



Blackstone
CHAMBERS

Presented by IRS in association with Blackstone Chambers

“Employment Law in the High Court”

Friday 25th February 2005

DATA PROTECTION IN THE HIGH COURT

KATE GALLAFENT

Blackstone Chambers, Blackstone House, Temple, London EC4Y 9BW
Tel: +44(0)20-7583 1770 Fax: +44(0)20-7822 7350 Email: clerks@blackstonechambers.com
www.blackstonechambers.com

DATA PROTECTION IN THE HIGH COURT

ROUTES TO THE HIGH COURT

1. Under the Data Protection Act 1998 a data subject is able to apply to the High Court for:
 - (a) An order requiring a data controller to comply with a **subject access request** (section 7(9) DPA).
 - (b) An order requiring a data controller to cease or not to start **processing data in a manner likely to cause damage or distress** (section 10(4) DPA).
 - (c) An order preventing a data controller processing data for the purposes of **direct marketing** (section 11(2) DPA).
 - (d) An order that a person taking a decision which significantly affects the data subject based solely on **automatic processing** reconsider the decision, or take a new decision not solely based on such processing (section 12(8) DPA).
 - (e) An order that a data controller rectify, block, erase or destroy **exempt manual data** which are **inaccurate or incomplete**, or cease holding such data in a way incompatible with legitimate purposes pursued by the data controller (section 12A(3) DPA).
 - (f) An order that a data controller rectify, block, erase or destroy data which are **inaccurate** (section 14(1) DPA). Where the data accurately records information received or obtained from the data subject or a

third party (and the fourth principle¹ has been observed), the Court may instead make an order requiring the data to be supplemented by an approved statement of the true facts (section 14(2)(a) DPA), or, where it has not, make such order as it thinks fit for securing compliance (section 14(2)(b) DPA). The Court can also order the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction of data where it makes an order to that effect (section 14(3)&(5)).

2. Save in respect of an application under section 7 (subject access request) or under section 14 (inaccurate data), before applying to the Court under these provisions it is necessary for the data subject first to serve a formal notice on the data controller seeking the desired relief. The Court's jurisdiction in these cases is based upon the data controller's alleged failure to comply with the notice. However, an application under section 14 is entirely freestanding, and requires no prior formal notice.
3. The Court may award an individual compensation where:
 - (a) He suffers damage by reason of any contravention by a data controller of any of the requirements of the DPA (section 13(1) DPA).

¹ "Personal data shall be accurate and, where necessary, kept up to date." 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 (Schedule 1, Part II, paragraph 7).

- (b) He suffers distress by reason of such contravention in addition to damage, or the contravention relates to the processing of data for the special purposes² (section 13(2) DPA).
4. It should be noted that in order to obtain compensation the individual concerned need not be the data subject: rather, he simply needs to have suffered damage by reason of a contravention by a data controller.
 5. It is important to distinguish between the role of the Court and that of the Information Commissioner in this context. A data subject may request that the Information Commissioner assess whether it is likely or unlikely that processing has been or is being carried out in contravention of the DPA (section 42 DPA). The Commissioner must notify the data subject, to the extent that he considers appropriate, of 'any view formed or action taken as a result of the request', in other words, whether it is 'likely or unlikely' that there has been a breach of the DPA (section 42(4) DPA). Such an assessment does not bind the court in any way.
 6. That is not to say that the Information Commissioner is without any real powers: if he is satisfied that there was or is a contravention of any of the data protection principles, he can serve a notice requiring the data controller to take (or refrain from taking) specified steps, or refrain from processing particular data (section 40(1) DPA). A person who fails to comply with an enforcement notice is guilty of an offence (section 47 DPA). However, it nevertheless remains the case that in order for an individual to obtain relief (and compensation) under sections 7 - 14, the Court must nevertheless find for itself that there was a relevant violation.

² "the special purposes" means any one or more of the following (1) the purposes of journalism, (b) artistic purposes, and (c) literary purposes.

WHAT ARE PERSONAL DATA?

7. The DPA defines 'personal data' as being:

“data which relate to a living individual who can be identified –

- (a) from those data, or
- (b) from those data and other information which is in the possession of, the data controller,

and includes 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” (section 1(1) DPA)

8. In order to fall within the ambit of the DPA, the 'data' must be processed by means of equipment operating automatically in response to instructions given for that purpose, or be recorded as part of 'relevant filing system'³.

9. In Guidance issued in March 2002⁴ the Information Commissioner provided examples of what sort of data would be likely to fall within the definition of 'personal data' in the employment context:

“Examples of personal data likely to be covered by the DPA

³ Or, in either case, be recorded with such intention. “Relevant filing system” means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. Data also falls within the DPA where it forms part of an 'accessible record', being a 'health record, 'educational record' or 'accessible public record' (section 68 DPA).

⁴ The Employment Practices Data Protection Code Part 1: Recruitment and Selection. There are three further parts: Part II: employment records, about collecting, storing, disclosing and deleting records, Part II: monitoring at work, about monitoring workers' use of telephone or email systems and vehicles, and Part IV: medical information, about occupational health, medical testing, drug and genetic screening.

