FROM THE RIGHT HONOURABLE THE LORD IRVINE OF LAIRG

HOUSE OF LORDS,
LONDON SW1A 0PW

CS
cc: GR
SS
OMC.

24 August, 2001

Hazel Blears
Parliamentary Under Secretary of State (Health)
Department of Health
Richmond House
79 Whitehall
LONDON SW1A 2NS

Dear Hazel,

CHARGES FOR ACCESS TO MANUAL HEALTH RECORDS UNDER THE DATA PROTECTION ACT 1998

Thank you for your letter of 9 August seeking the agreement of CRP (FOI) to the retention after 24 October 2001 of the £50 maximum fee for subject access to manually held health records under the Data Protection Act 1998.

This letter gives CRP(FOI) clearance for your proposal, subject to it being made clear when the decision is announced that the retention of the £50 limit is intended as a temporary measure, pending discussions with the Information Commissioner with a view to finding an alternative long-term solution.

Stephen Twigg has commented, on behalf of Robin Cook. He is content with your proposal, but he makes clear that there should be a strong presumption against recourse to primary legislation to carry forward any alternative arrangements which might appear attractive in the immediate future. No other colleague has commented.

As Minister with responsibility for data protection policy, my own view is that we should do what we can to bring the subject access fee for manually held health records into line with the standard fee for access to other categories of record, including computerised health records. As you know, the standard fee is currently £10. £50 can be a significant amount for many patients. Having said that, I recognise the difficulties that allowing the fee to drop to £10 on 24 October would cause for GPs and others in the health sector. I welcome the Information Commissioner's helpful suggestion of discussions to try and resolve the difficulties and find an agreed way forward. This clearly cannot be done by 24 October. Accordingly, I believe that the right way forward is, as you suggest, to amend the relevant Regulations to retain the £50 for the time being. We should, however, make clear publicly that this is a temporary measure to permit discussions to take place with the Information Commissioner so as to find a long-term solution.

You therefore have CRP(FOI) approval to proceed on this basis, having regard to Stephen Twigg's point about primary legislation. I should be grateful if your officials could liaise closely with mine on the drafting of the amending Regulations, the handling of the announcement and the arrangements for the discussions with the Information Commissioner.

I am copying this letter to the Prime Minister, the other members of CRP (FOI) and to Sir Richard Wilson.

Yours ever,

Derry

File

CS

RtL 20/8

SS
JR
OML

Stephen Twigg MP
Parliamentary Secretary

PRIVY COUNCIL OFFICE
No.2 Carlton Gardens
London
SW1Y 5AA

020 7210 1020
(Fax) 020 7210 1073
stephen.twigg@cabinet-office.x.gsi.gov.uk

17th August 2001

Dear Lord Chancellor,

CHARGES FOR ACCESS TO MANUAL HEALTH RECORDS UNDER THE DATA PROTECTION ACT 1998

I am replying on behalf of the Leader of the Commons to Hazel Blear's letter of 9th August to you about charges for access to manual health records.

Hazel's letter of 9th August sought agreement from CRP (FOI) Committee to pursue secondary legislation to retain the current £50 maximum fee that can be charged for providing individuals with access to their manual records after 24 October 2001.

I have no objections to DH using secondary legislation to extend the time period during which the current £50 maximum fee can be charged. I understand that Hazel's officials are looking at ways in which the cost of access can be reduced in the future, for example by promulgating guidance about a sliding scale of fees or the use of new technology, in response to the likelihood of continuing pressure to do so. I would only wish to point out at this stage that there should be a strong presumption against recourse to primary legislation to carry forward any alternative arrangements in this area which might appear attractive in the immediate future.

I am copying this letter to the Prime Minister, members of CRP (FOI) and LP Committees, and to Sir Richard Wilson and First Parliamentary Counsel.

Yours sincerely,

STEPHEN TWIGG MP
(approved by the Minister and signed in his absence)

The Rt Hon The Lord Irvine of Lairg
Lord Chancellor

THE TREASURY SOLICITOR

Queen Anne's Chambers, 28 Broadway, London SW1H 9JS

Direct Line 020 7210 3450 Direct Fax 020 7210 3503 e-mail: rjeffreys@treasury-solicitor.gsi.gov.uk

Cabinet Office and Central Advisory Division

RF CJ 5/09

RF CJ 27/09

Please quote:

Your reference:

F

Jonathan Tross
Constitution Secretariat
Cabinet Office
4 Central Building
Matthew Parker Street
London SW1

Date: 10 August 2001

Dear Jonathan,

ADVICE ON DATA PROTECTION

I think you mentioned at the meeting with Lee Hughes the other day that you had still not seen a copy of the final version of the advice by Philip Sales and Jemima Stratford. Tessa Sterling circulated a copy round the data practitioners group and I am sorry that I assumed you would have received it that way, as I did. I enclose a copy for you now. It occurs to me that Clare Sumner and Pat Dixon will not have received one either and I enclose a copy for each of them also, with apologies for omitting to do so before. Pat, in particular, will be pleased to see the more optimistic advice on back-up data than we had feared.

yours,

Rosemary

ROSEMARY JEFFREYS

Cc Clare Sumner, No ~~10~~
Pat Dixon, No 10
Richard Heaton, Legal Adviser Constitution Secretariat

in the matter of subject access requests under s.7 of the data protection act 1998

---

joint advice

We are asked to advise Government departments in relation to a number of issues arising under the Data Protection Act 1998 ("the DPA"). Specific questions and areas of concern have been raised by departments including the Cabinet Office, the Department for Trade and Industry ("DTI"), the Department for Culture, Media and Sport ("DCMS"), the Department of Social Security Inland Revenue, the Legal Secretariat to the Law Officers ("LSLO") and MAFF.

We are instructed that the issues have arisen in the context of subject access requests made to several departments. We have most helpfully been provided with the results of certain such subject access requests, in order to provide examples of the context in which issues under the DPA may arise and to illustrate the difficulties encountered in conducting such an exercise. It is not appropriate in this advice to address the specific issues and difficulties which were raised by those requests, but we should be happy to advise separately on those issues, and suggest that this could perhaps most easily be done in conference.

It appears to us that the issues raised in our instructions fall into four broad groups:

Definitions;

Sections 7 and 8 of the DPA;

E-mails and other computer-related matters;

Disputes and legal professional privilege.

Accordingly, we address the issues under those broad headings and in turn.

In summary, our main conclusions are:

In the case of a Government department, it is most unlikely that individual officials working within the department who have responsibility for a particular database would be "data controllers" within the meaning of the DPA;

A reference to an individual's name alone is not in itself "personal data" within the meaning of the DPA, but thought will have to be given in any case to the question whether the particular context in which the name appears imports information about that individual falling within the concept of "personal data";

The question as to whether a particular manual record or file is a "relevant filing system" will be a question of fact in every case, and files or systems which do not have any clear systematic internal indexing mechanism probably do not fall under the definition contained in the DPA;

A data controller is not obliged to provide a copy of the actual document in which the personal data is contained, but may choose whether to provide either a redacted copy of the actual document showing only the personal data to which the individual is entitled, or an intelligible communication which has been prepared for the purposes of the subject access request and containing the personal data;

S.8(2)(a) of the DPA provides an exemption from the obligation to supply a copy of the information in permanent form where to do so would involve disproportionate effort, but probably does not provide an exemption from the obligation to supply the information itself constituting the personal data (as opposed to the information in permanent form) on the ground that providing the information (as opposed to the information in permanent form) will involve disproportionate effort;

S.8(3) cannot properly be read so as to exempt a data controller from complying with a s.7 request for access to information where that individual has made only one such request, albeit the request is one of many such requests made at the same time (perhaps as part of an orchestrated campaign);

In every case where a data subject is entitled to have communicated to him in intelligible form information which constitutes his personal data, but which will also disclose information relating to another individual (be it a Minister, an official, or a Third Party as defined in s.70 of the DPA), the data controller must conduct a balancing exercise taking account of the particular circumstances of the individual case in order to decide whether the information relating to the other individual should

be disclosed. The reference in s.7(1)(b)(iii) to "recipients or classes of recipients" may be read as giving the data controller a choice as to whether to provide individual names (where they have been stated) or only a generic description of the classes of recipients;

Under s. 7(3), a data controller may only ask for further information in so far as it is reasonably required to locate the information sought by the data subject. Thus further questions may be asked in so far as reasonably necessary, but should be directed towards and framed so as to refer to how the data controller may more readily locate the information sought. Where a data subject refuses to supply further information reasonably required so that the data controller can satisfy himself as to the identity of the person making the request, the data subject may not rely on Article 8 of the European Convention on Human Rights to defeat the s.7(3) exemption;

There is a reasonable argument that e-mails which have been deleted from the "live" system would no longer count as personal data which are being "processed" for the purposes of the DPA. If, on the other hand, they are being processed, they will benefit from the transitional exemption for back-up data, so long as they are only held for the purposes specified in paragraph 12 of Schedule 8 to the DPA, and for no other purposes. But then, when the transitional period expires, there would be no exemption in relation to them. Similar considerations apply to back-up or archive data, so that when the transitional period expires there will be no exemption in relation to them;

Searching an employee's e-mails would often involve processing personal data of that employee, and may on occasion involve the processing of sensitive personal data (depending on their particular content). Departments which do not currently inform their employees that e-mails may be monitored for lawful purposes should introduce some such message or in some other way obtain the consent of their employees to monitoring;

A retention schedule will provide good prima facie evidence of routine processing which would have taken place in any event, so that such checking and deletion could continue after receipt of a subject access request;

Where Government departments retain records in relation to individuals such as former employees due to concern that the individuals may bring some proceedings against the department in the future, it is very likely that one or more of the Schedule 2 conditions would be held to be fulfilled and that at least one of the Schedule 3

conditions would be held to be fulfilled, so that the records could lawfully be retained for so long as there was a reasonable basis for the view that they might be needed in the future. Where records relating to such individuals have been retained in anticipation of possible proceedings, those records remain liable to a subject access request under s.7 of the DPA unless the data controller can rely upon one of the miscellaneous exceptions provided for in Schedule 7 to the DPA;

Other than cases where reliance may be placed on one of the exemptions to s.7 provided for under the DPA (for example, the legal professional privilege exemption), there is no general right to refuse a subject access request on the grounds of current or imminent legal proceedings and/or a failed application for disclosure in the legal proceedings themselves;

The words of s.29(1) of the DPA are wide enough to cover a situation where disclosure of tax related personal data to a data subject will not prejudice the assessment or collection of tax owed by that data subject (taking him on a stand alone basis), but would be likely prejudice the assessment or collection in the future of "any tax", whether due from the data subject or other persons;

We consider that a claim to legal professional privilege could be maintained in legal proceedings in respect of a vexatious litigant submission. Consideration of European law and of rights under the Convention do not significantly weaken these arguments. This conclusion also applies more generally to other internal legal advice generated within Government departments, for which we consider legal professional privilege could be maintained.

The proper approach to construction of the DPA

The DPA implements into UK law Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("the Directive"). The domestic courts are under a strong obligation to interpret domestic legislation so as to give it a construction which is compatible with the underlying EC instrument which it implements, wherever it is possible to do so – including, where necessary, giving the domestic statute a strained meaning if it is necessary to achieve such compatibility: see e.g. *Litster v Forth Dry Dock and Engineering Co Ltd* [1990] 1 AC 546.

In turn, the issuing of the Directive was governed by general principles of EC law,

including the principle of proportionality: see generally Tridimas, *The General Principles of EC Law*, Chap. 3. The principle requires that the individual should not have his freedom of action limited beyond the degree necessary in the public interest: ibid. p. 89. The principle provides a ground for review of Community measures. In our view, for that reason, the principle is also capable of providing some guidance as to the proper construction of Community measures. It is more likely that Community institutions will intend to legislate in accordance with fundamental principles of EC law than contrary to them.

This point may have some bearing on the proper interpretation of the Directive, and hence on the proper interpretation of the DPA. It may be observed that at points the Directive expressly makes allowance for less strict controls in relation to processing of data where processing is unlikely adversely to affect the rights and freedoms of the data subject: see recital (49) and Article 18(2).

Further, one objective of the Directive is to give protection uniformly throughout the EC to fundamental rights and freedoms, "notably the right to privacy, which is recognised … in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms ["the ECHR"]" (recital (10)), and it is noticeable that the Directive at certain points adopts language and concepts apparently derived from or similar to those of the ECHR – see e.g. Articles 9 and 13(1)(g) of the Directive. We consider that, in view of this objective, consideration of the position under Article 8 of the ECHR may also provide some guidance as to the proper construction of the Directive.

(a) Definitions

Data Controller

Section 1 of the DPA provides in relevant part:

> "(1) … 'data controller' means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;
> …
> (4) Where personal data are processed only for purposes for which they are required by or under any enactment to be processed, the person on whom the obligation to process the data is imposed by or under that enactment is for the purposes of this Act the data controller."

A data controller may engage a "data processor", who is not an employee, to process personal data on their behalf (s.1(1) DPA). A data controller may also nominate a representative for the purposes of the DPA, whose name and address

must be registered (s.16(1)(b)) (and must nominate such a representative if established outside the EEA – s. 5(2)).

The Directive defines "controller" in Article 2(d) as the person who "determines the purposes and the means of the processing of personal data", and expressly recognises that this could be a natural or legal person and could be a public authority.

It is our view that a data controller within the meaning of the DPA is the person or body with ultimate authority and responsibility for determining the purposes and means of processing the personal data within their control. This is supported by the guidance issued by the Information Commissioner on the definition of data controller which states that where one person may decide the purposes for which personal data are to be processed, but delegates responsibility for the manner in which they are to be processed, it is the person who determines purpose who is the data controller.[1] We therefore concur with the view expressed by the Home Office that in the case of a Government department this would be most unlikely to be individual officials working within the department who have responsibility for a particular database. Such officials, even if having considerable day to day responsibility for the management and operation of a particular database, remain employees who are ultimately subject to decisions by their employer determining at least the purposes for which the personal data are to be processed.

The only exception which we can envisage would arise if there were a situation where a particular individual had been statutorily appointed to process certain personal data, and the personal data was only processed for that purpose. In such a case, s.1(4) would apply so that in respect of that personal data the statutorily appointed person would appear to be the data controller, and subject to the data protection principles and other obligations imposed under the DPA. We are aware that in the past the office of the Information Commissioner has held lengthy discussions over who should be registered as the "data user" under the Data Protection Act 1984 ("the 1984 Act") in such circumstances (for example, in the field of education where statutory provisions imposed separate legal obligations on the local education authority, the governors of a school, and the head teacher).[2] We do not know whether similar situations arise within any Government departments, but if they do this may be an issue which could usefully be discussed further with the Information Commissioner.

---

1 Guidance published on 12 January 2001.

2 "Data Protection Law and Practice" (Jay and Hamilton), p.142.

