The Campaign for Freedom of Information

Suite 102, 16 Baldwins Gardens, London EC1N 7RJ
Tel: 020 7831 7477
Fax: 020 7831 7461
Email: admin@cfoi.demon.co.uk
Web: www.cfoi.org.uk

Graham Sutton
Lord Chancellor's Department
Freedom of Information and Data Protection Division
Selborne House
54-60 Victoria Street
London SW1E 6QW

March 28, 2003

Dear Graham,

Data Protection Act 1998. Consultation Paper on Subject Access.

I am writing to comment on the above consultation paper. We have no objection to this submission being made public.

We hope this review will start from the recommendation in the Performance and Innovation Unit's report on data sharing that "access to personal data should be improved".[1] It should not lead to new restrictions on access.

In this paper we make a number of specific suggestions most of which would bring the Data Protection Act (DPA) into line with the Freedom of Information Act (FOIA). These are that:

(a) subject access applicants should be entitled to know when information has been withheld from them and on what grounds

(b) applicants should be able to appeal to the Information Tribunal against decisions of the Information Commissioner

(c) in deciding whether to disclose information about another identifiable individual, data controllers should be required to take account of any *harm* that could be done by disclosing or withholding the information

[1] Cabinet Office, Performance and Innovation Unit, 'Privacy and Data Sharing', April 2002, paragraph 1.18

(d) the subject access exemptions should be subject to a public interest test

(e) people whose FOI requests in involve both the FOI and DP Acts should not have to pay charges under both regimes.

Applicants have no right to know when exempt information has been withheld

We think data controllers should be required to tell applicants when and on what grounds exempt information has been withheld from them, unless to do so would itself be damaging. This would bring the DPA into line with the FOIA.

Under the DPA data controllers can withhold information from someone making a subject access request without acknowledging that they have done so. The Act permits information to be retyped before disclosure, so any gaps left by the withheld information may not be apparent to the applicant. Moreover, data controllers often give deliberately ambiguous responses such as *"we hold no information which we are required to disclose to you"*. This makes it impossible to know whether no information about the applicant is held, or an exemption is claimed for the entire file.

There may be cases where it could be harmful to acknowledge the withholding of information, for example, where this might reveal to a suspected criminal that he or she is under surveillance. But most subject access requests do not give rise to such concerns.

For example, until we raised the issue with the Metropolitan Police National Identification Service, people applying for details of any prosecutions or convictions recorded against their names would often receive the evasive reply: *"there is no information which the Chief Officer is required to supply under the provisions of the Act"*. This could suggest that people were being denied access to details of prosecutions/convictions recorded against their names on the Police National Computer - an alarming prospect, particularly for someone who with no such record. Following our representations in 1997, the NIS agreed that in future where no conviction or prosecution data was held that they would say so directly.[2] There may be many other areas where similarly ambiguous replies continue to be given unnecessarily.

The FOIA will highlight the unfairness of this provision. An individual seeking his or her own file under the DPA will have no right to know when exempt information has been withheld. But an *organisation* applying for a file about itself under the FOIA normally *will* be entitled to know. Businesses will be better protected against errors and unfair records than the ordinary citizen.

[2] See attached correspondence which can be downloaded from this link.

Openness should improve public confidence in work of authorities – but this provision undermines that process, encouraging people to suspect that information has been withheld even when it has not. It contributes to the "lack of public trust" over the use of personal data, identified by the Performance and Innovation Unit.[3] The Prime Minister himself has acknowledged that the proposed benefits of data sharing "will only be realised if people trust the way that public services handle their personal data".[4] The starting point should be the right to know when information has been withheld and why.

Withholding third party data

A common reason for withholding information is that it relates to another identifiable individual. The DPA allows such third party data to be disclosed if the other person consents. Acknowledging that such information is held may allow applicants to seek consent from those who they may correctly guess to be involved and who may be willing to give it if asked.