- Details of a worker's salary and bank account held on an organisation's computer system or in a manual filing system
- An email about an incident involving a named worker
- A supervisor's notebook containing sections on several named individuals
- A supervisor's notebook containing information on only one individual but where there is an intention to put that information in the worker's file
- A set of completed application forms

Examples of information unlikely to be covered by the DPA

- Information on the entire workforce's salary structure, given by grade, where individuals are not named and are not identifiable
- A report on the comparative success of different recruitment campaigns where no details regarding individuals are held
- A report on the results of "exit interviews" where all responses are anonymised and where the results are impossible to trace back to individuals
- Manual files that contain some information about workers but are not stored in an organised way, such as a pile of papers left in a basement

In practice, therefore, nearly all useable information held about individual workers will be covered by the Code."

i. Durant v Financial Services Authority⁵

10. Mr Durant applied under section 7(9) DPA for an order that the Financial Services Authority comply with his subject access request. The background to his request was that had complained to the FSA about Barclays Bank PLC, of which

⁵ [2003] EWCA Civ 1746, Judgment 8 December 2003.

he had been a customer, who had in turn investigated and closed its investigation without informing him of the outcome. The FSA provided copies of documents held in its computerised records, but refused his request in respect of information held on manual records, on the basis that it did not constitute “personal data”.

11. The Court of Appeal identified four issues:

- (a) What makes ‘data’ ‘personal’?
- (b) What is meant by a ‘relevant filing system’, so as to render personal information recorded in such a system ‘personal data’ disclosable under section 7?
- (c) How should a data controller approach the issue of when it is ‘reasonable in all the circumstances’ to comply with a request under section 7, even though it contains information about a third party who has not consented to its disclosure?⁶
- (d) When should the Court exercise its discretion to order a data controller to comply with a section 7(1) request?

12. The Court answered those questions in the following way:

- (a) For information to constitute ‘personal data’ it should have the data subject as its focus, rather than some transaction or event in which he

⁶ A data controller may refuse disclosure where the personal data requested discloses information relating to another individual unless that individual has consented or where it is “reasonable in all the circumstances to comply with the request without the consent” (section 7(4) DPA), in determining which 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.” (section 7(6)).

may have figured or have had an interest. It is not enough that a document be retrievable by reference to the individual's name.

- (b) A 'relevant filing system' is a system in which the files are structured so as to indicate at the outset of the search whether specific information capable of amounting to 'personal data' is held therein, and if so where, and must be of sufficient sophistication to provide the same or similar ready accessibility as a computerised filing system.
- (c) The approach to the redaction of information where another individual is named or identifiable is a two-stage process:
 - i. First, data controllers should consider what "legitimate interest" the data subject may have in requiring disclosure of the identity of another individual named or identifiable from personal data to which he is otherwise entitled, and whether such information is necessary part of the personal data requested;
 - ii. Secondly, where such data is a necessary part, the data controller must balance the data subject's rights with the obligations of confidentiality to the other party or to some other sensitivity that would require non-disclosure.
- (d) The Court's discretion is general and untrammelled.

13. The Information Commissioner subsequently issued Guidance on the impact of *Durant*⁷. So far as the issue of 'personal data' is concerned, he highlighted the relevance of considering whether or not the information is capable of having an

7

<http://www.informationcommissioner.gov.uk/cms/DocumentUploads/webversion%204%2004.10.042.pdf>

adverse impact on the individual's privacy in cases where it is not clear whether information relates to him.

14. In relation to the issue of 'relevant filing system', the Information Commissioner concluded "following the Durant judgment it is likely that very few manual files will be covered by the provisions of the DPA. Most information about individuals held in manual form does not, therefore, fall within the data protection regime."
15. The Guidance was updated to include a "Frequently Asked Questions" section. This introduces the "temp test" to assist a data controller in ascertaining whether he has a 'relevant filing system'. The "temp test" asks: if you employed a temporary administrative assistant would they be able to extract specific information about an individual without any particular knowledge of your type of work or the documents you hold?

ii. **Freedom of Information Act 2000**

16. The Freedom of Information Act came into force on 1 January 2005, creating a new right to request information from public authorities. Three points arise in relation to the DPA.
17. First, the DPA itself was amended by the FOI to expand the definition of data by adding an additional category of data known as 'category "e" data'. Category "e" data is "recorded information held by a public authority and does not fall within any of paragraphs (a) to (d) of section 1(1) of the DPA", i.e. it need not be held on a computerised or relevant filing system. However, a public authority is not obliged to comply with a request for such personal data under section 7(1) unless the request contains a description of the data, and, in any event, may decline to comply if the authority estimates that the costs of complying with the request so far as relating to those data would exceed the appropriate limit

(section 9A DPA). The appropriate limit under the Freedom of Information regime is currently set at £600 for 'central' public authorities⁸, and £450 for all others⁹. This equates to approximately 3 days at the stated rate of £25 per hour.