To date the practice between Government departments as to registration has varied. Some departments have notified the name of their Secretary of State (as the Minister in charge of the department), whereas some other departments have notified the name of the department.[3] There is no legal reason of which we are aware why one or other label is correct or incorrect. To date, the office of the Information Commissioner has accepted both types of notification, and we do not see that there is any need to disturb arrangements which have already been accepted. The terms of the DPA perhaps tend to suggest that the framers of the legislation envisaged that government departments would be notified by name, rather than by reference to their Secretary of State. Thus s.63 of the DPA which provides that the DPA binds the Crown states at 63(2): "for the purposes of this Act each government department shall be treated as a person separate from any other government department". But we do not think it is legally wrong for the name registered to be that of the Secretary of State. If there is a desire to introduce consistency in this practice, we note that an entry in the register generally lasts for 12 months (s.19(5) of the DPA) and therefore renewal could provide a convenient opportunity for amendment.

Personal Data

Pursuant to s.1(1) of the DPA, "data" are defined as information which are processed or recorded in specified ways. "Personal data" are defined as:

> "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, or is likely to come into 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;"

Therefore, in order for something to constitute "personal data" it must consist of identified or identifiable information within the meaning of the DPA[4]. The need for both information and an identifier is confirmed by the reference in s.7(1)(c) to "information constituting any personal data", and by Article 2(a) of and recital 26 to the Directive which refer to "information relating to an identified or

---

3 Both "government department" and "Minister of the Crown" are defined in s.70 of the DPA.

4 The definition of "personal data" in the DPA is broader than that which was contained in the 1984 Act, in particular in that (in line with the requirements of the Directive) identifiable information is now more broadly defined and in that (again in line with the Directive) indications of intention in respect of an individual are expressly included in the definition. The DPA refers to "data which relate to a living individual", whereas the 1984 Act referred to "information which relates to a living individual"; however, given the wide definition of "data" in the DPA, and in particular in the light of the fact that the Directive uses the expression "information relating to" a natural person, this change does not appear to have any material effect.

identifiable natural person" and to "information concerning an identified or identifiable person" respectively.

In the light of these definitions, and taking account of the overall purpose of the DPA and the Directive, we consider that a reference to an individual's name alone is not personal data. It is an identification, but without more is not linked to any information. However, it is likely that an individual's name will usually be contained within a document from which some information about that individual may be inferred; at that point, we consider that there is information which relates to an identified or identifiable living individual. For example, a list of names of persons who travelled on a particular airline flight would enable anyone possessed of that list and the flight time to know that the named individuals were flying at that time.[5] (In our view, the same test applies under s. 7(4) in determining whether the personal data includes "information relating to another individual who can be identified from that information": if the personal data relating to the data subject who makes the request includes a third party's name, but no information relating to that third party, then there would be no basis for the balancing exercise in s. 7(4) to be carried out; however, we would observe that in the vast majority of cases where the data subject's personal data include reference to the name of a third party, there will be some information relating to that other individual, so that the balancing test will fall to be carried out – indeed, we find it very difficult to think of a practical example where the data subject's personal data would include reference to a third party's name, but would not also convey information relating to that third party, within the scope of s. 7(4)).

The definition of "personal data" in both the DPA and the Directive is very wide, but we consider that a court would rule that there are limits to the process of inference which has to be engaged in to answer the question whether personal data are contained in the document which mentions the individual's name or not. The limits would, we think, be spelled out by a court by implication, having regard to the purposes of the Directive, the general EC principle of legal certainty in legislation and the general EC principle that legislation should not have effects disproportionate to its objectives. The regime under the Directive and the DPA would become unduly indeterminate if remote inferences had to be taken into account (a typical clerk, without detailed knowledge of the circumstances in which a document was drawn up, assigned to search through records in order to respond to an access request by a data subject would often simply not be able to tell what inference should or should not be

5 These were the facts of a case heard under the 1984 Act before the Sheriff Court in Aberdeen: see Jay and Hamilton (*ibid.*) at p.30.

drawn from the mere presence of a name in a document); moreover, the more remote the inference, the less likely it is that that document and the information it contains would be used for the taking of decisions likely to affect the interests of the data subject.

The question whether an inference is too remote or not to count as "personal data" is likely to be a matter of impression, and it is difficult to be prescriptive in the abstract about what will or will not fall within the concept of "personal data". By way of example, we consider that the answer to a parliamentary question asked by a named individual probably does not contain information relating to that individual, even though the person would be named in the answer. We think that the inference which can be drawn, namely that the individual asked a question which is now being answered, is just on the wrong side of the divide as to what counts as "personal data". But we are very conscious that there is room for an opposing view, as was forcefully put in conference. This highlights the impressionistic nature of the judgment which has to be made in such cases. The question as to whether an individual's name in a document amounts to personal data because it is linked to information in that document relating to that individual will be a question of fact (and impression) in each case. We regret that it is not possible to lay down any firm rule in this regard (it should be noted that the Information Commissioner has advised that if there are any doubts as to whether data are personal data they should be treated as personal data.[6])

The DTI provided us with further detailed argument regarding the definition of "personal data" in Supplementary Instructions, for which we are grateful. Central to the DTI's argument is an analysis as to whether it is only (a) information collected or obtained about a person which will constitute their personal data, but not (b) information involving executive or administrative decisions regarding a course of action to be taken which includes a reference to that person. We do not consider that a general distinction in these terms is supported by either the DPA or the Directive. Of course, information in category (b) might not, as a matter of construction, contain any datum of information about the individual himself, in which case it would not constitute "personal data"[7]. But in many cases information in category (b) will contain information about the individual himself, in which case that information will constitute "personal data". The definition of that term does not, as a matter of language, support the suggestion that whether information is "personal data" depends

---

6 Published guidance (December 2000) at numbered para. 5.

7 Although it must be remembered that the definition of "personal data" includes "any indication of the intentions of the data controller or any other person in respect of the individual".

upon the purpose for which it is held. Moreover, in many cases, where the administrative decisions in question may impact upon the individual concerned, this seems to us to be a paradigm case where the individual was intended to have rights of access to the data and, if necessary, to have it corrected, so that the administrative decisions affecting him should proceed upon a properly informed basis, and not on the basis of misinformation about him. We also note that a number of the exemptions provided for under the DPA would not be necessary or relevant if the meaning of "personal data" was so narrowly confined as the DTI suggest (see, for example, the exemptions for negotiations and examination scripts in Schedule 7).

We do not consider that draft documents are outwith the definition of "personal data" merely because of their draft status.[8] For so long as such draft documents have not been erased or destroyed, and if the other aspects of the definition of "personal data" are satisfied, those documents will remain "personal data" despite their draft status.

Manual Files

Section 1(1) of the DPA defines "data" to include:

> "information which … (c) is recorded as part of a relevant filing system …"

"Relevant filing system" is then defined as:

> "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, in such a way that specific information relating to a particular individual is readily accessible."

Therefore in order to constitute a relevant filing system, manual files must in particular (a) be structured by reference to individuals or criteria relating to individuals and (b) must be structured in such a way that specific information relating to a particular individual is readily accessible. (These two tests could be satisfied in a number of ways, for example: a set of files may be ordered by specific subjects, such as "disciplinary matters" – which would satisfy test (b) – and be structured with files compiled in alphabetical name order in such a way that the particular file containing that specific information about the particular individual can readily be located by a searcher, which would satisfy test (a); alternatively, one might have a set of files structured in the first place by names of individuals – which would satisfy test (a) - with clearly identifiable sub-

[8] The DPA differs from the 1984 Act in that text processing is no longer exempt.

divisions containing specific information relating to that individual, which would satisfy test (b)).

This statutory formula appears to be in accordance with the definition of "personal data filing system" contained in Article 2(c) of the Directive which refers to a "structured set of personal data which are accessible according to specific criteria".[9] Recital 27 to the Directive also emphasises that it is not intended to cover all manual records and that only files structured according to specific criteria are to be included within the scope of the Directive. The Directive therefore supports a relatively restrictive interpretation of the meaning of "relevant filing system", such that manual records must not only be structured by reference to individuals or criteria relating to them, but must also be structured internally so that specific information relating to a particular individual is readily accessible. This interpretation is in accordance with the Government's intention, which was to focus on highly structured files, and which led to an amendment to change the term "particular information" to "specific information" during the passage of the Bill.[10]

Accordingly, in our view, the question as to whether a particular manual record or file is a relevant filing system will be a question of fact in every case, and files or systems which do not have any clear systematic internal indexing mechanism probably do not fall under the definition. A personnel file with a name on the front, but which is arranged only chronologically will not necessarily constitute a relevant filing system within the meaning of the DPA, since specific information about that individual is then unlikely to be readily accessible. Although in the Information Commissioner's Introduction to the DPA she suggested a cautious approach which assumed that a set or sets of manual information which are referenced to individuals (or criteria relating to individuals), and which information is specific to an individual, would be caught by the DPA if generally accessible on a day to day basis, we do not consider that the definition of relevant filing system in the Act and the relevant provisions in the Directive support such a broad approach.

It might be objected that since one object of the Directive is to provide protection for

---

9 During debates on the Data Protection Bill the Government stated that its purpose in the definition of relevant filing system in clause 1(1) had been "to cover all the manual records that the directive requires Member States to cover, but to go no further than the directive requires": Hansard vol. 315, No. 198, cols 615-616, (HC) (2.7.98).

10 Lord Williams, Hansard Vol. 587, No. 95, col. 467 (HL) (16.3.98). Also see Lord Williams, Hansard (2.2.98), Col. 438: "We do not intend that it should catch files about named individuals where a variety of different kinds of documents is stored by date order. We want to focus on much more highly structured files."

individuals with respect to inaccurate information being recorded which may result in decisions being taken adverse to their interests, a relatively wide concept of "relevant filing system" should be adopted, so as to cover the sort of loosely structured personnel file referred to above. Such an interpretation would also have the effect of avoiding unattractive distinctions being drawn, with respect to individuals' access rights, between loosely structured personnel files and more highly structured personnel files.

This is undoubtedly a difficult point. However, in our opinion, the better view is to confine the concept of "relevant filing system" to highly structured filing systems. It seems to us that the main aim of the Directive is to provide a legal regime controlling automated processing of data (i.e. on computers), but extending that regime to manual filing systems which can be assimilated to automated filing systems – hence the reference in recitals (15) and (27) of the Directive to filing systems structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question.

We consider that it is only highly structured files, not loosely collated files with documents inserted in no particular (or merely chronological) order which were intended to be covered by the Directive, since otherwise the requirement of easy access to particular items of personal data is not satisfied. Such loosely collated files cannot, in our view, be regarded in the same light as automated filing systems. Similarly, we consider that it is legitimate to construe the DPA and the Directive in this way, having regard to the practical reality of data access searches which the draftsmen must have had in contemplation: clerks with no particular background knowledge of a set of files, tasked with searching for personal data to satisfy an access request, would, we think, be expected to be able to identify relevant personal information with a minimum of effort, by reference to clear referencing systems in the filing system in question (ie the statutory test will only be satisfied if the searching clerk can identify with reasonable certainty the file in which the specific data relating to the individual will be located, and not if it would in fact be necessary for the searcher to look through a number of files in order to see whether they did or did not contain specific information about the individual). If the filing system did not include such a referencing system, and a search would require great effort going through a mass of documents in the hope of finding relevant information, we think that the draftsmen did not intend to impose an obligation to carry out such a search, and that it was not intended to treat such a filing system as falling within the DPA or the Directive. (In fact, we are told, the view we have reached is in line with that of the

Commission expressed at the time the Directive was negotiated, although there is no formal record of this, and it is very doubtful that such an expression of view could be prayed in aid as a guide to interpretation of the Directive).

By the test which we consider is applicable, the personnel files held by MAFF, which are specifically referred to in our instructions, constitute a relevant filing system in so far as they contain separate named folders on specific issues (annual reports, leave, disability issues etc.) (since they are in those respects highly structured internally by reference to specific subject matters), but probably do not do so where the papers are merely placed on a file chronologically regardless of subject matter. The Information Commissioner's Introduction to the DPA anticipates that data controllers may find that their manual files consist partly of information which forms part of a "relevant filing system" and partly of information which does not.[11]

We do not consider that a filing system is a "relevant filing system" where, in relation to some but not all items of information about an individual in that system, it may be possible for the individual to point to something likely to be on a file relating to him – eg a request for access to a performance review for a specified year held on a chronological file relating to that individual. In our view, the key point is that the "filing system" or "set of information" in question is not structured "in such a way that specific information relating to a particular individual is readily accessible": this test seems to us to be directed at the general accessibility within the system as a whole of all specific information relating to the individual, and would not be satisfied by the possibility of his identifying, fortuitously (having regard to the circumstances in which the information came into being, but not by reference to the highly structured nature of the filing system itself), the precise location within the files of some item of information.

It seems to us that our view that the appropriate test is one of ready access to the generality of the information in the set is supported by the fact that it is logically necessary for the holder of a filing system to be able to identify whether it is a "relevant filing system" or not in advance of any particular request for information being made.

If files are not named by reference to a particular individual, but nonetheless are structured by reference to criteria relating to individuals and in such a way that specific information relating to that individual is readily accessible, they will fall

[11] p.4, final paragraph.

within the definition of "relevant filing system". Thus we agree with the suggestion of the Cabinet Office that the structuring of the files must in some way make it clear that information on a particular individual is held on those files so that the information can be said to be readily accessible.

For example, if a file were entitled "disciplinary and inefficiency matters", and within that file separate folders were held on particular individuals, we consider that set of information would be a "relevant filing system" within the meaning of the DPA – provided that the reference aids available within the filing system to a person (e.g. a clerk) searching for information about an individual would enable that person readily to know that the file so titled did relate to the individual (eg, if the searcher was looking for this information about Mr Bloggs, the file was ordered alphabetically by name, and it was marked in the index filing system "A to D"; then the searcher would know that he would find that information relating to Mr Bloggs – if there was any - in that file). To put it shortly, manual information will not fall outside the reach of the DPA merely because it is not contained in a file bearing an individual's name, but it must be readily apparent (eg from the filing system's index) that a particular file will be sub-divided so as to contain specific items of information about that individual at a physical point within the file which will be easy to locate (ie without examination of the whole file). In our view, only under these conditions will a person searching for that specific information have ready access to it.

On the other hand, for example, if the reference aids available within the filing system gave no indication that such a generally titled file related to the particular individual in question, then (even though the file might in fact be structured internally in a clear way, once one looked inside it) we consider that the filing system would not afford ready access to information about that individual – because it would be difficult to know in advance of physical examination whether the file did or did not relate to the individual in any way – and would not count as a "relevant filing system".

Finally, we are asked whether it is simply a matter of policy for Departments (either individually or collectively) to determine whether non-computerised personnel files should now be ordered so as to be highly structured, and satisfy the test for a "relevant filing system". In our opinion, neither the Directive nor the DPA contains any obligation on any person (including the Government) holding non-computerised files to carry out any operation to organise those files in any particular way. Therefore, it is our view that whether any such organisation measures should be taken or not is a matter of policy for Departments, and not a matter of legal obligation.

(b) Sections 7 and 8 of the DPA

Redaction

Pursuant to s.7(1)(c)(i) of the DPA an individual is entitled as part of his subject access request to:

> "have communicated to him in an intelligible form … the information constituting any personal data of which that individual is the data subject"

Thus the right of access is to the personal data, not to the document in which the personal data is contained. S.7(1)(c)(i) accurately transposes part of Article 12(a) of the Directive which provides that Member States shall guarantee every data subject the right to obtain from the controller "communication to him in an intelligible form of the data undergoing processing".

