The Campaign for Freedom of Information

Response to Home Office Consultation on EC Data Protection Directive (95/46/EC)

5 September 1996

The Campaign for Freedom of Information has a few general comments on the above consultation, though the bulk deal with the Directive's proposed right of access to manual records.

The Government proposed to create a new right of access to manual records held by public bodies three years ago in the 'Open Government' White Paper. (1) We regret that the promised legislation has still not been introduced. We therefore particularly welcome the new right of access to manual records under the Directive and the fact that, unlike the White Paper proposal, it will apply retrospectively, to existing manual records, and to records held in the private sector.

General observations

Exclusion of public security etc

We agree with the Data Protection Registrar's strongly expressed reservations about the exclusion from the Directive's scope of processing concerning public security, defence, state security and the state's activities in relation to criminal law. Many of these matters are already covered by the Data Protection Act (DPA), subject to appropriate exemptions. To exclude them from the new legislation altogether will create bizarre inconsistencies. In addition, it appears that some of the manual files which might not be covered by the Directive, could be subject to the White Paper's proposed right of access - police records appear to be one example. (2) We therefore regret the government's statement that it "intends to go no further in implementing the Directive than is absolutely necessary" (3) which we regard as incompatible with the White Paper's commitment to legislate for wider access to manual files.

Defence, security and law enforcement should in our view be subject to the new

legislation, with appropriate exemptions to protect vital interests. In particular, the expansion of the role of the security services, not merely into areas of traditional police activity but also into some aspects of 'civilian' civil service work (such as the transfer to it of some of the CCTA's responsibilities for computer security in Whitehall) makes it all the more important that, subject to necessary exemptions, the security services should be covered by the new legislation. The Cabinet Office has previously stated that the transfer of these computer security functions to the security service "has no implications for withholding of information that would otherwise be available to the public or to MPs". (4) We hope that this will mean that, in relation to these functions, the security service will be subject to the disclosure provisions of the Code of Practice on Access to Government Information, to the subject access provisions of the Data Protection Act and to any equivalent provision on access to manual files under the Directive.

Primary legislation

We agree with the Registrar's view that the Directive should be implemented by primary legislation. It would be inappropriate for such significant matters to be dealt with by secondary legislation, with its limited opportunities for Parliamentary debate and scrutiny, particularly as apparently minor nuances in the drafting of the new provisions will have substantial implications for the rights of individuals. If the Directive were implemented by secondary legislation there would be no power to go beyond its literal scope - for example by including manually held police records. In addition, the the actual wording of the Directive might have to be incorporated directly into UK legislation even where it is unclear or confusing. We have some experience of another area in which this has been done - the implementation of an EU Directive on access to environmental information, (5) which was introduced in the UK by secondary legislation and imported the Directive's wording in a number of key definitions. As a result, some central provisions of the Regulations are drafted in terms which have no clear meaning in the British context and these ambiguities have permitted some bodies to avoid their obligations under the Directive, perhaps having calculated that they are unlikely to be judicially reviewed on the point.

Duty of professional secrecy

Article 28.7 of the Directive requires that the supervisory authority should be "subject to a duty of professional secrecy with regard to confidential information to which they have access". This should not be translated into a statutory prohibition on the disclosure of information by the supervisory authority. Such restrictions in UK legislation have often proved unnecessarily broad and inflexible, preventing regulatory bodies from properly explaining their decisions to act (or not take action) in particular cases, even where they themselves wished to do so and where the information could be provided without breaching either individual privacy or business secrets. The Data Protection Registrar is not currently subject to any statutory restriction on disclosure and we are not aware of any problems as a result. The common law obligation of confidentiality already provides a "duty of professional secrecy" which should be sufficient to meet the Directive's requirements.

Manual records - consistency between access rights

The Directive would provide an opportunity to bring various existing rights of access to personal files into line with each other, and this has been advocated by the Registrar. However, a number of these are, in some important respects, significantly more favourable to the individual than the Data Protection Act.

We naturally hope the new right of access under the proposed legislation will be based on the higher standards of these existing rights. If this is not possible, the existing provisions should be retained in their present form - even if this leads to the preservation of inconsistencies.

Access rights that are superior to those under the DPA

The sections that follow describe those existing rights which are superior to those under the DPA and which in our view should not be sacrificed in the interests of consistency.

Fees

The DPA's £10 application fee is high, and will deter some potential applicants from exercising their rights. Fees under some other access laws are lower. For example, the cost of obtaining copies of credit reference agency files, under the Consumer Credit Act 1974, is £1. (The Consumer Credit Act also offers applicants a number of other advantages compared to the DPA. It requires that information be provided more quickly, and provides for much fuller access than would be possible under the DPA.)

Some access laws permits applicants who want only to *inspect* records, without being supplied with copies, to do so free of charge. This is the case under the Education (School Records) Regulation 1989, (6) the Access to Medical Reports Act 1988 (7) and the Access to Health Records Act 1990 (for records to which information has been added in the past 40 days. (8) This allows patients who are currently receiving treatment to see their records free of charge, and to obtain copies at cost.) People applying under the Code of Practice on Access to Government Information for information held on their personal files by government departments have *free* access if the request can be dealt with within a specified period. This varies from 1 to 5 hours, depending on the department.

