Guidance Note E9: Redaction of Personal Data

Includes information extracted from the *MOD DPA 1998 Guidance Note 12 Redaction of Personal Data* See also *Guidance Notes B2 Data Protection Act* and *E8 Redacting*

Data Protection Act 1998

Personal Data

1. "Personal data" (within the meaning of s.1(1) Data Protection Act 1998 (DPA98) means data which relates to a living individual who can be identified from those data or from those data and other information in the possession of, or which 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.

1.1 **Remember that the current MOD policy is that we remove names of officials from documents unless it is obvious (you wrote the document and you are responding) or you have their permission.** It is not always necessary to quote S.40 when removing names from documents where the name is not the information. For example, if the fact that Jane Bloggs wrote document X is not pertinent to the request it may be removed. The simple test is whether you would feel it appropriate to add the name into the response if you summarised the document to answer a request. If not, then the name could be removed without the need to quote S.40.

1.2 Cases where persons (e.g. officials or others) are seeking access to information about themselves must of course be treated as **Subject Access Requests** (SAR) under the provisions of the Data Protection Act 1998 (as extended by the Freedom of Information Act 2000).

1.3 It must be borne in mind that civil servants do not have an absolute right to anonymity. Indeed, a large number of civil servants already to some extent have a public face e.g.

- Staff working in front line service-delivery may already be operating under policies of public identifiability.
- Some senior executive staff work in a context of direct personal public accountability.
- The names and job titles of senior officials are already published in, for example, the Civil Service Year Book.
- Public contact names and numbers are available in many contexts in Government publications and on websites.
- Individual civil servants (not just very senior ones) speak publicly at conferences, etc.

1.4 There is no case for seeking to withhold under the FOI Act information of this sort which is already in the public domain. FOI exemptions should be considered *only* in cases where complying with a request would involve putting new information into the public domain. That will need consideration on a case by case basis. The fact that an official's name and job title are public does not automatically mean that, for example, his or her contact details, or the fact of his or her personal involvement in particular activities, are in the public domain.

1.5 Care should be taken when handling FOI requests relating to the costs of Official Residences. There is a clear public interest in knowing how public money has been spent but you must ensure that any disclosure relating to costs does not disclose personal information, such as the accommodation charges which the individual is paying for the residence. Occupation of an official residence does not mean that the address must be disclosed, it remains the residential home of the occupant and his or her family. The address can constitute personal data (when associated with an individual) and section 40 is engaged. However there is also a security dimension. All senior Service officers are considered to be potentially subject to the threat of terrorist attack. To minimise this possibility, their addresses are kept out of the public domain, both

for their own protection and for that of those who live or work with and around them. The consequence of disclosing the requested address would be substantially to increase the potential risk to a number of individuals. For the same reason addresses of MOD official residences should not be disclosed, even when the request is unconnected to any particular occupant. Section 38(1)(b) of the Act (Health and Safety) relating to disclosure that would, or would be likely to, endanger the safety of any individual should be cited . Section 38 (1)(a) (disclosure that would, or would be likely to, endanger the physical or mental health of any individual) also applies, as others may be at risk. To reveal the residential address could also be argued as breaching Article 8 (right to respect for private and family life) of the European Convention on Human Rights.

1.6 The extent to which Departments choose to make public information identifying individuals is now standard policy following the introduction of FOI. But in each of the cases mentioned above, it is important not to lose sight of the fact that only *some* identifying information is made available – and in very many other contexts no identifying information is available about an official. There may very well be good reasons for that, and it is not just, a question of the preferences of individual officials in the matter of public identification. This is the context in which the possibility of relying on an exemption to refuse disclosure needs to be considered.

1.7 Actual salary details and individual bonus payments are personal information and should not be disclosed without the consent of the individual.

See also paragraph 15 of this Guidance.

What is "Redaction"?

2. In the DPA 98 context, it means deleting information, to which the data subject (the individual who has made a SAR) is not entitled, from the personal data that are to be released to him/her in response to his/her SAR.