Accordingly, on the basis of s.7(1)(c)(i) and the Directive alone, it is clear that a data controller is not obliged to provide a copy of the actual document in which the personal data is contained, but may choose whether to provide either a redacted copy of the actual document showing only the personal data to which the individual is entitled, or an intelligible communication which has been prepared for the purposes of the subject access request and containing the personal data.

Some doubt is cast on this clear position by the terms of the exception contained in s.8(2) of the DPA which provides that:

> "The obligation imposed by section 7(1)(c)(i) must be complied with by supplying the data subject with a copy of the information in permanent form unless –
> (a) the supply of such a copy is not possible or would involve disproportionate effort, or
> (b) the data subject agrees otherwise;
> and where any of the information referred to in section 7(1)(c)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms."

Do these references to an obligation to supply a copy of the information in permanent form, if necessary accompanied by an explanation of the terms of that copy, mean that there is an obligation to supply a copy of the actual document? In our opinion the better view is that there is no such obligation, in particular because this would be contrary to the words of s.7(1)(c)(i) and would go beyond what is required by the Directive. S.8(2) is supplementary to and in part providing an exception from s.7(1)(c)(i), and should therefore be construed in accordance with the natural meaning of that section so as to refer to a copy of the information in permanent form which is not necessarily the actual document.

We also note that s.7(1)(b) requires that the data subject be given *inter alia* a description of the personal data, not the personal data itself or the actual document which contained the personal data. Accordingly, whilst we agree with Eleanor Grey to the extent that a recipient of information which is not given by way of a copy of the actual document might seek to argue that he had not been provided with "a copy of the information in permanent form", we disagree with her view as to the strength of any such argument: we consider that such an argument would be likely to fail.

Section 8(2)(a): disproportionate effort

As set out above, s.8(2)(a) provides for an exemption from the obligation on the data controller to provide a copy of the information in permanent form where the supply of "such a copy" is not possible or would involve disproportionate effort. On balance we agree with the view expressed by the Home Office that this exception, which as an exception must be narrowly construed, provides an exemption from the obligation to supply a copy of the information in permanent form where to do so would involve disproportionate effort, but does not provide an exemption from the obligation to supply the information constituting the personal data on the ground that providing it will involve disproportionate effort. The exception would therefore apply where the information was of such a size or held in such a form that to provide it in permanent hard copy form would involve disproportionate effort. In those circumstances, the data controller would still have to make alternative arrangements so as to communicate the information to the data subject in an intelligible form (for example, provide it in electronic form, or allow some form of viewing or inspection).

This interpretation of the DPA is probably supported by consideration of the Directive, and application of the principle of interpretation in *Litster* (see above). Article 13 provides that Member States may adopt only specified exceptions to restrict the scope of the right of access provided for under Article 12; there is under the terms of the Directive no general right on the part of Member States to adopt an exception where the exercise would involve disproportionate effort. Therefore, a wider interpretation of s. 8(2)(a) than that proposed by the Home Office might well be incompatible with the Directive[12]. We would add that we consider that the reference in the introductory words to Article 12 to the "right to obtain from the controller … without excessive delay or expense … communication to him in an intelligible form

[12] Although we are to be instructed to consider this point further in a separate Advice: an issue arises whether the Directive might permit a general disproportionality defence to be included in domestic legislation, on the basis of Article 13(1)(g).

of the data undergoing processing ..." refers to the right of the data subject to obtain the data without excessive delay or expense, not to any right of the controller not to have to expend excessive time or resources in providing the information.

Our advice also accords with the views expressed by the Information Commissioner to the Department of Social Security, and with the advice previously given to the Home Office by Eleanor Grey. Thus, although we consider that it would be possible to argue for a wider meaning of s.8(2)(a), we are of the view that such arguments would be likely to fail.

We have considered whether there are other provisions in the DPA which could be relied upon so as to avoid Government departments having to make disproportionate effort to comply with subject access requests. We note that in the specific context of subject access to personal data contained in e-mails, the Information Commissioner has issued guidance which states that in practice she might exercise her discretion and not seek to enforce a data subject's rights if she were satisfied that to give access to back-up data or deleted e-mails would involve disproportionate effort on the part of the data controller.[13] Whilst this indication of the possibility of non-enforcement in such circumstances is encouraging, it does not provide a guarantee that a refusal in such circumstances would not be held to be contrary to the DPA (also, this advice has been issued in reference only to the specific areas of back-up data and deleted e-mails).

The only general exception available to data controllers concerning disproportionate effort is an exception from the obligations of the fair processing code where personal data has been obtained from someone other than the data subject (see, in particular, para. 3, Part II of Schedule 1 to the DPA). This exception does not assist in relation to subject access requests.

Our instructions refer in particular to the extensive efforts which some departments have already had to make to provide to data subjects personal data which were in the public domain. In this regard, some assistance may be gained from the exemption provided for information available to the public by or under any enactment and contained in s.34 of the DPA. Some information held by Government departments which is already in the public domain may well have been published or made available for inspection on a statutory basis, and therefore some use may be made of this exemption. However, other information already in the public domain, but which

[13] P.5-6 of Guidance issued on 14 June 2000.

the Government department is not obliged to make available to the public by or under any enactment (such as a record of a television interview), would not come within the s.34 exemption. Given the view expressed above as to the lack of any general exemption on grounds of disproportionate effort, such information would prima facie have to be communicated to the data subject.

Repeated Subject Access Requests

S.8(3) of the DPA provides that:

> "Where a data controller has previously complied with a request made under section 7 by an individual, the data controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request."

Factors to be taken into account in determining what is a "reasonable interval" in any case are laid down in s.8(4).

We are asked to advise whether there is any scope in s.8(2)-(4) or elsewhere in the DPA to exempt a data controller from the obligation to provide permanent copies of personal data where multiple similar and repeated applications are made by different individuals.

We do not consider that s.8(3) can properly be read so as to exempt a data controller from complying with a s.7 request where that individual has made only one such request, albeit the request is one of many such requests made at the same time (perhaps as part of an orchestrated campaign). S.8(3) clearly refers to repeated requests by a single individual, so that the word "individual" cannot in this instance be read so as to refer also to the plural "individuals". Such an interpretation would also be contrary to the wording and intention of Article 12(a) of the Directive, which provides that every data subject shall be guaranteed the right to obtain personal data from the controller "without constraint at reasonable intervals". The emphasis in the Directive is on the data subject being able to exercise subject access rights without constraint, and we consider that an interpretation of s.8(3) so as to permit Government departments to refuse subject access requests due solely to such requests having been made by other data subjects would be contrary to the Directive.

There is greater scope for arguing that s.8(2)(a) may be invoked to exempt a data controller from providing a copy of the information in permanent form where to do so would involve disproportionate effort by reason of the large number of identical or

similar requests received by that data controller at the same time. The DPA does not expressly state that the disproportionate effort has to arise by reason of some special feature of the information to be provided to an individual, and thus it could be argued that disproportionate effort by reason of the multiple number of similar such requests could be relied upon. Thus if such a situation arose, and it would involve a department in disproportionate effort to supply a copy of the information in permanent form to each individual, arrangements could be made for those individuals to obtain or view the information in some other form.

The Information Commissioner has stated that in considering what would amount to disproportionate effort in the context of the fair processing code she will take into account a number of factors including:

> "(i) the cost to the data controller in providing the fair processing information, for example, postage and/or manpower/employee time expended weighed against the benefit to the data controller of processing the data;
> (ii) the length of time it will take the data controller to provide the information, again weighed against the benefit to the data controller;
> (iii) how easy or how difficult it is for the data controller to provide the information, also weighed against the benefit to the data controller;
> These factors will always be balanced against the effect on the data subject, i.e. the extent to which the withholding of the information may be prejudicial to the data subject. In this respect a relevant consideration would be the likelihood that/extent to which the data subject already knows about the processing of their personal data by the data controller."[14]

These factors are not directly relevant to the concept of disproportionate effort in the context of subject access requests. Nonetheless, they do contain some indication of the type of balancing exercise which the Information Commissioner (or, indeed, a court) would be likely to undertake were such an issue to come before her.

Naming of Ministers and Officials

We are asked to advise as to the extent to which it is necessary to name individuals, in particular Ministers and officials, when responding to subject access requests. These names may appear in documents together with opinions or advice which they have given.

Ss.7(4), 7(5), 7(6) and 8(7) of the DPA together establish a regime to cover the circumstances where complying with a subject access request will disclose information "relating to another individual". It is notable that these provisions do not

[14] P.13 of "The Data Protection Act 1998: An Introduction".

refer to a "third party", which is defined in s.70 of the DPA to exclude employees or agents of a data controller, but rather to the wider concept of "another individual".[15] Thus Ministers and officials of a Government department are not third parties of that department, but are other individuals who themselves have certain rights to protect information which relates to them.

S.7 of the DPA provides in relevant part:

> "(4) Where a data controller cannot comply with the request 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 individual.
>
> (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."

In general it is to be noted from these provisions that the emphasis is on compliance with a subject access request so far as possible (and sometimes even without consent of the other person). It is also notable that redaction is expressly envisaged in the second part of s.7(5), but not as a routine exercise or necessarily one which will excuse the data controller from full communication. S.8(7) further defines the circumstances in which another individual would be held to be identifiable from disclosed information. These provisions are justified under Article 13(1)(g) of the Directive, which simply provides that Member States may adopt legislative measures to restrict the scope of the subject access

---

15 Some commentaries on the DPA appear to overlook this distinction, using the term "third party information" in relation to ss.7(4)-(6) and subject access rights. See, for example, Guidance issued by the Information Commissioner and entitled "Subject Access Rights and Third Party Information".

rights when such a restriction constitutes a necessary measure to safeguard the rights and freedoms of others.

In every case where a data subject is entitled to have communicated to him in intelligible form information which constitutes his personal data, but which will also disclose information relating to another individual (be it a Minister, an official, or a Third Party as defined in s.70 of the DPA), the data controller must conduct a balancing exercise in order to decide whether the information relating to the other individual should be disclosed[16]. We do not think that a blanket policy of non-disclosure of the names of Ministers and officials in every case (except where those names have been previously disclosed) would be justified. Equally, in so far as the Information Commissioner's statement that she would expect to see names of officials being routinely disclosed indicates a blanket policy towards disclosure, we do not consider that approach to be the proper one. Rather, in every such case regard must be had in particular to the factors set out in s.7(6), together with any other factors which are relevant to the balancing exercise. The list of factors in s. 7(6) is not exhaustive. We consider, for example, that the factors taken into account could properly include the nature of the reason for the subject access request (e.g. whether the information is wanted as "tittle tattle", or whether the data subject is genuinely concerned that decisions were being taken with regard to him on the basis of possibly inaccurate information), the nature of the information in question (is it information which is likely to be relied upon in the taking of decisions affecting the data subject), expectations as to the level of disclosure public servants ought to be prepared to endure by virtue of their position as such, and considerations as to possible detriment to efficient government in politically sensitive areas.

This last point gives rise to the question, would it be legitimate for a data controller to ask a data subject who requests access to personal data, why they are making that subject access request? In our view, when the subject access request is first made, it would not be appropriate for the data controller to ask such a question as a matter of routine. Prima facie, the right of the data subject to have access to his personal data is not conditional upon his having any particular aim or motive, and we do not think that a practice which might have the effect of deterring individuals from exercising their

[16] For the avoidance of doubt, we would make this point. Where a data subject requests access to personal data about himself which is contained in a document, and that document also contains information relating to another individual, but that information does not form part of the personal data relating to the data subject, the data controller has no obligation to provide that information to the data subject, and may instead simply redact it – it would in those circumstances be unnecessary and inappropriate to engage upon a balancing exercise under s. 7(4).

rights under the DPA should be adopted. However, if it becomes clear after a subject access request is made that a s. 7(4) balancing exercise is called for, and the data controller considers that he would be assisted in carrying out that exercise if he had information available about the data subject's reason for seeking access to that data, we think it would be legitimate for the data controller to ask the question.

It is important to note that the test for disclosure under s. 7(4), where the other individual does not consent (i.e. is it reasonable to disclose the information without the consent of the other individual), is expressed in objective terms. Thus, a court would be entitled to form its own view as to what was reasonable in the circumstances, rather than being confined to a review on *Wednesbury* grounds of the data controller's opinion as to the reasonableness or otherwise of disclosure of the information.

The factors expressly referred to in s.7(6) concern duties of confidentiality and the obtaining of consent. In broad terms, an obligation of confidence arises where the information in question is not known to others and was imparted in circumstances which led to an expectation of confidentiality. Accordingly, in relation to internal memoranda, letters and other documents written by or referring to Government Ministers and other senior officials it may very often be that a duty of confidence will arise (although it might, in any case, be a difficult question whether the duty of confidence which arose was a duty owed to such individual, falling specifically within s. 7(6)(a), or rather a duty of confidence owed e.g. to the department). However, such a duty will not always necessarily exist, and it could be for example that it would not arise in relation to some relatively routine communications. Each subject access request will have to be assessed on its facts in order to determine whether a duty of confidentiality arises in relation to another individual.

The emphasis in s.7(6) on the obtaining of consent, and the reference to any steps taken by the data controller with a view to seeking the consent of the other individual, suggest that consent should generally be sought before disclosure of information is refused. This is particularly the case where the other individual is a Minister or official within the data controller's department, so that it would be very straightforward to make such a request. It may be that in relation to communications which attract a duty of confidence, Ministers and senior officials will very often refuse to give consent to disclosure (and we consider that they would be entitled so to refuse[17]), but the data controller should nonetheless have sought such consent. Accordingly, we do not

[17] Notwithstanding the apparent suggestion to the contrary by the Information Commissioner at

consider that it would be prudent to introduce guidance stating that consent from officials and Ministers need not be actively sought unless there is a particular reason to seek consent.

Where Ministers or officials are mentioned in documents merely as recipients or copy recipients, and that person's name does not otherwise constitute personal data to which the data subject is entitled, s.7(1)(b)(iii) of the DPA provides that the data controller must give a description of:

> "the recipients or classes of recipients to whom [the personal data] are or may be disclosed"

"Recipient" in relation to any personal data is defined in s.70 of the DPA in relevant part as:

> "... any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller ...) to whom they are disclosed in the course of processing the data for the data controller ..."

S.7(1)(b)(iii) of the DPA is taken directly from Article 12(a) of the Directive which refers to the right to obtain information as to "the recipients or categories of recipients to whom the data are disclosed". It is important to note that both in the Directive and in the DPA, the s.7(1)(b)(iii) right to a description of recipients and the s.7(1)(c)(i) right to information which may include information relating to another information are separate rights which impose different obligations on the data controller.

May the reference in s.7(1)(b)(iii) to "recipients or classes of recipients" be read as giving the data controller a choice as to whether to provide individual names (where they have been stated) or only a generic description of the recipients? Or must s.7(1)(b)(iii) be read more narrowly so as to permit reference to classes of recipients only where that is how they were actually described in the information in question? In our view, there are good arguments to support the former approach, so that a data controller retains a discretion as to how he describes mere recipients in this regard.[18] However, so as to comply with s.7(1)(b)(iii) and the Directive as a minimum a description of the classes of recipients must be given (for example, "submission to

---

paragraph 7.6 of her guidance on "Subject Access Rights and Third Party Information". However, it should be noted that there is a provision for an independent review of refusal of consent in s.15(2) – this is in part to take account of the requirement for an independent review laid down in *Gaskin v UK* (1989) 12 EHRR 36.