All these provisions are more advantageous to the individual than the DPA, and provide access without the same high cost. They should not be undermined as a result of the Directive. If consistency is an objective, it should be achieved by *lowering* the DPA fee, and not by raising others.

We agree with the Registrar's reservations about charging individuals for exercising subject access. (9) The existing fee will prevent some people whose records are in fact inaccurate from detecting and correcting errors which may jeopardise their rights. Someone who suspects that data is inaccurate may need to apply not just to a single data user but to a *series* of them, at £10 a time, to identify the source of the inaccuracy and to discover who else has received incorrect data. Inaccurate data from a social work record, for example, may also have been passed to the GP, health authority, school, local education authority, education welfare service and other professionals. To track these records down paying a separate fee for each application will involve what for many is a punitive cost. To add to the potential injustice, the fee is not refundable - even if no information is held, or what is held is found to be grossly inaccurate.

Moreover, the cost of applying to a single data user may be considerably more than £10, if the data user has separately registered data held for different purposes. We hope that the provisions of section 21(3) of the Data Protection Act, which permit such multiple charges, would not be retained under the Directive.

In our view access should normally be permitted without charge. One of the explicit purposes of the DPA is to ensure that personal data is accurate, a legal obligation under the fifth data protection principle. Encouraging individuals to check their records is one of the most effective ways improving accuracy, and thus securing compliance with the law. Accurate records are also indispensable for effective administration and for achieving the data user's commercial objectives. We question why people should be required to pay for the privilege of assisting organisations which hold information about them to achieve these benefits and to comply with their legal obligations.

Response times

The Data Protection Act allows the data user 40 days in which to respond to a subject access request. Again, this compares unfavourably with comparable provisions:

- The Consumer Credit Act 1974 requires access to be given within 7 days
- The Education (School Records) Regulations 1989 require access to be given within15 school days of the application (10)
- The Code of Practice on Access to Government Information sets a 20 day time limit for simple requests
- The Access to Health Records Act requires access to be given within 21 days, when access is sought only to information recorded in the past 40 days. (11) The purpose is to permit access to information about the patient's current condition to be given relatively quickly. Requests for other information are subject to a 40 day period.
- The Consumer Credit Act requires inaccurate information to be corrected within 28 days. Neither the DPA nor other personal files legislation provides a time limit

for the making of corrections.

We question whether a period as long as 40 days for responding to requests for access to personal data is necessary under the DPA, particularly as shorter periods have been considered adequate elsewhere. We suspect that it merely encourages data users to leave applications sitting in in-trays for a longer period before beginning to process them.

Third party information

The DPA provides a sometimes excessive degree of protection for third parties who have provided information about the data subject. Information about someone else or details which reveals who has provided information about the data subject can be withheld. (12) As a result the data user can suppress the names of any individual mentioned on the data subject's file, even if the person is acting for the data user in an official capacity. A government department could withhold the names of civil servants or ministers who had been involved in decisions about the data subject or merely corresponded with him. The same is true of people acting in an official capacity for any other organisation. There is no legitimate privacy interest in protecting such information.

A slightly more flexible approach has been adopted in other personal files legislation, where the identities of those acting in a professional capacity (such as health professionals, (13) social workers,(14) housing officers, (15) or teachers and local education authority staff (16)) are not protected. The Directive should not protect the identity of persons acting on behalf of the data user or in accordance with their duty on behalf of another organisation.

It should also be noted that the exemption for personal privacy in the Code of Practice on Access to Government Information is not phrased in the absolute terms used in the DPA. The Code exempts information whose disclosure would involve an "unwarranted invasion of privacy" (17) and even such information may be disclosed if "any harm or prejudice arising from disclosure is outweighed by the public interest in making information available". (18)

Notification that information has been withheld

Under the DPA, applicants are not told if information has been withheld under a subject access exemption and will not know whether they have received *all* the information held on them or an edited version. Equally, if they receive no information, they may not know whether this is because no information is held on them or because the *entire contents* of a file has been withheld. (Applications may be met with deliberately ambiguous responses such as *"We hold no information on you which we are required to disclose to you".*)

In this respect, the DPA falls short of the Code of Practice on Access to Government Information, (19) the regulations on access to housing records (20) and the Access

to Medical Reports Act 1988, (21) which all require that applicants are told when information has been withheld. Indeed, the first two of these also require the specific exemption to be identified. Such notification permits applicants to challenge any unjustified secrecy and discourages the arbitrary withholding of information. A similar procedure should be adopted in implementing the Directive.

It may be argued that to specify the exemption which has been relied on may, in some cases, undermine the purpose of the exemption. We suspect this will rarely be the case. However, if it is considered that it could be seriously damaging to acknowledge the particular exemption involved the data user could merely refer to the fact that information had been withheld under one of the permitted exemptions.

Access rights which are inferior to the DPA's

There are other areas, however, where existing access laws are clearly defective and fall well short of the degree of protection for the individual under the DPA.