What is the process?

3. A copy of the information must be taken before any redaction takes place. Originals must not be used as these are Departmental records. In order to redact information, it is suggested that: (a) the information to be withheld is cut out and then the document photocopied and given to the data subject; or (b) redaction tape can be used and, once the text has been covered up, a photocopy of the redacted document may then be given to the data subject; or (c) a black felt-tip pen (i.e. opaque ink) is used to obliterate the ineligible data and then a photocopy is taken of the redacted document (to prevent reading the redacted data through holding the page up to the light). If using (c) particular care must be taken to ensure that the withheld information cannot be read through the ink.

Who is responsible for redaction?

4. If the document has been generated by MOD, its originator is responsible for redacting the information because he/she will be best placed to decide what can and cannot be released in accordance with the Act. If the information does not originate from MOD, then the owner or, in cases where it is no longer possible to contact the owner, the holder of the information must be asked to decide whether any redaction is required.

When should redaction take place?

5. If, in response to a SAR, personal data relating to the data subject contains reference to third parties (e.g. names of officials or to other persons) or to personal details of other persons (e.g. addresses, telephone numbers etc) then those details must usually be redacted. In cases of official information, the appointment may remain but any details identifying the individual post (and

therefore the individual in it), should be redacted. For example, *"CIO Access Pol 1"* redacted becomes *"CIO Access Pol"* and the name of the post holder should also be deleted.

5.1 There are exceptions to this general rule. For example, it may be inappropriate to redact names where the individual is known to the data subject e.g. individuals seeking copies of their annual reports will know the names of the various reporting officers or if an official has been in correspondence with the data subject. The Information Commissioner's office has stated that they would not expect names of public figures to be redacted. For instance, Secretary of State's name and appointment are well publicised and are in the public domain.

Exemptions

6. There are provisions in the **DPA98** Act which permit data controllers to withhold certain types of personal data to the data subject. The main provisions of interest to MOD are:

Exemptions:

- Section 28 – *National security* - see paragraph 7 below
- Section 29 – *Crime and taxation*
- Subsection 33 – *Research, history and statistics*
- Schedule 7 – *Miscellaneous exemptions* , paragraphs (1) – *Confidential references given by the Data Controller* , (2) - *Armed Forces*, and (10) - *Legal professional privilege* and other paragraphs

(Other exemptions are listed in Part IV of the Act, which can be viewed at http://www.hmso.gov.uk/acts/acts1998/19980029.htm).

6.1 **Third party confidentiality**

- Subsections 7(4)(5)(6) and subsection 8(7) – Confidentiality and third parties

Paragraphs 6.1 and 6.2, above may assist when considering requests for personal data.

National Security, Crime and Taxation

7. Examples of redaction is that necessary for the purpose of safeguarding National Security (s28 DPA98 – *National Security* refers) (see *DPA Guidance Note 7*) or for the prevention or detection of crime or for the apprehension or prosecution of offenders (s29 DPA98 – *Crime and taxation* refers).

7.1 There may be cases when even to disclose the existence (or not) of personal data may be prejudicial to the safeguarding of national security or may jeopardise an investigation.

Do we need to seek the consent of third parties? What about information provided in confidence?

8. In some cases (e.g. medical information) individuals may have provided information on the understanding that it would not be disclosed to the data subject. This should be clear from the papers. Information specifically provided in confidence should be redacted unless the consent of the provider to the release of the information to the data subject has been given in writing, and then only the relevant extract should be provided.

8.1 In other cases, individuals may have provided the information without realising that disclosure might be sought. In such cases, a judgement needs to be made whether to seek the consent of the individual and, if so, consent should be sought in writing, providing a copy of the information in question for review.

What is the situation regarding references? See DPA *Guidance Note 13*.

What happens if there is only one line in the document that contains personal data?

10 You may decide either to redact the whole document except for the relevant line, or to type out the releasable extract and provide it on a separate sheet, explaining to the data subject why you have done so.