[18] This is also the view expressed in Jay and Hamilton (*ibid.*), p.167.

Ministers and senior officials of X department(s)"), and it would not be sufficient merely to state the type of document and its date.

Requiring Information from Individuals Making Subject Access Requests

A data controller is not obliged to comply with a subject access request if he has not been supplied with such information as he may reasonably require to satisfy himself as to the identity of the persons making the request and to locate the information sought (s.7(3) DPA). Therefore if a data controller considers that a person making a request has not provided sufficient information to enable location of the information sought, and it is reasonable to require him to provide further information to help locate it, the data controller must inform the person that he requires such further reasonable information in order to trigger the s.7(3) exemption. This is further emphasised in the new s.7(3) which is substituted by paragraph 1 of Schedule 6 to the Freedom of Information Act 2000,[19] and which stresses that the data controller must inform the person making the request of the requirement for further information.

It should be emphasised that s. 7(3) is framed in terms of what may reasonably be required from the data subject. Where the data subject is an outsider so far as the department is concerned, with no knowledge of what its records comprise or of how its records are ordered, it may well not be reasonable to expect the data subject to provide any additional information – at least, if he is simply asking for access to all his personal data (if he is seeking more specific information, it may be reasonable to ask him for, e.g., the approximate date of a particular incident). S. 7(3) does not reflect any specific provision in the Directive, and courts are likely to take a fairly restrictive approach to its application. Where, on the other hand, the request is made by someone with inside knowledge of the department, it might be reasonable to expect them to provide more information about where the information they require is likely to be held.

Against that legislative background, we are asked to advise whether may routinely ask any person making a subject access request to it, why that person believes data relating to him are being processed. We consider that, as a data controller, may only ask for further information in so far as it is reasonably required to locate the information sought. Thus further questions may be asked in so far as reasonably necessary, but should be directed towards and framed so as to refer to how the data controller may more readily locate the information sought. A question as to why a person believes that data relating to him are being processed may

[19] Coming into force on 14 May 2001.

indirectly assist in this regard, but we consider that it would be preferable if requests for further information were framed explicitly in terms of where the person believes the data may be held, in what form, relating to what range of dates and so on. This is in accordance with the guidance issued by the Information Commissioner on subject access and e-mails.[20] However, once again each case must be assessed on its facts, and it would not be in accordance with s.7(3) routinely to make requests for further information even where that information was not reasonably required to locate the information sought. As the Information Commissioner has indicated in her guidance, the reasonableness test would not be satisfied either if the data controller could find the information without the further information or if the data subject could not reasonably be expected to provide the further information.

We agree with the Cabinet Office view that where a data subject refuses to supply further information reasonably required so that the data controller can satisfy himself as to the identity of the person making the request, the data subject may not rely on Article 8 of the ECHR to defeat the s.7(3) exemption. A request for further information as to identity which was reasonably required under s.7(3) would be in accordance with the law (the DPA) and necessary in a democratic society for the protection of the rights and freedoms of others (in particular, the true data subject, should the person requesting access in fact be an imposter). Thus even if such a request for further information prima facie constituted a breach of Article 8(1) as an infringement of private life, we consider that it would be justified by Article 8(2).

E-Mails and Other Computer-Related Matters

Deleted E-Mails (or other electronic documents)

The first question which arises under this heading is whether e-mails which include personal data but which have been deleted on a computer system, continue to be personal data which are "processed" within the meaning of the DPA. In this context, we think that two situations should be distinguished. First, where the deletion of the e-mail consigns it to a storage area within the computer which is in practice used as a repository of information, and it may on occasion be accessed to retrieve information held there. Second, where the deletion of the e-mail consigns it to an area of the computer memory which could (by arcane technical means) be accessed, but in fact is not used for the purpose of accessing the information. We understand that, with modern sophisticated computer systems, the second situation is quite common: in practice, the computer operator does all that they reasonably can to eliminate the

[20] Issued on 14 June 2000.

document from their computer, but with the result that it is not wholly eradicated from the computer memory. The intention of the computer user is then, in effect, defeated by technology.

In the first situation, the storage by the computer user is, in a sense, "active", in that the computer user intends the information to be stored as an archive to which it is possible he may wish to resort in future. We have no doubt that this would constitute "processing" of the information for the purposes of the DPA. But we consider that it is much more doubtful whether the storage in the second situation, which does not have this "active" character, would constitute "processing" of the information.

The definition of "processing" in s.1(1) of the DPA includes "recording or holding the information". The definition is very broad. It echoes the definition of "processing" in Article 2(b) of the Directive, which itself is very wide indeed. In particular, the Directive definition expressly includes the operations of "recording", "storage", and "erasure or destruction", and the list of specified operations is only inclusive rather than comprehensive.

In our opinion, there is a reasonable argument to the effect that both in the DPA and the Directive, the definition of "processing", although broad, does not extend to the deleted e-mails in our second scenario. In s. 1(1) of the DPA, we think that there is a shade of meaning for the words "recording" and "holding" which contemplates some "active", or intentional, element on the part of the data controller or processor. Likewise, the opening words of Article 2(b) of the Directive refer to "any operation or set of operations which is performed upon personal data", which again seems to us arguably to contemplate some "active" element on the part of the data controller or processor.

Although, conversely, it is possible to interpret both definitions as not requiring any such "active" element, and as covering any passive holding or storage of information (intentional or otherwise), we think that there is reasonable scope for arguing that other indicators apart from the shading of the language also suggest that the meaning to which we refer in paragraph 64 above should be preferred. First, we consider that construction of the Directive (and the DPA) against the background of the EC principle of proportionality tends to support our favoured construction: the regime in the DPA and the Directive applies to individuals and private corporations as well as Government departments, and we think that it is well arguable that imposition of highly onerous data subject access obligations in relation to deleted data in our second

scenario, in relation to which there is no practical possibility of the data forming the basis for any decisions affecting the data subject, would be disproportionate, such that the Directive and the DPA should be interpreted in the narrower sense which we prefer. Second, it seems that the type of storage of personal data which is necessary to fall within Article 8 ECHR as an interference with the right to respect for private life is storage with some "active" element as discussed above: we think that the notion of "interference" suggests something more active than the type of storage in our second scenario, and the leading decisions of the ECtHR concerning storage of information as an interference have more the flavour of "active" storage - see *Leander v Sweden* (1987) 9 EHRR 433, para. 48; *Amann v Switzerland* (2000) 30 EHRR 843, paras. 68-69. This point again tends to support the "active" interpretation of "processing" in the Directive, given the objective of the Directive to give effect to rights under Article 8 ECHR.

On any view, the answer to the question posed above is very difficult. The conclusion we have reached as to the ambit of the term "processing" is arrived at very much on balance. Certainly, we think the argument in favour of the "active" meaning is respectable. But there is a serious risk that, notwithstanding our view that it is the better interpretation, a court could come to a different conclusion.

If, contrary to our view above, deleted e–mails in our second scenario are being processed (and, in any event, in relation to e-mails in our first scenario, which clearly are being processed), we consider that transitional relief probably applies. Where processing was already underway immediately before 24 October 1998[21], transitional exemptions apply in respect of *inter alia* back-up data. Paragraph 12 of Schedule 8 to the DPA provides:

> "Eligible automated data which are processed only for the purpose of replacing other data in the event of the latter being lost, destroyed or impaired are exempt from section 7 during the first transitional period."

We are asked to advise whether this transitional exemption also applies in respect of e-mails which have been deleted from the "live" system. In her guidance, the Information Commissioner has indicated that in her view such deleted e-mails are likely to be covered by a transitional exemption, although

---

21 Where e–mails have already been stored by that date, they are clearly eligible data. There is an issue, which we do not expand upon here, whether e-mails deleted after that date, but as part of a practice established before that date, would count as eligible data for the purposes of the exemption.

22 P.4 of the guidance.

she has not specified which one.[22] In our view, e-mails which have been deleted from the "live" system would benefit from the transitional exemption for back-up data, so long as they are only held for the purposes specified in paragraph 12 of Schedule 8 to the DPA, and for no other purposes. The definition of "back-up data" implicit in paragraph 12 is a relatively un-technical one, which concerns the purpose for which the data held, and so long as the deleted e-mails are not held for any other purpose we consider that they fall within the exemption whether or not in technical terms they constitute "back-up data".

After the first transitional period has ended on 23 October 2001, the subject access provisions will in principle apply to "deleted" e-mails which are being "processed" within the meaning of the DPA and the Directive, and which are capable of recovery, however difficult that recovery may be.

In relation to those "deleted" e-mails which are caught by the definition of processing, how should Government departments respond to subject access requests in relation such e-mails which are capable of recovery, albeit in some cases only with very considerable difficulty and expert assistance? The DPA does not contain any guidance on this issue, but as noted above the Information Commissioner has stated that she would expect to exercise her discretion not to seek to enforce a data subject's rights where she is satisfied that to give access to deleted e-mails would involve disproportionate effort on the part of the controller.[23] In the light of this guidance, we suggest that a pragmatic approach for Government departments to adopt pending any further clarification of this issue from the Commissioner or the courts would be as follows:

In circumstances in which such deleted e-mails can be searched for personal data and that information can be retrieved without undue difficulty or disruption to a department's computer system the search should be made. Full use should be made of the right under s.7(3) to ask the data subject for such information as the data controller may reasonably require to assist in narrowing the search (e.g. whether it is believed that e-mails are held in archived or back-up form, the names of the authors and recipients of the messages, the subjects of the e-mails and the dates or range of dates on which the messages were sent[24])

In circumstances in which such deleted e-mails cannot be searched for personal data

---

23 Guidance at p.5-6.

24 P.2 of the Commissioner's guidance on "Subject Access to personal data contained in e-mails".

without exceptional difficulty, for example necessitating the shut-down of a department's computer system, the data subject should be informed that it is possible that personal data are held in the form of deleted e-mails which are no longer available in the data controller's "live" system, that any such personal data are not held for any current processing purpose, that the controller's policy is to retrieve such data only in exceptional circumstances (such as serious criminal allegations), and that it is not possible to search the "non-live" system without expending disproportionate time and resources. The data subject could also be informed that accordingly a copy of any information in permanent form could not be provided without disproportionate effort.

> We recognize that this is a pragmatic solution only, which could in theory still leave a Government department open to a successful enforcement action by a data subject. However, in the early days of the DPA, it is appropriate to take a relatively cautious approach to disclosure in this regard. We suggest that departments may also wish to take advice from information technology specialists as to how e-mails could be permanently deleted and destroyed in such a way that they would no longer fall within the definition of "processing" in the DPA. If this were possible, departments could develop guidelines as to how and when e-mails should be permanently destroyed.[25]

Back-up or Archive Data

The approach set out above in relation to deleted e-mails applies also to back-up or archive data. After the end of the first transitional period, back-up or archive data will prima facie constitute personal data which are being processed and are therefore subject to s.7 of the DPA. We suggest that a similar pragmatic approach to that advocated in relation to deleted e-mails above should be taken in respect of such data. Furthermore, it is relevant to note that since a data subject's right under s.7(1)(c)(i) is to information constituting any personal data, and not to the actual document in which the personal data is contained, to the extent that back-up or archive data repeat information also contained in the current version of a document, a data subject has no right to two, three or four sets of that information. The only right would be to have communicated in an intelligible form (and in a copy in permanent form if that did not require disproportionate effort on the part of the data controller) those aspects of the information which were different from the information contained in the current record.

---

[25] This would also have the advantage of obviating any argument as to whether the fifth data protection principle (personal data shall not be kept for longer than is necessary) had been complied with in this class of case.

We note the discussions which the DSS have had with the Information Commissioner concerning the issue of back-up data. We consider that it would be disproportionate for the DSS to spend more than £20 million and put benefits payments at risk solely in order to cater for searching back-up files for the purposes of subject access requests. Whilst it is unsurprising that the Information Commissioner was unable to give a blanket ruling in this regard, we consider that the DSS could reasonably adopt an approach along the lines of that outlined above.

Searching E-Mails

We are asked to advise whether, for the purposes of locating personal data on computer systems in response to a subject access request, individual employees should search their own e-mails, documents and files, or whether such a search may legitimately be conducted by an employee's manager or by central information technology personnel (on behalf of the data controller) without the employee's consent.

Searching an employee's e-mails would often involve processing personal data of that employee, and may on occasion involve the processing of sensitive personal data (depending on their particular content). We are instructed that in some departments computers display an automatic message to employees when they log on to the network, stating that communications may be monitored and recorded to secure the effective operation of the system and for other lawful purposes. In departments which have such a system, by logging onto the network employees may be taken to have consented *inter alia* to the monitoring of their e-mails for lawful purposes such as compliance with a subject access request under s.7 of the DPA. Departments which do not currently inform their employees that e-mails may be monitored for lawful purposes should introduce some such message or in some other way obtain the consent of their employees to monitoring. Absent such a message, it would be a question of fact in each case whether it was an express or implied term of an individual's employment contract that their e-mails could be monitored for lawful purposes. Since such monitoring would be likely to include, in relation to the employee in question, processing of their personal data, and since e–mails may include sensitive personal data within the meaning of the DPA, departments should obtain explicit consent from their employees before monitoring their e–mails.[26]

[26] To this end, we consider that it would be desirable for any on-screen message to make it clear that by using the network e-mail system, the employee is consenting to the monitoring of his/her e-mails for lawful purposes. Furthermore, we suggest that consideration should be given to making the requirement to give such consent a term and condition of employment, so as to cater

Consent would also (in so far as necessary) make the monitoring lawful for the purposes of the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.[27]

Amendment or Deletion of Data

S.8(6) of the DPA allows routine processing of data to continue irrespective of receipt of a subject access request. Thus although the normal rule is that the information given must be based on the data held at the time the data was received (not, for example, when any further information is obtained or the request is complied with), where the data controller would have made amendments or deletions irrespective of receipt of the request, these can still be made and the information can be given based on the data as they are at the time of satisfying the request.

We are instructed that the DCMS is setting up a document retention schedule against which files will be regularly checked so that irrelevant or unnecessary documents are deleted in order to comply with the third and fifth data protection principles. We consider that such a retention schedule will provide good prima facie evidence of routine processing which would have taken place in any event, so that such checking and deletion could continue after receipt of a subject access request. We further agree with the suggestion in our instructions that files must be checked in a logical order (i.e. according to the retention schedule), and not merely because a request has been received.

Disputes and Legal Professional Privilege

Data Kept in Case of Potential Dispute

We are asked to advise whether Government departments are entitled to maintain records in relation to individuals such as former employees in circumstances in which the departments are concerned that the individuals may bring some proceedings against them in the future. Such data would constitute personal data, which may only be processed if one of the conditions set out in Schedule 2 to the DPA is fulfilled. It is also possible that records such as employment records could constitute sensitive personal data as defined in s.2 of the DPA (for example if they consisted of

---

for situations in which, for example, an e-mail received by a particular employee is monitored/searched before that employee has had an opportunity to log on to the network.

