiality owed to the other individual,***

(b) any steps taken by the data controller with a view to seeking the consent of the other individual,

(c) whether the other individual is capable of giving consent, and

(d) any express refusal of consent by the other individual.”

“8(7) For the purposes of section 7(4) and (5) another individual can be identified from the information being disclosed if he can be identified from that information, or from that and any other information which, in the reasonable belief of the data controller, is likely to be in, or to come into, the possession of the data subject making the request.”

Section 7(9) provides:

“If a court is satisfied on the application of any person who has made a request under the foregoing provisions of this section that the data controller in question has failed to comply with the request in contravention of those provisions, the court may order him to comply with the request.”

The rights of data subjects - under the DPA are as follows:

- *rights of access to personal data;*
- *rights to prevent processing likely to cause damage or distress;*
- *rights to prevent processing for purposes of direct marketing;*
- *rights in relation to automated decision taking;*
- *rights of data subjects in relation to exempt manual data;*
- *rights to seek rectification, blocking, erasure and destruction of inaccurate data; and*
- *rights to make a request for assessment (such requests are made to the Information Commissioner).*

The main question to address is **whether the content of the email amount to personal data** for the purposes of the DPA? If it does, then as data controller you **have to determine whether the data relates to the contractor or the main focus of the email was concerned with the contractor**. If the content of the email relates to the contractor or the main focus of the email is about her, then the content will have to be disclosed to her as part of a Data Subject Access Request.

If you have deduced that the **content of the email amounts to personal data** of the contractor, you need to consider whether in accordance with section 7(4)(b) of the DPA, it is “**reasonable in all the circumstances**” to disclose the **identity of the other individual** supplying the data without obtaining consent where such data may identify the source of the information and whether you owe a duty of confidentiality to the discloser.

In the Court of Appeal decision in *Michael John Durant v Financial Services Authority [2003] EWCA Civ 1746*, the Court of Appeal decided that:

*“...The data subject may have a legitimate interest in learning what has been said about him and by whom in order to enable him to correct any inaccurate information given or opinions expressed. The other may have a justifiable interest in preserving the confidential basis upon which he supplied the information or expressed the opinion. Sections 7(4)-(6) and 8(7) - prompted by the European Court's decision in *Gaskin v. United Kingdom [1990] 1 FLR 167, ECtHR, at para. 49* - provide a machinery for balancing their respective interests, and do so compatibly with Articles 12 and 13.1(g) of the Directive, which, as Mr. Sales observed, mirrors the*

balance provided by Article 8.2 to 8.1 ECHR. Article 12, to which section 7 of the 1998 Act is intended to give effect, provides a right of access for every data subject to his personal data, which it describes as a “guarantee”. And Article 13 permits member states to adopt legislative measures to restrict such right when necessary to safeguard various specified interests, including, in paragraph 1(g), the protection of the rights and freedoms of others. The protection that the 1998 Act gives to other individuals is similarly qualified, reflecting, in this respect, the principle of proportionality in play between the interest of the data subject to access to his personal data and that of the other individual to protection of his privacy...”

“...It is important to note that the question for a data controller posed by section 7(4)(b) is whether it is reasonable to comply with the request for information notwithstanding that it may disclose information about another, not whether it is reasonable to refuse to comply. The distinction may be of importance, depending on who is challenging the data controller's decision, to the meaning of “reasonable” in this context and to the court's role in examining it. The circumstances going to the reasonableness of such a decision, as I have just noted, include, but are not confined to, those set out in section 7(6), and none of them is determinative. It is important to note that section 7(4) leaves the data controller with a choice whether to seek consent; it does not oblige him to do so before deciding whether to disclose the personal data sought or, by redaction, to disclose only part of it. However, whether he has sought such consent and, if he has done so, it has been refused, are among the circumstances mentioned in the non-exhaustive list in section 7(6) going to the reasonableness of any decision under section 7(4)(b) to disclose, without consent...”

You need to determine whether the details ought to be redacted. It arguably does not form part of his personal data so it could be redacted.

*“...Where a data controller cannot comply with the request without disclosing information about another individual who can be identified from the information”. .if such information about another is not necessarily part of personal data sought, no question of section 7(4) balancing arises at all. The data controller, whose primary obligation is to provide information, not documents, **can**, if he chooses to provide that information in the form of a copy*

document, simply redact such third party information because it is not a necessary part of the data subject's personal data.

66. The second stage, that of the section 7(4) balance, only arises where the data controller considers that the third party information necessarily forms part of the personal data sought...

“... Where the third party is a recipient or one of a class of recipients who might act on the data to the data subject's disadvantage (section 7(1)(b)(iii)), his right to protect his privacy may weigh heavily and obligations of confidence to the third party(ies) may be non-existent or of less weight. Equally, where the third party is the source of the information, the data subject may have a strong case for his identification if he needs to take action to correct some damaging inaccuracy, though here countervailing considerations of an obligation of confidentiality to the source or some other sensitivity may have to be weighed in the balance. It should be remembered that the task of the court in this context is likely to be much the same as that under section 7(9) in the exercise of its general discretion whether to order a data controller to comply with the data subject's request (see para. 74 below). In short, it all depends on the circumstances whether it would be reasonable to disclose to a data subject the name of another person figuring in his personal data, whether that person is a source, or a recipient or likely recipient of that information, or has a part in the matter the subject of the personal data. Beyond the basic presumption or starting point to which I referred in paragraph 55 above, I believe that the courts should be wary of attempting to devise any principles of general application one way or the other.

Conclusion

The first question for you as the data controller when considering a Data Subject Access Request is **whether the information sought is capable of being that person's personal data within the definition of the DPA**, regardless of whether it is held in computerised or manual form.

You have certain responsibilities in relation to any personal data in respect of any individual that is obtained, stored or used.

Author: Dr Rosanna Cooper who is a data protection lawyer specialising in data protection, website security and data security law. Please contact a solicitor by email: enquiries@rtcooperssolicitors.com or tel: 0207 488 9947. For more information on the services we provide at RT Coopers on [data protection](#), visit http://www.rccoopers.com/practice_dataprotection.php

Tags

Data protection lawyers, data protection law firm, DPA solicitors, law, data protection lawyer, DPA lawyers, data processor