Appeals

The most notable of these is the lack of an independent appeals mechanism under several sets of Regulations. Thus:

- *social work records* - appeal is to an ad hoc committee of three councillors of the local authority, one of whom may be a member of the social services committee (22)

- *housing records* - appeal is, at the discretion of the authority, either to a meeting of the full authority or to an unspecified number of councillors who took no part in the original decision (23)
- *school records* - appeal is to the school's governing body (24)

These procedures are all grossly defective. They permit a complaint to be dealt with by persons who cannot be assumed to be impartial and who may have an interest in protecting the body from embarrassment, criticism or legal challenge. We consider that whatever appeals mechanism is introduced in implementing the Directive should apply to all personal records, including social work, housing and school records. Another unnecessary requirement applying to manual social work and housing records is that any appeal must be made within 28 days of the decision complained of - a restriction not found in the DPA .

Exemptions

If a health professional wishes to withhold information that is potentially damaging to the patient's health from a medical record to which the DPA applies, the health professional must, in the case of a computerised record, be able to show that disclosure *"would be likely to cause serious harm to the...data subject"* (25) This is

an objective test. If the same health professional wishes to withhold information from the patient's manual record the test is that the record *"in the opinion of the holder of the record would disclose...information likely to cause serious harm..."* (26) This is a subjective test, which makes the decision almost impossible to challenge, except where it is demonstrably taken on grounds unrelated to any concern for the patient's health. We hope that such unjustifiably wide exemptions will be remedied by the new legislation.

Other matters

The Directive permits the data user to provide an applicant with the data held on him "in an intelligible form". (27) This is considerably less satisfactory than the present right, under the DPA, to be provided with a precise copy of the data held, with an *additional* explanation of any unintelligible terms. (28) Individuals must be entitled to a copy of the data held on them in *precisely* the form in which it is held. Rewriting it, so as to make it "intelligible" would provide an opportunity, irresistible to many data users, to suppress data. It would also be inconsistent with existing rights of access to manual files and with the 'Open Government' White Paper proposals on access to personal files, which proposed a right of *"access to the documents or papers - or more specifically to copies of documents or papers, with exempted material edited out as necessary".* (29)

Under the Directive data subjects will be entitled to be informed of "any available information" about the sources from which information about them have been obtained. Referring to this, the consultation document states *"Use of the word 'available' indicates that controllers need not go out of their way to find this information if they do not already have it".* (30) This comment should apply only to data obtained *before* the Directive is implemented. Once the Directive is in force data users should be required to record the sources from which data is obtained.

Footnotes:

1. Cm 2290, HMSO, 1993, Chapter 5.

2. White paper, paragraph 5.9

3. Home Office Consultation Paper, paragraph 1.2
4. Letter from Mr G.E.T. Green, Office of Public Service & Science, to Campaign for Freedom of Information, 29.11.94
5. Council Directive 90/313/EEC on the freedom of access to information on the environment, implemented by the Environmental Information Regulations 1992

6. Regulation 6(1)(b)
7. Section 4(4)
8. Section 3(4)(a).
9. Data Protection Registrar. *Our Answers. Response to the Consultation Paper on the EC Data Protection Directive*, page 57
10. Regulation 6(2)
11. Section 3(5)(a)
12. Data Protection Act, section 21(4) and (5)
13. Data Protection (Subject Access Modification)(Health) Order 1987, paragraph 4(3)(a); and the Access to Health Records Act 1990, section 5(2)(b)
14. Data Protection(Subject Access Modification)(Social Work) Order 1987, paragraph 4(4)(a); and the Access to Personal Files (Social Services) Regulations 1989, regulation 9(3)(a).
15. The Access to Personal Files (Housing) Regulations 1989, regulation 4(3)(b)
16. The Education (School Records) Regulations 1989, regulation 9(b)
17. Exemption 12
18. See the introduction to Part II of the Code, 'Reasons for Confidentiality'
19. The Code states that "Where information cannot be provided under the terms of the Code, an explanation will normally be given." *Code of Practice on Access to Government Information, Part I, paragraph 5*. The Office of Public Service's guidance on the code suggests that it might sometimes be necessary to to respond to requests relating to security, defence or international relations, without confirming whether the requested information exists but by stating that if it were held, it would be exempt. Even this, however, is a substantial improvement on the DPA approach which in all cases, even those which have no sensitivity, absolve the data user of the need to acknowledge that information has been withheld.
20. The Access to Personal Files (Housing) Regulations 1989, regulation 5(2)(b)
21. Access to Medical Reports Act 1988, sections 7(3)(a) and 7(4)(a)
22. The Access to Personal Files (Social Services) Regulations 1989, regulation 11(1)
23. The Access to Personal Files (Housing) Regulations 1989, regulation 8(1)
24. The Education (School Records) Regulations 1989, regulation 8
25. Data Protection (Subject Access Modification)(Health) Order 1987, paragraph 4(2)(a)
26. Access to Health Records Act, section 5(1)(a)
27. Article 12(a)
28. Data Protection Act, section 21(1)
29. 'Open Government' White Paper, paragraph 5.11(vi)
30. Paragraph 3.24