27 Consideration should also be given by departments to amending the standard form e-mail used by their employees, so as to include a reference to the fact that e-mails sent or received by the department may be monitored for lawful business purposes. In this way, recipients of an e-mail would also probably have consented to its possible future monitoring.

information as to the racial or ethnic origin of the data subject or his political opinions). Schedule 3 to the DPA establishes a set of further conditions, one or more of which must be satisfied in order to legitimise the processing of sensitive personal data. Accordingly, it is appropriate to consider whether one or more of the Schedule 3 conditions would also be fulfilled.

We consider that in such circumstances it is very likely that one or more of the Schedule 2 conditions would be held to be fulfilled and that at least one of the Schedule 3 conditions would be held to be fulfilled, so that the records could lawfully be retained for so long as there was a reasonable basis for the view that they might be needed in the future.

The Schedule 2 condition which might perhaps most readily be invoked would be paragraph 6(1) of Schedule 2 concerning the data controller's legitimate interests in the processing of the data. Although this paragraph has not yet been the subject of rulings by the Tribunal or the courts, nonetheless for so long as the retention of the records could not be said to be an unwarranted interference in the rights, freedoms or interests of the data subject, in our view the paragraph would apply. If the data controller has a reasonable concern that the data subject may in the future bring proceedings against the department, then the legitimate interests of the data controller in retaining the information would outweigh any interests of the data subject in having them destroyed.

Alternatively, Government departments may be able to rely upon the seemingly wide terms of paragraph 5(c) of Schedule 2, and argue that the processing is necessary for the exercise of any functions of a Government department. It might be suggested that this paragraph should only apply to functions which are peculiar to the public nature of Government departments, but given the wide terms of the language used (in particular, the reference to <u>any</u> functions), and the separate provision in paragraph 5(d) for other functions of a public nature exercised in the public interest by any person[28], we consider that paragraph 5(c) could properly be invoked in relation to the retention of records such as employment records. Furthermore, this condition is also duplicated in paragraph 7(c) of Schedule 3, and thus processing on these grounds would be legitimate also in relation to sensitive personal data.

The Schedule 3 condition relating to legal proceedings may also be relevant to sensitive personal data which is retained where there is concern about a possible

---

[28] Considered in *R (A) v Chief Constable of C* [2001] 1 WLR 461

future claim. Paragraph 6 of Schedule 3 provides:

> "The processing –
> (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
> (b) is necessary for the purpose of obtaining legal advice, or
> (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights."

It appears to us that this paragraph is drafted in sufficiently wide terms so as to cover the retention of records where there is a reasonable concern about a possible future claim. Indeed, it is notable that the Draft Code of Practice on "The use of personal data in employer/employee relationships" issued by the Information Commissioner gives general guidance as to the retention of records of former employees even absent any prospect of legal proceedings (pages 39-40 of the Draft Code).

Our instructions also suggest that it might be possible to rely upon the implied consent condition in paragraph 1 of Schedule 2 and/or to invoke paragraph 2 of Schedule 2 which concerns processing necessary for the performance of a contract to which the data subject is a party. Whilst we consider that it would be possible to argue for the applicability of these conditions, we consider that such arguments would be weaker than those set out above.

We are asked how long Departments should keep personal data which have been gathered together for purposes of responding to a subject access request, in case of a dispute arising in relation to that request. We find it difficult to give any firm guidance in answer to this. If, in substance, the whole of the personal data has been made available to the data subject, it would seem to be unnecessary for a Department to continue to hold the data for purposes related to the request. If, on the other hand, for example, difficult questions relating to the balancing exercise under s. 7(4) have arisen, and there are reasonable grounds to suppose that litigation about the extent of access given may follow, we think it would be proper and appropriate for the underlying information to be retained for so long as those reasonable grounds subsist.

Where records relating to individuals such as former employees have been retained in anticipation of possible proceedings, those records remain liable to a subject access request under s.7 of the DPA unless the data controller can rely upon one of the miscellaneous exceptions provided for in Schedule 7 to the DPA. The most relevant paragraphs would appear to be paragraph 1 (confidential references given by the data

controller), paragraph 7 (negotiations) and paragraph 10 (legal professional privilege). It is also relevant to note that paragraph 4 provides that the Secretary of State may by order exempt from the subject information provisions personal data processed for the purposes of assessing any person's suitability for Crown employment and Crown or Ministerial appointments. However, the Data Protection (Crown Appointments) Order 2000 (SI 2000 No. 416) only lists a limited number of offices to which appointments are made by Her Majesty.

If the records do not fall within one of the Schedule 7 exemptions, then recourse may be had in appropriate cases to s.7(4)-(6) so as to avoid disclosing information relating to another individual. An opinion expressed about X by Y is a piece of personal data about Y as well as X, so that having conducted the balancing exercise referred to in s.7(6) the balance might, but would not necessarily, come out in favour of Y so as to prevent disclosure. This balancing exercise has been discussed in more detail in relation to the naming of Ministers and officials above. Since s.7(5) of the DPA imposes an obligation on a data controller to communicate so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, we consider it most unlikely that there could be a case in which it was not necessary as a minimum to disclose a general description of the personal data in accordance with s.7(1)(b)(i).

Subject Access Where Legal Proceedings are Current or Imminent between Data Subject and Data Controller

We are asked to advise whether the subject access provisions allow data subjects to obtain information prior to or during legal proceedings against the data controller even where access to such information has been previously denied on an application for disclosure under the CPR. Does the fact of the current or imminent legal proceedings and/or an unsuccessful disclosure application of itself constitute a ground to refuse a subject access request under s.7 of the DPA?

We agree with the view expressed by the Information Commissioner that the DPA establishes a separate set of subject access rights, and that consideration of whether subject access should be provided must be undertaken by reference to the provisions of the DPA alone (together with any legislation relevant to interpretation of the DPA such as the Directive and the ECHR). The DPA in effect establishes a separate regime by which persons may obtain certain information, in the form of a statutory obligation to publish that information to a limited class of persons. Accordingly, the rights which it introduces are additional to and separate from disclosure rights under the CPR.

Other than cases where reliance may be placed on one of the exemptions to s.7 provided for under the DPA (for example, the legal professional privilege exemption), there is no general right to refuse a subject access request on the grounds of current or imminent legal proceedings and/or a failed disclosure application.

Section 29: Assessment or Collection of Tax Exemption

We are asked to advise on the interpretation of s.29 of the DPA, and in particular as to whether the exemption may apply even where an investigation into the tax affairs of a particular individual has concluded and payment been made. S.29(1) provides in relevant part:

> "(1) Personal data processed for any of the following purposes –
> ...
> (c) the assessment or collection of any tax or duty or of any imposition of a similar nature
> are exempt from ... section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection."

S.29(2) provides that where such data have been transferred to someone who processes them for the purpose of discharging statutory functions, those data are also exempt in the hands of the transferee to the same extent as they were in the hands of the original processor. S.29(4) provides a special exemption from the rights of subject access contained in s.7 for personal data which consist of some risk assessment information.

As an exemption, s.29 must be construed narrowly. However, we take the view that the words of s.29(1) are wide enough to cover a situation where disclosure of tax-related personal data to a data subject will not prejudice the assessment or collection of tax owed by that data subject, but would be likely prejudice the assessment or collection in the future of "any tax", whether due from the data subject or other persons. The words "any tax" in s.29(1)(c) are wide, and have not been limited by reference to tax of the data subject who makes the s.7 request. This exemption may only be claimed on a case by case basis, if and to the extent to which the application of s.7 to the data would be likely to prejudice the assessment or collection of tax, duty or similar imposition. Whether there is a likelihood of prejudice in a particular case is a question of fact which should be objectively assessed. In her published "Introduction" to the DPA the Information Commissioner expressed the view that:

> "... for any of these three exemptions to apply, there would have to be a substantial chance rather than a mere risk that in a particular case the purposes would be

noticeably damaged. The data controller needs to make a judgement as to whether or not prejudice is likely in relation to the circumstances of each individual case."[29]

Accordingly, we consider that the line suggested at paragraph 103 of our instructions could be taken in an appropriate case so as to invoke the s.29 exemption, but that consideration must be given on a case by case basis to whether and the extent to which disclosure of the personal data in question would in fact be likely to prejudice the assessment or collection of any tax, duty or other similar imposition.

Scope of the Legal Professional Privilege Exemption

The exemptions contained in Schedule 7 to the DPA (given effect by s.37) include at paragraph 10:

"Personal data are exempt from the subject information provisions if the data consist of information in respect of which a claim to legal professional privilege or, in Scotland, to confidentiality as between client and professional legal adviser, could be maintained in legal proceedings."

By virtue of s.27(2) of the DPA, "subject information provisions" are defined to include s.7 subject access requests.

We are asked to advise whether the Attorney General may rely on the legal professional privilege ("LPP") exemption to refuse to disclose the contents of vexatious litigant submissions to a vexatious litigant who makes a request under s.7 of the DPA[30]. We are also asked to advise more generally whether Government departments may rely on the LPP exemption to refuse to disclose legal advice provided by in-house lawyers when a request is made under s.7 of the DPA.

The Attorney General has power under s.42 of the Supreme Court Act 1981 to apply to the High Court to have a person declared a vexatious litigant. Prior to making such an application, the Attorney General instructs the Treasury Solicitor's Department to gather information about the person's litigation, and on the basis of that information the Treasury Solicitor's Department instruct outside counsel to advise on the merits of the application. This outside legal advice is received by the Treasury Solicitor's Department, forwarded to legally qualified officials in LSLO, and then summarised and submitted, with a recommendation as to whether a s.42 application should be made, to the Attorney General. It is this submission which is referred to in our

29 Chapter 5, para. 2.2.4.

30 The DPA has already been raised in proceedings concerning vexatious litigants and access to bench memoranda: *AG v Covey* and *AG v Matthews* [2001] EWCA CIV 254.

instructions as a "vexatious litigant submission".

English Law

In our view, a claim to LPP could be maintained in legal proceedings in respect of a vexatious litigant submission. LPP has its origins in the concept of confidence. Legal advice privilege[31] concerns the obtaining of legal advice and assistance, and all things which are reasonably necessary in the shape of communication to legal advisers are protected from production or disclosure in order that legal advice may be obtained safely and sufficiently.[32] Thus confidential communications between lawyer and client which come into existence for the purpose of giving or obtaining legal advice are privileged at all times. The privilege covers direct communications and communications through agents, and covers all documents generated for the purpose of obtaining or giving legal advice, including working papers and drafts. The privilege exists whether or not litigation is contemplated or pending.

A vexatious litigant submission as described in our instructions is legal advice so as to fall within the legal advice privilege category of LPP. It is a summary of the legal advice provided by outside counsel, and a submission to the Attorney General with legal advice as to what steps to take in the light of that legal advice. Furthermore, the fact that a vexatious litigant submission is prepared by in-house lawyers (i.e. legally qualified officials in LSLO) does not deprive it of LPP status as a matter of English law. LPP covers all members of the legal profession, including in-house lawyers and legal advisers within Government departments.[33]

We do not consider that arguments based upon the decision of Moore-Bick J in *Goodridge v Chief Constable of Hampshire Constabulary* [1999] 1 All ER 896 would succeed in persuading a court that LPP did not attach to a vexatious litigant submission. The case illustrates the importance of considering the capacity in which the documents were created, and in particular whether a relationship tantamount to that between client and legal adviser existed between the parties. Moore-Bick J held that although LPP could come into existence between the police and the DPP where the relationship was tantamount to that of a client and legal adviser, where the police

---

31 One category of LPP. The other category – litigation privilege – is potentially wider than legal advice privilege (extending to communications with third parties), but arises only when litigation is in prospect or pending.

32 *Wheeler v Le Marchant* (1881) 17 Ch. 675, 681. See also *R v Derby Magistrates Court, ex p. B* [1996] 1 AC 487 and *Anderson v Bank of British Columbia* (1876) 2 Ch. D. 644, 649.

33 *Alfred Crompton Amusement Machines Ltd v Commissioners of Customs & Excise (No. 2)* [1972] 2 Q.B. 102, 129. This case concerned salaried legal advisers to the Commissioners of Customs & Excise.

were merely reporting to the DPP pursuant to their statutory duties no such relationship arose and thus the claim for privilege failed in that case. However, in the case of a vexatious litigant submission there is a relationship tantamount to that of a client and legal adviser between the Attorney General, his chain of Government legal advisers, and external counsel. The fact that the vexatious litigant submission in part contains advice as to whether to institute proceedings which have a statutory basis in s.42 of the Supreme Court Act 1981 does not detract from this analysis.

We also agree with the view expressed in our instructions that any argument that LPP should not attach to a vexatious litigant submission due to the underlying policy justifications for the privilege would be very likely to fail. Although the Attorney General may have a less obvious personal interest in the legal advice which he receives than an individual acting in a merely private capacity, and could therefore be said to be less likely "to hold back half the truth",[34] he has just as much interest as any other potential litigant (be it individual, company or public authority) in being able to consider fully with legal advisers both the strengths and weaknesses of a potential application in the knowledge that discussion of any weaknesses will remain confidential. Existing cases in which LPP has been held to be capable of existing between government legal advisers and their clients also support this view.[35]

European Law

The DPA implements the Directive into UK law. In particular, s.7 of the DPA implements the right of access provided for in Article 12(a) of the Directive into UK law. Member States are only entitled to restrict the scope of the rights provided for under *inter alia* Article 12(a) when such a restriction constitutes a necessary measure to safeguard certain interests named in Article 13(1) of the Directive. Article 13(1)(g) specifies the interest which forms the basis for the LPP exemption contained in paragraph 10 of Schedule 7 to the DPA. Article 13(1)(g) of the Directive refers to:

> "**the protection** of the data subject or **of the rights and freedoms of others**." (emphasis added)
>
> Thus the LPP exemption is only in accordance with European law to the extent that it protects "the rights and freedoms of others" as recognised under European law.

Our instructions contain a careful analysis of the approach in European Community

---

34 *R v Derby Magistrates Court ex parte B* [1996] 1 AC 487, 507 D.

35 For example, the *Alfred Crompton* case referred to above.

law to the scope of legal privilege, and the fact that as a general principle of Community law it is only relations between a client and an independent lawyer which attract privilege against disclosure.[36] However, it is relevant to note that the Court of First Instance has held that legal professional privilege extends to internal documents which pass on legal advice received from independent lawyers.[37] This would appear to cover vexatious litigant submissions at least to the extent that they summarise and report to the Attorney General the legal advice received from outside counsel.