What about CCTV images, digital images and photographs?

11. Individuals asking to see any of these must be asked to provide a photograph as part of the initial authentication procedure (*see DPA Guidance Note 2*). Times and locations when the data subject's image were purportedly caught on CCTV will also be necessary, as MOD CCTV systems are 24 hour and 7 days a week coverage. All requests should be dealt with by a designated member of staff.

11.1 Images captured digitally or on CCTV will need to be carefully reviewed. If the data subject is part of a group of persons then the identifiable images of other persons should be redacted unless consent can be sought, if feasible. Where practicable, the data subject should be asked if they would be satisfied with merely viewing the images recorded. Any travelling expenses etc are to be met by the data subject.

11.2 Any redaction of CCTV or digital images must be carried out electronically by the holder of the equipment. Replies to SARs for images must be provided within the 40 calendar days stipulated in DPA 98. (For further information see the Information Commissioner's CCTV Code of Practice. MOD policy contained in *DPA Guidance Note 17* – "Security Closed Circuit Television (CCTV) and the Data Protection Act 1998")

What about restricted areas?

12. It is unlikely that a CCTV image will disclose restricted areas, as cameras will have been sited to prevent persons gaining entry to such areas. However, it is possible that the disclosure of non-restricted images may reveal certain vulnerabilities, such as the .scope of the camera sweep. It is possible that some or all of the images requested may be exempt from disclosure either on grounds of s28 (National Security) or s29 (Crime and Taxation) of DPA 98. However, in the majority of cases, all but the data subject's image can be redacted electronically.

Do we have to tell the individual why we have redacted the information?

13. The advice of the Information Commissioner's Office is that data holders should not provide the data subject with reasons for any redaction. The reply to the data subject should include the words *"You asked for (as set out in their SAR). I attach copies of the personal data to which you are entitled under the Data Protection Act 1998."* However, much will depend on the data subject, whether there has been earlier correspondence, and so in such cases it may be helpful to explain the reason for, say redaction e.g. relates to third parties, is not personal data relating to you.

Record Keeping

14. Data holders must keep a copy or a comprehensive record (i.e. a list of documents disclosed) of what was provided to the data subject, together with the reasons for redaction, in case their decisions are subsequently challenged. See also MOD Form 1694 – **Subject Access Request Form** (Revised Jan 2008) which sets out the SAR retention period of 2 years.

Freedom of Information - Guidance to removing Individual's Names and Contact Details from information provided in FOI Responses

If in any doubt please contact the CIO Information Access DPA/FOI Team for clarification.

If the names are not part of the information requested

15. If the applicant has not asked for names in their request then they should be redacted as they are not relevant to the information requested. For instance if some one has asked for copies of all communications about a certain subject then the names and contact details of the people sending and receiving those communications should be removed. The accompanying letter should say something along the lines of "the names and contact details of individuals have been removed as they are not a substantive part of the information you requested." Be sensible though - there is no need to remove PUS' name as his name and appointment are already in the public domain.

If the names are a central part of the information requested.

15.1 If the applicant has asked for the names of staff then an exemption may have to be used to withhold the names. You should contact the CIO Access FOI team to discuss which might be the most applicable exemptions to use. Exemptions may include:

- S36 - Prejudice to the conduct of public affairs
- S38 - Health and Safety
- S40 - Personal Information
- S41 – Information provided in confidence

15.2 Requests that may fall into this category may include requests for staff lists or directories, names of staff who attended a specific meeting or a copy of an organisational chart. The names of some senior officials and their responsibility for a particular subject are already made public (via the Civil Service Yearbook). In these cases it may be inappropriate to withhold the details.

15.3 As a general rule the names of officials below the Senior Civil Service (1* or equivalent), should be withheld unless an individual is in an outward (public) facing post and their name is already in the public domain.

For further information on this subject please contact the Data Protection Team in CIO Information Access.