18. Secondly, the FOI expressly categorises as "exempt information" information which constitutes personal data of which the applicant is the data subject (section 40(1) FOI). Thus it is not possible to seek to circumvent the provisions of the DPA by making the equivalent of a subject access request under the FOI.
19. Thirdly, if the information requested consists of personal data of a person other than the applicant, it is exempt from disclosure if that would breach any of the data protection principles, or processing of which would be likely to cause distress or damage (section 40(2) FOI).

SUBJECT ACCESS REQUESTS: JOHNSON V MEDICAL DEFENCE UNION¹⁰ (I)

20. Mr Johnson was dissatisfied with the Medical Defence Union's response to his subject access request. He applied to the Court (i) for an order under section 7(9) DPA that the Medical Defence Union comply with his subject access request, (ii) for an order under section 10(4) DPA to prevent the MDU improperly processing information about him, (iii) for an order under section 14(4) DPA for the rectification, blocking or destruction of certain data, and (iv) for compensation under section 13 DPA for damage and distress.
21. The issue of compliance with his subject access request was ordered to be determined as a preliminary issue. It was determined by Laddie J. on 20

⁸ Namely, any Government Department, the House of Commons, the House of Lords, the Northern Ireland Assembly, the National Assembly for Wales, and the armed forces of the Crown (save for Special Forces and those assisting GCHQ) (Part I of Schedule 1 of the Freedom of Information Act).

⁹ SI 2004 No. 3244

¹⁰ [2004] EWHC 347 (Ch)

February 2004, shortly after the Judgment in *Durant*. The following issues of importance arise.

- (a) The date at which information must be 'data' within the meaning of section 1(1) DPA for it to be disclosable is that of the date of the request.
 - (b) A summary of entries, none of which contain personal data, may nevertheless itself constitute personal data disclosable under section 7.
 - (c) The ancillary right to have communicated information as to the recipients of the data (section 7(1)(b)(iii) DPA) should be construed narrowly, and does not cover every hand through which data have passed.
 - (d) In deciding how to respond to a request for information which includes information as to third parties, the statement in *Durant* that the data controller should be entitled to ask what, if any legitimate interest the data subject had in disclosure of the identity of that third party (paragraph 61) does not impose an obligation on the data controller to enquire of the data subject why he wants the information. Rather, the data controller is entitled to ask himself, based on all the material before him (including any reasons communicated to him by the data subject) what are the reasons or likely reasons for wanting such information, and the relevance and force of any such reasons.
22. Applying these principles, Laddie J. held that there was no 'significant fault' in the way in which the MDU had responded to his request.

IV. Disclosure: Johnson v Medical Defence Union¹¹ (II)

23. Mr Johnson was refused leave to appeal against the decision by Laddie J. on the preliminary issue and by the Court of Appeal. Mr Johnson's case was therefore set down for trial in January 2005.
24. However, in around October 2004 Mr Johnson made an application for specific disclosure which, in substance, covered all the documents which were the subject of the previous application.
25. He argued that although the right to bring proceedings is created by the DPA, the conduct of such proceedings had to be in accordance with the provisions of the CPR including in particular the obligation on the parties to give disclosure of documents.
26. The MDU argued that the express limitations on disclosure provided by the DPA would be undermined by such an application for disclosure, and that the legislature had indicated that disclosure should not be ordered in such a case, hence even if the Court retained jurisdiction to order disclosure, it should always be exercised in accordance with the legislative intent.
27. Laddie J., noting that the application gave rise to a point which might be of some general importance, considered the structure and scope of the DPA. In essence, the data subject's ability to make use of the safeguards given to him by sections 10 to 14 DPA were dependent upon knowing what personal data relating to him was controlled, and how it has been or will be processed or used by the data controller. To this end, section 7 establishes a right to find out whether personal data are being processed, and if so, how, but is not concerned with whether the data controller is acting improperly.

¹¹ [2004] EWHC 2509 (Ch).

28. The MDU argued that the legislative intent, confirmed by the wording of section 15(2), was to prevent data subjects obtaining disclosure. Section 15(2) provides that in determining an application under section 7(9) the Court can order the information constituting any data to be made available for its own inspection, but “shall not, pending the determination of that question in the applicant’s favour, require the information sought by the applicant to be disclosed to him or his representatives whether by discovery or otherwise”.
29. Laddie J. held that ‘as attractive as this argument may appear, I do not think it is right’. As section 15(2) is only concerned with applications under section 7(9), and is not concerned with whether there has been a breach of the data protection principles by the data controller, it has no direct bearing on whether there should be disclosure, or its extent, in proceedings where the data subject has made out an arguable case that there has been such a breach.
30. He pointed out that documents which might be highly material to an allegation of breach of the data protection principles and would fall within the ambit of disclosure might well not be personal data within the meaning of the DPA and therefore not within the scope of sections 7 and 15.
31. However, he emphasised that whilst section 15(2) has no direct bearing on whether there should be disclosure, it does have some indirect impact, in that the Court should bear in mind the concern of the legislature that confidential information relating to third parties should not be disclosed to a data subject. It may therefore reinforce the Court in a decision either to refuse disclosure in whole or in part or to allow redaction of documents.

KATE GALLAFENT

Blackstone Chambers

February 2005