Further and in any event, given the wide and general nature of the exception permitted under Article 13(1)(g) of the Directive, and in particular the fact that it does not refer to legal professional privilege but to "the rights and freedoms of others", we do not consider that the LPP exemption under the DPA need be co-extensive with the concept of legal professional privilege as a matter of European law. The relevant question is instead whether the LPP exemption is necessary to safeguard "the protection of ... the rights and freedoms of others". We consider that the United Kingdom was properly able to implement this aspect of the Directive *inter alia* by the introduction of the LPP exemption, which is manifestly concerned to protect the rights and freedoms of others (i.e. the right of legal advisers and their clients to confidentiality of communications), and which is a proportionate means of achieving this aim. We are reinforced in this view by the recognition afforded by the European Court and the legislature to the importance of the confidentiality of in-house legal advice received by the institutions in the context of public access to EU documents.[38]

In the light of this advice, it is not essential to consider further other arguments which might be available to Government departments if it were necessary to argue that legal advice privilege between Government legal advisers and their clients was within the general principle in European law of legal professional privilege. The Directive has chosen to leave to Member States a wide discretion as to exemptions which they may introduce for the protection of the rights and freedoms of others, and LPP as understood as a matter of English law is in our view properly within that discretion. To put it more shortly, Article 13 of the Directive does not introduce harmonised derogations (which must have the same scope in all Member States), but allows for

---

36 The leading case is Case 155/79 *AM&S v Commission* [1982] ECR I 575. The question of privilege arose in the context of a Commission administrative investigation under the competition rules of the Treaty, but the decision was based on general principles of law which also apply to proceedings before the European Court.

37 Case T-30/89 *Hilti AG v Commission* [1990] ECR II 163.

38 See, for example, Case T-610/97R *Carlsen* and Article 4(2) of the Draft Regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents.

derogations from harmonisation (such derogations permissibly having a different scope in different Member States).

The ECHR

Consideration of rights under the ECHR does not affect our conclusion that a claim to LPP could be maintained in legal proceedings in respect of a vexatious litigant submission. We agree with the view expressed in our instructions that there is only a very limited right of access to information under Article 8 of the ECHR,[39] and no such right has been developed under Article 10.[40] In condemning a search of a lawyer's offices as contrary to Article 8 ECHR, the ECtHR recognised the particular importance of professional secrecy in the legal context.[41] Accordingly, we do not consider that there is any real risk that the LPP exemption provided for in paragraph 10 of Schedule 7 to the DPA would be held to be in violation of the ECHR.

Other Internal Government Legal Advice

Our conclusion in relation to vexatious litigant submissions also applies more generally to other internal legal advice generated within Government departments. Much of the reasoning set out above in relation to vexatious litigant submissions applies with equal force to other advice provided by departmental lawyers, save for the observations which relate specifically to the fact that the legal advice was obtained from external and independent counsel and summarised for transmission to the Attorney General. Thus we consider it strongly arguable that legal advice provided by departmental lawyers to their clients is information in respect of which a claim to LPP could be maintained in legal proceedings, and we do not consider that there is any significant risk that the LPP exemption would be held to be contrary to European law or to violate the ECHR.

---

39 *Gaskin v UK* (1990) 12 EHRR 36: Article 8 imposes a positive obligation upon the State to ensure that the interests of an individual seeking access to confidential records relating to his private and family life (childhood years spent in care) is secured when a contributor to the records either is not available or improperly refuses consent to access to those records.

40 *Leander v Sweden* (1987) 9 EHRR 433, para. 74. In *Z v Austria* (1988) 56 DR 13, the Commission stated that the freedom to receive information which is protected by Article 10 is "primarily a freedom of access to general sources of information which may not be restricted by positive action of the authorities.".

41 *Niemietz v Germany* (1993) 16 EHRR 97, para. 37.

PHILIP SALES

11 King's Bench Walk
Temple
London EC4Y 7EQ

JEMIMA STRATFORD

Brick Court Chambers
7-8 Essex Street
London WC2R 3LD

19 June 2001

in the matter of subject access requests under s.7 of the data protection act 1998

---

joint advice

Legal Adviser's Branch
Home Office
50 Queen Anne's Gate
London SW1H 9AT

Attention: Victoria Bather

F

From: Clare Sumner
Date: 13 July 2001

PRIME MINISTER

cc: Jonathan Powell
Jeremy Heywood
Andrew Adonis

DATA PROTECTION : ADVICE FROM THE LORD CHANCELLOR AND HANDLING

Advice from the Lord Chancellor

Derry has provided advice on how we should proceed on data protection. It contains no real new elements. In his view we should:

- Apply the act sensibly using exemptions where we can – central guidance will be provided to assist departments.
- Consider further whether we should amend the act to exempt policy formulation but only if our experience of case handling provides evidence that we have insufficient protection from the current exemptions.

In my view this approach is broadly right. Our current experience of case handling has shown that it is possible to apply exemptions intelligently and prevent embarrassing material from being released. The cases we have had so far have been from individuals pushing at the limits of the spirit of data protection to try and get as much material as possible from the government.

To date what we have sent out, although large in volume has not been damaging.

Derry also thinks we should wait and see what the Information Commissioner rules if our approach is challenged.

Changing the law is fraught with difficulty, not least because it would draw public attention to the problem that if you apply to the Government using the DPA you are likely to get access to more material than under FOI. This in my view will encourage more people to submit requests as the legislation goes through.

I also think it would be extremely difficult to get any such bill through as these issues have a devoted following who would not want to concede this principle.

During the passage of FOI Jack was forced to amend the act in favour of more openness, not less.

It is worth officials doing more work on this but I also think we need to get more definiitve legal advice on the application of the exemptions and that this should form part of the central guidance package. Our problem to date has been that we have had to persuade lawyers that the exemptions are valid which is the wrong starting point.

?Content for Derry to work on improved central guidance which focuses on the application of exemptions, and for further consideration to be given to potential amendment to the DPA

Yes but quickly

CLARE SUMNER

FROM THE RIGHT HONOURABLE THE LORD IRVINE OF LAIRG

HOUSE OF LORDS,
LONDON SW1A 0PW

On Mb.

12 July 2001

PRIME MINISTER

DATA PROTECTION ACT 1998

In sharp contrast to the highly effective cross Whitehall preparation for implementation of the Human Rights Act, we have not prepared well within government for the responsibilities imposed by the Data Protection Act, and in particular for the right of access to personal information held by Departments about an individual in the context of policy development. Unlike the Freedom of Information Act, the Data Protection Act does not contain an exemption for the formulation of policy. As a result there has been some confusion about how to deal with such requests and understandable concern about the practical consequences of this right, in particular in relation to the disclosure of sensitive personal material. I propose that:

- **we produce robust guidance on handling subject access requests as quickly as we can; and**

- **we look further at the extent to which we could legislate for further exemptions under the Act;**

- **but only do so if experience after robust guidance and robust interpretation of the exemptions proves these to be insufficient in practice in any case.**

We must recognise that there will be difficult cases as people test out the scope and implications of the Data Protection Act. As I said during the run up to implementation of the Human Rights Act, we must promote a culture of respect for the rights and responsibilities set out in the Act, but in a sensible way. We need to proceed in a way which is sufficient to meet the Directive, which underpins the Act, but we should not seek excessive or over enthusiastic compliance. We should not be excessively risk averse, as this will lead to unnecessary disclosures. We must be especially wary of Departments believing, on the advice of Counsel or otherwise, that they must meticulously search for references to individuals across a range of databases, or apply exemptions from disclosure cautiously to be certain of avoiding challenges. In many cases it will be more sensible to wait until challenges are brought before the Information Commissioner (who has statutory enforcement duties under the Act) or the courts. Where we have a sustainable, arguable case for invoking an exemption, or treating information as not falling within the scope of the Act, which has

a reasonable chance of success, my advice is that we should not be rushing to anticipate the judgement of the Commissioner or the courts, but should follow a policy of "wait and see". It is Ministers, not lawyers, who must decide whether it is worth running the risk of litigation when practice or procedure is under challenge. We should be ready to defend ourselves before the Information Commissioner, or, if necessary, in court, where we have sound reasons for seeking to uphold our interpretation of the Act.

You will recall that Government, as a whole, made good use of the two-year delay in implementing the Human Rights Act. There were zealots who pressed us to get on with it and Jonahs who opined that, whenever we implemented, there would absurd decisions and disaster in the courts. In practice, the story is good and the period of preparation has served us well. For example, a potential upset was avoided in the Alconbury case in which the House of Lords held that, notwithstanding the Secretary of State's involvement in the formulation of planning policy, his powers to determine planning applications are not incompatible with Article 6 of the ECHR, given the ability of the courts to judicially review planning decisions.

Unfortunately there was no cross Whitehall preparation for the implementation of the Data Protection Act 1998. The probable reason was that the 1998 Act was seen as simply an updating of the Data Protection Act 1984. The 1984 Act implemented the provisions of the 1981 Council of Europe Convention on Data Protection. The 1998 Act was needed to implement the EC Data Protection Directive of 1995. The main difference between the two Acts was that the 1998 Act extended the data protection regime to structured manual files. The 1984 Act applied only to computerised files. However, what has happened, since the 1984 Act was brought into force, is a vast extension of the amount of information held electronically and so coming into the scope of the data protection regime. Those parts of Government which have held personal data on computer for many years appear to be coping with subject access requests under the Act fairly well. For example, the Benefits Agency received, 2,300 requests, and the Child Support Agency, 1,500 (both figures for financial year 2000/01). These requests were handled alongside day to day business.

By contrast, your office has greatly extended the range of its information held in computerised files (and therefore subject to the Act's provisions) comparatively recently - the Matrix system was introduced only last year. I understand that your office had not received a subject access request until late last year. It seems likely that the publicity surrounding the implementation of the Data Protection Act, and the consequential higher media profile of the Data Protection (now Information) Commissioner, has led to the current surge of applications for subject access under the Act. It was unfortunate that there was no preparation or guidance available to your office from within Government; even more so as, by and large, the information held in central policy areas is more sensitive and difficult to deal with than that held elsewhere.

That said, I understand that, so far, subject access requests have been handled without the disclosure of sensitive material, although at the cost of significant disruption to the business of your office. We have a report from Cabinet Office on the subject access request from which states that information disclosed included relevant extracts of official correspondence between Ministers and officials, and information from media monitoring, which was essentially a summary of information already in the public domain, rather than new information created in Government. The report further explains that reliance was placed on exemptions for legal professional privilege, the granting of honours and to prevent the disclosure of the names of third parties. There was difficulty in determining which information fell within the scope of the exemptions and legal advice had to be sought.

The request, currently under consideration, raised similar issues as well as additional difficulties in securing consistency of approach between Departments. I gather that you expect requests from Northern Ireland which may place a further strain on the ability of your office to cope with the administrative burden and stretch the boundaries of the exemptions under the Act. As a first step what we would have to do is prepare practical guidance on the operation of the Act, which will set out a consistent approach across Government and reduce the administrative burden on Departments. The guidance, in my view, must follow a route of minimal, defensible, compliance and avoid an over enthusiastic maximalist stance. I have instructed officials to give priority to working on this guidance and a first draft should be available at the end of this month.

We have sought the opinion of First Treasury Counsel, Philip Sales, on a number of points relating to the operation of the Act. His opinion is helpful. For example, he advises that a structured manual file (to which the 1998 Act will apply) is one which has a clear, systematic, internal referencing system. This is a much narrower definition than that proposed by the Information Commissioner.

He has also, importantly, advised that we are not obliged to provide a copy of the actual document in which the personal information is contained, but may choose to provide a separate note containing the information. This avoids the problem of supplying copies of documents with large areas blanked out, which in practice incites an applicant to challenge the response.

Further advice is that we would have a respectable argument for treating e-mails and other information which has been deleted from a live system as not being "processed" within the meaning of the Act.

Philip Sales is also helpful about the interpretation of some of the exemptions under the Act. We can avoid disclosing information where to do so would identify a third party who has not consented to disclosure and where, on balance, it would be unreasonable to identify that person without that party's consent. Such protection would, in principle, be available to Ministers and officials, as well as other individuals.

Overall, therefore, Philip Sales' advice encourages me to believe that a sensible and balanced approach to guidance with due regard to the needs of government in its policy making area, as well as to the legitimate rights of individuals, is sustainable.

Robust guidance of the kind proposed will reduce the administrative burden of dealing with subject access requests and minimise the risk of sensitive material being disclosed. But we need also to consider whether further legislation is needed to safeguard the Government's position and what is feasible given our international legal obligations, though I do not recommend that at this stage.

It is important to recognise that, unlike the Freedom of Information Act, where we had a free hand to provide whatever exemptions we could justify, our room for manoeuvre with data protection legislation was constrained by the provisions of the EC Data Protection Directive and the Council of Europe Convention on Data Protection.

For example, it has been proposed that we could exempt foreign affairs information altogether from the data protection regime because an EC Directive can only have effect in areas where the EC has competence, which does not include foreign affairs. But the Council of Europe Convention does apply across the full range of Government activities. If we went down this route, we would need to make a declaration that we would not apply the Convention to this information. This action is permissible under the terms of the Convention, but could be difficult politically. There are

additional risks to this approach, not least in defining whether any particular information fell within, or without, the scope of EC competence.

A more fruitful area would be consider whether we could create further exemptions in the legislation which would be consistent with our international legal obligations. Article 13(1) (g) of the Directive permits us to enact an exemption to protect "the rights and freedoms of others". We believe it reasonable to interpret "others" as including the Government. During negotiations on the Directive, the European Commission said that they took the view that "others" included organisations holding personal data. In a democratic society we ought to be able to argue that, for example, it is necessary to have an exemption relating to the policy formulation process in order to protect the right and freedom of the Government to develop public policy. We need to consider how wide such an exemption could go to meet the test of "necessity" but some movement should be possible.

We could also explore whether more could be made of the permitted exemptions in the Directive under Article 13 (1)(a), national security and 13(1) (c), public security.

Before we go down such a route, however, we need to consider our options very carefully. To date the exemptions under the Act have been sufficient to prevent the disclosure of sensitive information. If we were to amend the legislation, we would be unable to cite any examples of why legislation was necessary which would take away rights which have existed since the 1984 Act was brought into force and which were reaffirmed under this Government in 1998. We would have serious difficulty in getting such legislation through Parliament, and we would face some press hostility.

We would be on far stronger ground if we could point to instances where disclosures put the Government at risk of serious damage. And, given that the Data Protection Act applies to the private sector as well as to public authorities, we might be on even stronger ground if we could demonstrate that the regime placed an unacceptable burden on business.

In the longer term we could see whether there is any scope for amendment of the Directive, but this is unlikely to bear fruit in the foreseeable future.

I propose, therefore, that we get on with the guidance as quickly as we can and that officials look further at the extent to which we could legislate for further exemptions under the Act. This would put us in a position where we could move quickly to legislation if the need arose and we felt that such action was justified in the light of the threat to Government, perhaps if difficulties arose, for example, in the handling of requests for disclosure from Northern Ireland.

I am copying this minute to Sir Richard Wilson.

Irof h

LORD CHANCELLOR
10 July 2001

RESTRICTED - POLICY

(1)

cc JSh Sawers
JJH
DN
LL

Jonathan Sharrock
European Secretariat

09 July 2001

Stephen Wall

Cc **Martin Donnelly**
Rachel Green
Michael Roberts
Paul Heardman
Richard Crabtree

Climate Change: preparations for COP6bis

Attachments

There are three key documents setting the context for the meeting:

A. Correspondence between John Ashton, Nicola Brewer (FCO) and Pete Betts (DEFRA) on handling options for climate change negotiations.

B. Letter from BE Washington (3 July) on latest US thinking.

C. Draft letter for Mrs Beckett to send to EP and ENV committees seeking agreement to UK line at Bonn.

Other papers give a wider background to discussions:

D. Washington Post article by Ballentine on options

E. DEFRA paper on general questions to be addressed before COP6bis. This is being discussed at a pre-meeting on Tuesday.

F. Telegrams from Washington, Moscow, Berlin, Brasilia and New Delhi, and reporting telegram from Hague informal, on a videoconference with the Japanese and on the views of the G77.