Third party data can also be disclosed *without* consent if to do is "reasonable in all the circumstances".[5] But the data controller may have no knowledge of the applicant's circumstances or his relationship with the other individual, and may be unable to make any such decision without hearing from the applicant. As the Act stands, this is unlikely to occur, since the applicant will not be told that (a) third party data has been withheld or (b) the provision under which this is done contains a balancing test.

For example, the record may contain untrue statements made about the applicant by a malicious third party. The data controller may not realise that these allegations have been made before and disproved (eg by a child abuse investigation or an acquittal on a criminal charge). It may nevertheless conceal the allegations from the applicant, on the grounds they could only have come from a single identifiable informant. The applicant may have no idea that these allegations have reached the data controller and be denied the opportunity to demonstrate their falsehood, although they may prejudice the data controller's treatment of him. Of course, the applicant could volunteer the fact that false allegations have been made against him or her in the past, but people are understandably reluctant to risk damaging themselves further by unnecessarily drawing attention to such matters.

[3] Cabinet Office, Performance and Innovation Unit, 'Privacy and Data Sharing', April 2002, paragraph 1.14
[4] Forward to the PIU report.
[5] Data Protection Act 1998, section 7(4)(b)

We think the DPA should be brought into line with the FOI Act, by -

- requiring data controllers to notify an applicant when and on what grounds exempt information has been withheld;[6]

- waiving this requirement only where compliance would itself cause the harm (e.g. prejudice to law enforcement) referred to in the exemptions, *and* be contrary to the public interest. This is the double test found in the FOI Act.[7]

Exemptions and the public interest

We think the DPA should be amended to allow exempt information to be disclosed on public interest grounds, at least in the case of public authorities. This would bring the DPA into line with the FOI Act, the forthcoming Environmental Information Regulations and the present Code of Practice on Access to Government Information - which all contain such a public interest test.

Exemptions which *are* subject to a public interest test under the FOIA but not under the DPA include those for: national security,[8] the prevention or detection of crime,[9] regulatory functions,[10] danger to an individual's physical or mental health,[11] armed forces,[12] honours[13] and legal professional privilege.[14]

For many of these, the FOI and DP exemptions adopt almost identical wording. But because the DP exemptions lack a public interest test, decisions are *less* likely to result in disclosure than comparable decisions under the FOI Act. Ironically, this means that an applicant with a direct interest in a matter (because it involves his or her personal circumstances) has *weaker* rights than someone with no such interest.

For example, suppose the police have a policy of not investigating burglaries unless more than a certain value of goods are stolen, but do not disclose the cost threshold because they believe this would encourage burglars to steal up to this limit. The report on a particular burglary might acknowledge that the incident was not investigated because the value of the stolen goods was below the limit in question. The police might

---

[6] This would be analogous to section 17(1) of the FOI Act

[7] Under the FOI Act, an authority could to refuse to confirm or deny the existence of information prejudicial to law enforcement only where (a) confirming of denying that such information is held would itself prejudice law enforcement [section 31(3)] and (b) the balance of public interests favours confirming or denying that such information is held [section 2(1)].

[8] DPA s 28; FOIA s 24

[9] DPA s 29, FOIA s 31

[10] DPA s 31, FOIA s 31(1)(g)

[11] E.g. The Data Protection (Subject Access Modification) (Health) Order 2000, article 5(1); FOIA s 38(1)

[12] DPA Schedule 7, para 2; FOIA s 26(1)(b)

[13] DPA Schedule 7, para 3(b); FOIA s 37(1)(b)

[14] DPA Schedule 7, para 10; FOIA s 42

wish to withhold the reference to this limit, citing the DPA's law enforcement exemption - a decision which would be difficult to challenge without a public interest test.

However, if a policy document describing this limit was sought in an FOI request, a public interest test *would* apply and the applicant would be entitled to argue for its disclosure. The public interest case for disclosure might be that the threshold had been set so high as to allow most burglaries to go uninvestigated, and most burglars free to carry on stealing - an argument which, as the threshold increases (e.g. to £100,000), ultimately becomes unanswerable. A public interest test should be available regardless of whether, in any particular context, the information is dealt with under the DPA or the FOIA.