Objectives of the meeting

2. Pete Betts chaired yesterday a meeting on the detail of preparations for Bonn. This meeting will complement that, and focus on the strategic issues running on to Marrakesh and into 2002.

3. You should therefore:

- Clarify the basic approach to COP6 negotiations; and the key messages for Genoa and the PM's bilateral with Bush. **More work may be needed on a couple of detailed points** within this e.g. on money available for the developing country funding package.

- Broaden the scope of discussions to address the longer-term strategic issues. The key point will be how to play in the USA, and to build bridges with them. **The Ashton-Betts correspondence sets out the handling options and is a good place to start.** It can be supplemented by feedback from the DPM's people and reports from his recent visits to the Far East.

- Commission **Ministerial correspondence** to finalise this position, and to clarify the basic approach to G8. Margaret Beckett needs to write to EP and ENV as a starting point.

Process

- COP6bis convenes on Monday 16 July, and will finish at the end of the following week. Ministers will attend from Thursday 19 July to Sunday 22.

- The Genoa G8 summit will run from Friday 20 July through to Sunday 22. President Bush is calling in London on 18 July, en route to Italy.

- COP7 will be in Marrakesh from 29 October to 9 November. No formal timetable has been set for a further round. But the Johannesburg summit in September 2002 and further G8 meetings are relevant to ongoing work.

Background

4. Gothenburg did not kill Kyoto. But it did deal it some heavy blows. And the stalemate with the USA has drained much of the creative thinking and most of the impetus away from negotiations.

5. The US were pleased with the result they got in Gothenburg. But they have now taken their foot off the gas in developing further their climate policy. The have promised to participate fully at Bonn, and not to stand in the way of others reaching agreement on specific point. Whether they will stick by this remains to be seen. A bigger risk comes from their growing confidence that Kyoto will

sink under its own inertia, and that climate change is slipping down the international agenda. They are likely to be encouraging others (e.g. Japan, Australia, Canada and Latin American countries) to play the longer game and not seek a deal at Bonn.

Bonn

6. DEFRA have chaired a pre-meeting today, looking at some of the details in the package on the table (the so-called Pronk package). The conclusion was that the best outcome would be to take forward the agreement at Gothenburg – i.e. for USA to agree not to participate, and for all other signatories to develop details of specific issues within the package.

7. Ideally, this would be done by agreeing some of the formal text that the Dutch Presidency have prepared. A more achievable fallback could be a more concise set of Council-style conclusions, taking forward some of the key issues at stake. A bottom line could be to achieve something concrete on one or more of the specific issues at stake.

8. The issues at stake here relate to the operation, functioning and financing of the detailed mechanisms within Kyoto i.e. emissions trading, clean development mechanisms, joint implementation (i.e. developed countries fund in 3rd World). There will also be policy decisions on points such as supplementarity (principle that domestic action is more important than international bargaining), the role of carbon sinks (i.e. using forests to soak up carbon), the compliance regime (i.e. penalties for not meeting targets) and a funding package for developing countries.

9. The UK position on most of these is pretty clear, and agreed at official level. But there has been no Ministerial correspondence, and a couple of issues remain to be decided between Departments. The most important is the availability of UK funds for a 3rd world package. We need to find £58million. Clare Short has said today that this needs to be new money – HMT are likely to resist. The DPM may wish to get involved. This needs to be clarified and agreed before next week.

After Bonn – do we develop 'Kyoto plus'?

10. COP is likely to get bogged down in detail on this sort of point. The purpose of our meeting will be to consider our tactical approach to international consideration of climate change in the

margins of the COP, at the G8 – and towards Marrakesh and beyond.

11. The question is how we should seek to evolve international work on climate change towards a position that the US and other Umbrella Nations will find more acceptable.

12. In considering this issue, there will be five major themes for the meeting to consider:

i. Views on tactics

13. The most important point is whether the UK should take a lead in evolving Kyoto to get full international buy-in. FCO and DEFRA correspondence postulates two basic approaches: a 'Kyoto plus' tactic, where we invest substantially in evolving Kyoto to make it palatable to the US and umbrella group. Or a 'Kyoto minus' which seeks just to get the most we can out of the package on the table at the moment.

14. The US are not really open to any specific developments of this kind at the moment. But work with others in the umbrella group – who may be wavering but not quite so far – may have more effect. We need to think about putting work in hand that will bear fruit in the longer run, and that may require the PM to expend political capital in taking the lead.

ii. Latest intelligence

15. In deciding whether or not we push for a 'Kyoto plus' solution, and how we do it we need to consider the likely reaction of key players. These are:

- **the USA.** We expect them to play a slow hand at Bonn to obfuscate Kyoto without actively sinking it. But what should our message be in Genoa and bilateral work with Bush? How should we seek to engage them up to and after Marrakesh? How should we build a dialogue with them? Should we do this as EU/ US work, or within a group of industrialised nations? Would the PM, DPM or officials lead?

- **Japan, Russia, Australia, Canada**. Are all likely to seek shelter from the US stance, even if they protest their commitment to Kyoto. How do we keep them onside? What can we do to

encourage them? What are messages for Putin and Koizumi at Genoa? What has the DPM learned from his trip to Tokyo?

- **EU**. Our commitment to Kyoto has gone down well. How should we focus our work now? Would we have a lot of persuading to do in favour of a 'Kyoto plus' option? What do we need to know about Italy, France, and Germany? Can we do more to lobby them?

- **G77 and China**. They are likely to be most resistant to any changes to the Kyoto acquis. What did the DPM learn in India and China? What bilateral work can we do to boost our hand – i.e. facilitating a good Third World Chair for Marrakesh, and getting funding to pay for the package on the table in Bonn.

iii. Handling of G8 and US meetings

16. Meetings and bilaterals in Genoa need to be properly prepared and briefed for. We also need to ensure that there is good communication between Bonn and Genoa so that issues arising in COP can be got across if necessary.

17. The briefing needs to cover: at the meeting, a robust UK line in favour of Kyoto, a good result at Bonn and the long-term success of global action. More importantly, briefs for bilaterals with Japan, Russia, Canada and the USA should give tailored messages on the detail of negotiations and on the veracity of a 'Kyoto plus' mechanism.

iv. Need for inter- ministerial agreement and a written record

18. Margaret Beckett needs to write to clarify the UK position going into Bonn. Important to clarify with HMT, DFID and the DPM the position on funding for developing countries' package.

19. In the longer term, we will need to draw up a strategy for developing and promoting any 'Kyoto plus' deal – with a role for relevant Ministers and a way of assessing its success.

v. Presentation of atmospherics, handling expectations

20. There will surely be great interest in Kyoto from the press, and from stakeholders such as NGOs, and business – particularly those affected by the climate change levy.

21. Our aim must be to minimise expectations of Bonn, to make clear that Marrakesh will be going ahead whatever the outcome of COP6bis and to make the most of its achievements.

Handling

22. Everybody at the meeting has an interest in a successful long-term policy on climate change. But not everybody is up to speed on the detail of COP6bis and preparations for it. Key people will be **Dinah Nichols, Henry Derwent and Pete Betts** from DEFRA, **John Ashton** from FCO and **Peter Unwin** from the DPM's office. No10 will be represented by **Liz Lloyd**, who has taken over responsibility for climate change since the election.

23. You could begin by **stressing that this meeting will complement, not to duplicate, the one that DEFRA chaired yesterday**. Aim today to focus on the handling and footprint of COP6bis, rather than the detailed issues for discussion.

24. But given that the cast lists at the meetings are slightly different, you could begin by asking **Pete Betts** to summarise the conclusions and the outputs of the meeting that he chaired. What issues are outstanding on the UK line for Bonn? What about question of UK funding for the package for Developing Countries?

25. Turning to the **likely outputs from Bonn**, you could ask DEFRA to give a sense of what we can expect from the conclusion of COP6bis. What can we realistically expect to be agreed? Is there any scope for presenting it as a success? Is there a risk of a spectacular failure, or will the process just run into the sand?

26. Moving onto the more **strategic issues**, it is clear that Bonn will not be the end of the Kyoto process. COP7 at Marrakesh will happen regardless of conclusions. And climate change is sure to be a theme up to and at the Johannesburg Summit in September 2002. We need to identify a wider strategy for a successful outcome, and decide how we try and involve the US in it. You could ask **John Ashton** to outline the thinking in his paper on options for Kyoto Plus or Kyoto Minus.

27. What do others think of this? Key views will be from **No10, Peter Unwin,** and **DEFRA**. Any initiative will require political capital, and concrete ideas to make it work. What will be the PM's and

DPM's views on this? Is it not better just to stick with Kyoto without the Americans?

28. Is there a risk of other Umbrella Group countries breaking ranks on Kyoto as time goes by? You could ask **John Ashton** and **Peter Unwin** to update us on latest intelligence from them.

29. **What might a Kyoto plus initiative look like?** How would we broker it with EU partners? Should we focus just on the USA, or on other important links e.g. Russia and Japan? Could we do it through existing structures, or bilaterally. Or would a new initiative – e.g. a forum of industrialised countries – be more appropriate?

Conclusions

30. You should be able to conclude that:

- **On detailed preparations for Bonn**, DEFRA Ministers should write round seeking agreement to their line. Important for DFID, HMT and the DPM's team to clarify the specific question of funding for developing countries before negotiations. Press work will be particularly important. DEFRA should keep No10 and Cabinet Office squarely in the loop.

- **On preparations for Genoa**, FCO and DEFRA need to make sure that briefing is suitable for use in meetings and in bilaterals with Putin, Koizumi, Chretien and Bush. This must be cleared with DPMs people and the Secretariat.

- On **developing a 'Kyoto plus' model**, DEFRA and the FCO should quickly prepare a paper after Bonn setting out what this might mean in terms of policy and specifics. It will need to quantify what we are seeking to get from the USA and others, and how we could achieve this. It would need to cover lobbying, initiatives and other work with EU partners and other countries. DPM's people will need to contribute to this. It will need to be put to No10.

- When this is produced, we will need to consider an action plan for taking this forward. All Ministers with an interest will need to play their part in delivering something.

Jonathan Sharrock

From: Jeremy Heywood
Date: 9 July 2001

SIR RICHARD WILSON

cc: Gus MacDonald
Michael Barber
Wendy Thomson

MANAGEMENT OF PROJECTS

The Prime Minister has seen Andrew Smith's minute of 29 June summarising evidence from the OGC's Gateway scrutiny of major projects.

The Prime Minister is very concerned about this damning report. He believes that by Christmas we need a radical and comprehensive action plan for addressing the critical weaknesses identified in Peter Gershon's report. He wonders whether this would not be a good early project for Wendy to handle, drawing on Peter Gershon's expertise. He has also asked whether we should be making personnel changes now.

JEREMY HEYWOOD

Treasury Chambers, Parliament Street, London, SW1P 3AG

RESTRICTED - POLICY

PRIME MINISTER

29 June 2001

MANAGEMENT OF PROJECTS

Early evidence from the OGC's Gateway scrutiny of major projects shows 70% suffering critical weaknesses, the most common being lack of appropriate skills. The evidence points to the importance of ensuring that top priority projects have high calibre management accountable at the highest level.

A recent meeting of the Supervisory Board of the Office of Government Commerce (OGC), which I chair and is made up of a number of Permanent Secretaries from across Whitehall, considered progress on the Gateway process. The Board agreed the conclusions were important and pressing and I said I would minute you accordingly.

The Gateway process, launched in February, applies the best techniques of staged appraisal to investment projects, and is especially valuable in keeping complex, innovative and risky projects, for example innovative IT systems, on track. It is a key to delivery of investment and services to the required quality, on time and to budget.

The Gateway process is now providing us with the first 'real time' information on progress. It has already begun to highlight some generic problems at the early stages of projects. Our evidence shows that 70% suffer from at least three of the five most common critical weaknesses. The most frequently found deficiency is a lack of appropriate skills. The other four are a need for clarity about management roles and responsibilities, inadequately defined success criteria, weakness in the level of risk management undertaken, and a shortage of market knowledge.

The Board agreed that we need to respond urgently to the emerging lessons. We need renewed efforts to address persistent and fundamental weaknesses. The Gateway process helps to do this by spotlighting problems at much earlier stages in projects than we have previously been able to do, thus enabling the OGC to work with departments, including their agencies and NDPBs, to take corrective action both at the individual project level and to significantly reduce the incidence of such problems in the future.

But it is becoming clear that departments need to do more to get, and keep, their service delivery projects on the right track. This requires both:

- behavioural change, including far greater recognition at the top that public services will not be successfully delivered if critical projects fail or get delayed, and
- much more senior input at Permanent Secretary level, and those reporting directly to them.

Two of our other key initiatives, Achieving Excellence in Construction and Successful Projects in an IT Environment (SPRITE), are also highlighting the need for the professional management of major projects and programmes.

Successful delivery must be seen as a core activity in the Civil Service and our best available talent deployed on the management of critical public service delivery projects in each department. To tackle this head on, departments need to ensure they have identified their top priority projects and assigned top quality people to them.

This all links very naturally to the work which Sir Richard Wilson is doing on improving our delivery capability through promoting greater interchange and training in project sponsorship at the top of the civil service. I know that he is inviting Peter Gershon to share these lessons directly with a wider group of Permanent Secretaries on the Civil Service Management Board. It would be helpful also to involve the Delivery Unit in supporting departments in ensuring that they have the people and skills needed to deliver successfully the projects central to attainment of their key objectives.

I am copying this to colleagues in charge of departments, Gus MacDonald and Sir Richard Wilson.

ANDREW SMITH

SUCCESSFUL DELIVERY OF PROJECTS

The successful delivery of projects (and programmes comprising a number of interdependent projects in support of a common goal) involving the acquisition of goods, services or works from the private sector is a critical success factor for the new Government. This short paper, based on my private sector experience in project-based industries, sets out some thoughts on what Central Government (Departments, Agencies and NDPBs) needs to address in order to improve its capability in this area, especially in the area of high and medium risk projects, so as to help deliver the Government's objectives and avoid the incidence of high profile project failures.

By way of introduction it is useful to recap two points:

1. Projects have the following characteristics:
   - a well-defined finite life-cycle
   - all contain risk and uncertainty
   - complex cultural, economic, organisational and technical interactions
   - no two are identical
   - the outcome is invariably impacted by decisions made early in the lifecycle

2. Many projects in Government are undertaken by client organisations on an infrequent basis, making it difficult to develop and sustain the necessary management capabilities. This lack of expertise increases the risk of a successful outcome.

My assessment is that at the heart of the challenge to Government lie two fundamental questions:

- is the successful delivery of projects regarded as an essential core competence of Government?

- to what extent should all projects funded with taxpayers' money be required to operate within a standard framework that encourages and supports success, and avoids unnecessary duplication and learning from (often) bitter and costly experience?

I shall now consider each of these questions in turn.

A. ESSENTIAL CORE COMPETENCE?

In simple terms if the answer to the question is "no" then Ministers and top officials have to recognise the inevitable consequence that the delivery of projects will continue to be inconsistent and unpredictable, and, with increased investment funds being made available, the number of project failures will increase! We shall continue to live in a world characterised by heroic fire fighting activity, adverse publicity, and brilliant performances in front of the PAC.