Applicants have no right of appeal to the Information Tribunal

Although the Information Commissioner plays a key part in enforcing both the DPA and FOIA, the enforcement procedures are inconsistent. This may cause confusion particularly where a request involves *both* laws.

To take a hypothetical example, someone may apply for information about the *handling of a complaint* which he or she has made to the authority, and the *internal guidance* on the handling of such complaints. The first part of this request would be dealt with under the DPA, the second under the FOIA. An applicant who was unhappy with both sets of responses would have to follow two different appeals processes. Although both could involve the Information Commissioner, any subsequent appeals would diverge.

Under the FOIA, either the applicant or the authority can appeal to the Information Tribunal against a decision of the Commissioner.[15] But under the DPA, only the *data controller* can appeal to the Tribunal.[16] The applicant's only remedy is to apply to the court.[17] So if the Commissioner finds that under both the FOIA and DPA the authority should have disclosed some but not all the requested, appeals could be made as follows:

(i) The *authority* may appeal to the Tribunal against the *FOIA* decision notice requiring it to disclose some of the requested information;

(ii) The *authority* may appeal to the Tribunal against the *DPA* enforcement notice requiring it to disclose some of the personal data;

(iii) The *applicant* may appeal to the *Tribunal* against the Commissioner's FOI decision *not* to require the remaining information to be disclosed;

---

[15] Freedom of Information Act 2000, section 57(1)
[16] Data Protection Act 1998, section 48(1)
[17] Data Protection Act 1998, section 7(9).

(iv) The *applicant* would have to apply to the *court* for an order requiring the authority to disclose the remaining personal data.

Apart from being confusing and wasteful, this division discriminates against the applicant in favour of the data controller.

- In court proceedings, the losing party pays the winner's legal costs. This prevents most applicants using this remedy, since they could not risk a bill of several thousand pounds should they lose. But in the Tribunal each party pays only its own costs.[18] It is clearly unfair that data controllers, who will usually be relatively wealthy, should enjoy a low cost appeal mechanism which is denied to the ordinary individual.

- This also distorts the checks and balances that should operate on the Information Commissioner. Because it is relatively easy for a data controller to challenge the Information Commissioner, rulings which favour the *applicant* are exposed to much greater judicial scrutiny, and risk of reversal, than rulings that favour of the data controller. In a finely balanced decision, the Commissioner will be at greater risk of legal challenge if he rules in favour of disclosure than if he rules against it. That is an unwelcome imbalance which may skew the appeals process against disclosure.

The best solution would to allow applicants the option of appealing to the Tribunal against the Commissioner's decisions, at least where subject access is involved. This would not involve removing any existing remedy in the courts, but would provide an alternative option for those who wanted it. This would be particularly helpful for unrepresented complainants, as the tribunal's specialist knowledge of the legislation will tend to compensate for any failure on their part to argue the case effectively. It would be particularly appropriate in cases where a single request for information involved both the FOIA and the DPA, where a common appeal mechanism, to the Tribunal, must be preferable.

Identity of third parties

In responding to a subject access request, information which identifies another individual can be withheld unless that individual consents, or disclosure without consent is "reasonable in all the circumstances."[19] The Act specifies four factors which must be taken into account in reaching this decision. We think the list of statutory factors should be amended to require data controllers to consider the *harm* that could result, either to

[18] Under the Tribunal rules, a party would only be liable for costs if its appeal had been "manifestly unreasonable" or it had behaved in a "frivolous, vexatious, improper or unreasonable" manner. The Data Protection Tribunal (Enforcement Appeals) Rules 2000, rule 25(1)

[19] Data Protection Act 1998, section 7(4)(b)

the data subject or to the other individual, from withholding or disclosing the information.

The four statutory factors which *must* be considered when deciding whether to release information which identifies someone else are: (a) whether a duty of confidentiality is owed to the other individual (b) any steps taken to seek the other individual's consent (c) whether the individual is capable of giving consent and (d) whether the other individual has expressly refused consent.[20] Because only these factors are given statutory weight, they may play a disproportionate role in determining whether disclosure is 'reasonable' in any particular case.

The four factors are presumably based on the ECHR judgment in the *Gaskin* case[21], but we question why all data controllers should *always* be obliged to consider *these* issues as opposed to potentially more relevant questions. Why, for example, is the other individual's capacity to give *informed consent* more important than the question of whether that individual is likely to be *harmed* by the disclosure?

The mandatory factors may also encourage data controllers to concentrate on the case *against* disclosure. A duty of confidentiality, or the express refusal of consent, will both encourage the *withholding* of information. Neither of these is conclusive - but there is no indication of what might be set against such considerations. It may be easy for data controllers to overlook any pro-disclosure circumstances, or give them little weight in the face of the statutory factors.

An important countervailing factor must be whether the withholding of this information would *harm the data subject*, for example, by denying him or her the opportunity to correct inaccurate information, answer damaging allegations or otherwise defend his or her interests. Data controllers are more likely to consider such important matters if the question of harm is specifically referred to in the Act.

Equally important is the question of whether disclosure would harm *the other individual*. The capacity in which the other individual is acting may be relevant to this question. A distinction should be made between those who are involved in their private capacity (e.g. a relative or neighbour of the data subject) and those acting *on behalf of* the data controller (eg a personnel manager recording information about an employee). In the latter case, the individual will presumably have little privacy interest and should normally be identified, subject to a test of harm (e.g. would disclosure expose them to risk of attack or of being victimised as a whistleblower).

---

[20] Data Protection Act 1998, section 7(6)

[21] *Gaskin v UK* 12 EHRR 36.

This would build on the precedent of the subject access orders. These do not permit the identities of health professionals, social workers, teachers and education authority staff to be withheld where they appear in the data subject's health, social work or education records respectively, unless disclosure would endanger their safety.[22] This approach should be extended.

Fees

There should be no increase in the subject access fee. On the contrary, we would prefer to see subject access being permitted free of charge, which would appear to be the more common approach elsewhere in Europe. This would recognise that it is in the data controller's own interests to ensure that its records are accurate, and that poor records are damaging to the work of organisation concerned and not just to the individual. Subject access should be seen as a means of improving accuracy, and promoting compliance with the data protection principles. Reducing the subject access fee would encourage this.

Although the fee a particular data controller can charge is now limited to £10, applicants may in practice have to make multiple applications and pay multiple fees as a result of data sharing. The cost of tracking down and correcting an error which has been shared between different public authorities or amongst commercial bodies may be prevent some individuals from exercising their rights under the Act altogether.

We are also concerned that individuals whose requests for information to public authorities involve both personal and official information may have to pay separate fees under *both* the Data Protection Act and the Freedom of Information Act. The fact that a requested document makes a passing reference to the applicant may be enough trigger a £10 subject access fee, although request is primarily an FOI request and involves too little work for any FOI fee to be charged.

Other points

Referring to some of the other questions raised in the consultation paper:

(1) We have no objection to data subjects being required to provide information to help data controllers identify the information they seek, provided a request can still be made *all* personal data held on the applicant.

(2) There should be no change in the basic rule that applicants should be entitled to a hard copy of any personal data held on them.

---

[22] The Data Protection (Subject Access Modification) (Health) Order 2000, Article 8; The Data Protection (Subject Access Modification) (Social Work) Order 2000, Article 7; The Data Protection (Subject Access Modification) (Education) Order 2000, Article 7.

(3) There should be no extension of the exemptions available to data controllers.

(4) We would prefer to see the 40 day time limit reduced to the FOI limit of 20 working days.

Yours sincerely,

Maurice Frankel
Director