If the answer is positive the focus turns to developing and sustaining such a core competence which enables HMG to successfully harness the capabilities, products and services offered by the private sector. In my experience this has a number of interrelated components which have to be addressed:

1. **SKILLS**

a) Are the top management, senior responsible owners and other key resources being trained and developed in a consistent way to discharge their responsibilities in the successful delivery of projects and to use standard tools and processes?

b) What mechanisms are in place to identify and nurture key specialist skills (eg project management)?

2. **PROCESSES**

Are there standard processes for managing and reviewing projects, and identifying and managing project risk? (N.B. With the introduction of the Gateway Review process HMG now has a standard process for independent reviews at key points in the project lifecycle)

3. **SYSTEMS**

a) Are there common systems for measuring project progress in cost, schedule and output terms?

b) Are Ministers and top management provided with regular progress reports on all significant projects, including those in the relevant Agencies and NDPBs?

4. **TOOLS**

Is there investment in, and use of standard sets of management tools and methodologies (eg PRINCE)?

5. **ALLOCATION OF SCARCE RESOURCES**

a) Do top management allocate sufficient time to reviewing progress on their most significant projects? (N.B. this may require organisational changes in some organisations such as the appointment of a Chief Operating Officer or Board level projects Director).

b) Are the best people working on the most significant projects? (N.B. this may require directed re-allocation of resources across Departmental, Agency and NDPB boundaries).

c) Do senior responsible owners spend sufficient time discharging their project responsibilities?

6. **VALUES**

a) Is there an explicit value that projects will be delivered to cost and schedule, and meet agreed business requirements?

b) Do the reward and recognition systems support this?

c) Is there intolerance of behaviours where narrow interests threaten project success?

B. STANDARD FRAMEWORK

As with many other aspects of Government there are arguments both for and against allowing every accounting officer to determine the most appropriate way of achieving the successful delivery of projects in his/her Department, Agency or NDPB.

I do not believe the status quo approach is viable for the following reasons:

1. It has failed historically to produce a consistent level of even acceptable, let alone world-class level, of delivery of projects.

2. The evidence emerging from the Gateway Reviews undertaken on pre-OJEC projects earlier this year continues to indicate very serious weaknesses across a broad range of projects i.e. there is evidence of continuing failure.

The heightened emphasis by this Government on successful delivery requires a radical response if there is to be a step-change in HMG's capabilities in this area.

One solution is to develop a standard framework comprising all of the components described above, within which all significant HMG projects are conducted. This would create the environment in which HMG-wide organisational capability can be developed and enhanced as well as providing a much greater level of assurance about the standards of management of projects being applied across the board. It would of course be open to Accounting Officers to seek dispensation if they felt that parts of the framework were inappropriate to their business needs.

CONCLUSION

The problems that HMG faces in improving its capability to successfully deliver projects are not novel. Resolution of these problems requires firstly recognition that this capability needs to be a core competence of Government and secondly a decision on how such a capability should be developed.

PETER GERSHON
OGC
11 JUNE 2001

Secretary of the Cabinet and Head of the Home Civil Service

PRIME MINISTER

DATA PROTECTION ACT

The Lord Chancellor in his minute of 12 July about data protection proposes that we should:

i. **produce robust guidance on handling subject access requests as quickly as we can;**

ii. **look further at the extent to which we could legislate for further exemptions under the Act, but only do so if experience after robust guidance and robust interpretation of the exemptions proves these to be insufficient in practice in any area.**

2. This approach, while helpful, seems rather more optimistic about the likely success of a robust approach than our experience so far suggests is likely. Derry Irvine also accepts rather lightly the extra work which these cases involve for Number 10 and the Cabinet Office. I think we should ask him to put in hand urgently not only the robust guidance which he helpfully proposes but also the work on legislation which he seems a little wary about. If you agree I will give your office a draft accordingly. And as a first step, as agreed this morning, we should test out on him the advice which we are getting

I have sent him the papers.

3. My own view is that the legislation is flawed, not least because we have not taken full advantage of the exemptions allowed under the EU directive. There are four particular concerns:

i. personal data where the legal definition of the material which we are required to release is extremely wide;

ii. the lack of specific exemptions for policy documents;

iii. the lack of specific exemptions for material on international affairs; and

iv. the amount of bureaucracy required in releasing material where there is no real protection against disproportionate effort and the work is time consuming.

Putting this right may be difficult. But we are caught between a rock and a hard place.

4. It is helpful that Derry Irvine thinks we can be more robust about what we disclose. We need to test out how far this is so in practice. Unless there really is a lot more scope than we are being told at present to cut back on what has to be disclosed, and to reduce the work involved in each case, the arguments for legislation seem stronger than he acknowledges.

5. It seems clear that the basic problem is that we have not made full use of all the exemptions which the EC Directive would allow in respect of public security, the protection of important economic and financial freedoms and the protection of rights and freedoms of others. Building on these exemptions seems the most promising way forward. The Danes for instance have an exemption to protect 'vital public interests' although it is not always clear what they base this on. It seems to me that we ought to do a thorough study of what other EU countries have done and make use of their practice as precedents where helpful.

6. In addition we might consider whether it would be possible to make changes to the legislation by Order under the Regulatory Reform Act 2001 in order to reduce the burden where justifiable within the EU Directive

7. In the longer term we might conceivably seek changes to the EU Directive itself, including, for example, introducing a specific exemption for the workings of Government. But this would require support from the Commission, which has the sole right to propose amendments and shows no sign of contemplating any such action.

8. I attach a paper prepared by Jonathan Tross which helpfully analyses the position in more detail.

RTW

RICHARD WILSON
16 June 2001

Ref. AO2001/1826

DATA PROTECTION

BACKGROUND

The issue is the right of people to have access to the data held on them. The right is most extensive in relation to electronic records; less so on manual records.

2. The current provisions reflect a long history, in the course of which the access rights have broadened: from the original Data Protection Act of 1984 implementing a Council of Europe Convention; through the 1995 EU Directive on the Protection of Personal Data, given effect in the Data Protection Act 1998; with further changes on manual records due when the Freedom of Information Act 2000 is implemented. Over time the right of access has broadened from electronic to manual data, and the coverage of personal data releasable has extended. Originally, primarily an obligation affecting large scale computerised service provision in the public and private sectors, the effect now reaches the centre of departments with the spread of electronic Government. A few general points:

i. The definition of personal data to which people have access is wide. The Directive defines this as "any information relating to an identifiable natural person". The 1998 Act covers data relating to a living individual who could be identified from that data and includes expressions of opinion or intention towards the individual. The definition covers data which is obtained, recorded, held or acted on. So capture and storage as well as active use of the data are covered;

ii. There is no formal exemption for Government policy making, although people have the right only to data about themselves, not to that of others or the policy itself;

iii. The drafting of the legislation is not easy but generally requires case by case consideration. So there is inevitably uncertainty. It is hard to produce hard and fast guidance;

So, while there are things we can do within the law, substantive further restrictions in the law would need Law Officers' confirmation to proceed.

(a) Better management of our current obligations

3. We have taken Counsel's advice on where we might take a restrictive interpretation. The potential areas are:

i. Provision of material: we should relay material taken from documents not the documents themselves;

ii. Recipients and names of commentators: we should seek to refer to classes of recipients (e.g. Ministers) rather than named individuals and to respect the right of those commenting to their personal data privacy. But there cannot be a hard and fast rule on this, Counsel advises;

iii. National Security: there is an exemption for National Security. We should look to protect as much of our international dealings as we can under that heading. On the more normal security aspects, we should take a rigorous line on areas we want to protect

iv. Electronic data: we should treat material (such as deleted e-mails) we have sought to remove from the system as outside the scope of access and take advantage of the protection for back up material till October (looking for further protection thereafter – see below);

v. Manual material: we should use the transitional exemption till October, and thereafter apply rigorously the restriction to material in structured files rather than extend the search. There is a longer term issue on unstructured files (see below);

vi. Further information: we should use, where we can, the right to request more information to help identify the material. But realistically this may not help much with electronic material given current search engines.

4. If you are content, we will then circulate revised guidance across Whitehall reflecting this approach.

5. And there is more we can do simply through smarter handling. Some departments have searched and offered more than strictly they need to; have presented the material back to people in a way that is counter productive (names dotted on otherwise blank sheets of paper); and there has been insufficient co ordination of round robin access requests. It would help if you were specifically to endorse the best practice guidance and make clear your expectation that people adopt common handling, without over compliance. We should use, the network of experts co-ordinated by the Cabinet Office as a clearing house.

(b) Changes to our law within EU obligations

6. The EU Directive broadened rights of access to data in relation to matters covered by Community Law. The UK abstained on its adoption (all others supported). It added coverage of manual files. It is broadly worded in terms of coverage of data, but does include specific exemptions which might be looked at. However Counsel's initial reaction was that the room for manoeuvre was limited.

7. So far as implementation is concerned, France, Ireland and Luxembourg have not so far transposed. Others have in different ways. Some have copied out the provisions of the Directive – it is too early to understand the practical effect. Others have adopted specific exemptions beyond those we have – e.g. Denmark has an exemption to protect "vital public interests" and a time limited exemption for drafts, although it is not always clear what is the legal basis in the Directive. Of the two main areas for action, building on the exemptions looks more promising than varying the definitions in our law.

8. Areas you might be asked to be looked at include:

i. Adoption of EU exemptions: the EU Directive contains some exemptions we have not directly transposed – public security, important economic or financial interests of a member state, and protection of rights or freedoms of others (although we have relied on them for some of our specific exemptions, e.g. corporate finance and some specific appointments). Others, such as national security, regulatory functions and prosecution for offences, have been more directly transposed. One option would be to copy out the wording of the Directive given their potentially broad nature. However, we could not be confident how that would be interpreted either by the Information Commissioner in giving her authoritative guidance, nor the Courts. The better way would be to introduce specific provisions relying on the general exemptions we might exploit in (ii) to (iv) below;

ii. National and Public Security: we could explore using this exemption to give more cover to protection for our international dealings,

We would need to test with lawyers how far we could rely on the worded exemptions to cover specific exceptions for international dealings etc. We could also test whether "public security" can be extended into more general protection of the workings of Government, although the prospects may not be promising;

iii. Economic and financial interests: this is currently used to cover protection of tax raising and commercial corporate finance. We could look to test whether that could be built on to cover broader commercial interests and confidentiality, and protection of public money beyond tax itself. That might also be welcome to business;

iv. Rights and freedoms of others: this may be the origin of some of the qualifications of access other States appear to have made. We could look to see whether we could extend this into protection of advice and comment given in the expectation of confidentiality as a potential (but risky) way into protecting Government policy, as well as more obvious areas such as personal references. Also look at any scope for protection of material which has been passed on by its originator/owner in confidence to others. We may (no more than that) be able to use this provision to support some "disproportionate effort" test although this is straining the interpretation of the Directive;

v. Back-up and deleted data: look to see whether we can get a basis for restricting access to data in effect removed from use. Although the legal basis is not clear, we doubt if other States plan to search back-up material. We could combine that with looking at other changes which reduced the bureaucracy of notification. Areas that business too would welcome;

vi. Public appointments: we could review the earlier policy decision to restrict protection of data in public appointments to only a limited number of crown appointments;

vii. Manual records: the Directive restricts access to manual files to specifically structured material. The FOI Act, when implemented, will extend access to unstructured manual material in relation to public bodies (but with exemptions for public appointments). This was to bring Data Protection in line with FOI law. There are good reasons for that. However, we could either delay implementation to the maximum 5 year period after enactment, or indeed review the provision;

viii. Definition: generally the Directive gives us little comfort. However we could consider whether the EU reference to "identifiable individuals" gives us any scope to restrict access where the material is a by-product of more substantive information;

ix. A two-tier system: the coverage of the Council of Europe Convention is in principle broader than the EU Directive given

the latter's link to community law, (although the EU provision extends access within that competence.) It would in principle be possible to operate a two tier system reverting to a Council/1984 regime for non-EU material. However, that was explicitly rejected – people including business thought it would be burdensome and unworkable. That seems right – we would not propose to explore further;

x. charging regime: the basic maximum fee is £10, which some departments waive. Although this would not deter some of the people who have sought to exploit the Act and conversely might deter some with a legitimate interest in their data, we could raise the fee, particularly where significant effort was required; for example raise to £50. The Directive says that the fee must not be "excessive". A decision is needed soon on release of medical records which currently carry a £50 fee. Against DOH wishes it is due to come down to £10;

xi. time limits: there could be eased possibly by use of a target figure at the current limit but with some scope to extend in particular cases. The Nordic countries offer some support for this approach. Although the DP 40 calendar day limit is longer than the FOI Act 20 working days.

9. Changes would in the main require primary legislation. However, where we were reducing a burden which covered the private as well the public sector, we might be able to use the Regulatory Reform Act orders. Changes to charges would need subordinate legislation.

10. All the above comes with a considerable health warning. They all have more or less risks; if you are attracted we would need advice from the Law Officers to confirm there was an arguable legal basis for their implementation.

(c) Amendment of the EU provisions

11. In principle, there is a hook to re-open aspects of the EU provision with a Commission Review of implementation this Autumn. However, we understand the Commission will be adopting a minimal approach, essentially reporting on the state of transposition rather than the effectiveness of the Directive. Given the Commission right of initiative, if you wanted to pursue changes, it would require some sustained effort with like minded colleagues in Europe. Areas that we might in principle explore include:

i. International dealings: more specific exemption for international dealings including negotiation between Member States, to the extent not coverable above;

ii. Policy protection: more recognition of the need to protect the workings of Government, as the Commission have put in for the FOI regime in respect of their own EU handling;

iii. Definitions: some restriction of access to direct and actively managed data;

iv. Bureaucracy: changes to those parts of the Directive which require cumbersome procedures, and introduction of the concept of disproportionate effort;

v. Back up and deleted electronic material: strengthening of the concept of deletion of material, and protection of back up data, to the extent not covered above.

12. All of this is uncertain and long term. Judgement is linked to how far we can meet our needs by change within our current EU obligations. Subject to that, do you wish us to pursue?

(d) Context

13. The law is extremely uncertain, so we will have to take legal advice on what is possible. There are three further points of context that are relevant:

i. Information Commissioner: she has a statutory remit to give advice and enforce compliance. She will be concerned to protect the rights of access of individuals and will be critical in public of attempts to introduce restrictions;

ii. Parliament: although there will be grumbles about tightening up, your majority in the Commons will enable you to take through main legislation. However, this is an area where the Lords will take a particular interest where you have no majority, where they are likely to protect existing freedoms as they see it. The Liberal Democrats in particular will be hostile;

iii. E-Government: the PIU Study looks for more use and sharing of electronic data in delivering public service. There needs to be public confidence in the accuracy and integrity of use of that data, which implies more right of access and correction. You will need to balance and distinguish needs of public services against government policy considerations.

14. Finally, the obvious practical point - we are where we are – it is harder to row back now from what was introduced as recently as 1998, as compared to a situation where you are legislating for the first time. None of these factors undermines the case for review and consideration of action, but they will need to be reflected in the handling of any changes.

27 June 2001