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

Response to the Ministry of Justice's Call for Evidence on the Current Data Protection Legislative Framework

December 2010

INTRODUCTION

This submission deals with a number of issues relating to subject access, the individual's right to see his or her own personal data under section 7 of the Data Protection Act (DPA) 1998. It also deals with an apparent obstacle to the release under the Freedom of Information Act (FOIA) of anonymised statistics derived from personal data.

There are substantial discrepancies between subject access rights under the DPA and the rights of any member of the public to obtain official information under the FOIA. In some cases, people seeking their own personal information have substantially weaker rights to that information than they do when seeking other information under the FOIA. Since many requests to public authorities are 'mixed' requests, involving the applicant's personal data and other information, it makes sense for the two regimes to be as closely aligned as possible. In fact, mixed requests are dealt with under two diverging regimes, often to disadvantage of the subject access element.

The result may be that an individual whose rights to family and private life under Article 8 of the European Convention on Human Rights may be directly affected may in some respects have significantly weaker rights to information than an ordinary member of the public with no direct interest in the matter.

DISCREPENCES BETWEEN FOIA AND SUBJECT ACCESS RIGHTS

Public interest test

Most exemptions under the FOI Act are subject to a public interest test which requires exempt information to be disclosed unless the public interest in withholding the exempt information outweighs the public interest in its disclosure.[1] No equivalent test applies to DPA exemptions. This discrepancy can be found in relation to, amongst others, the exemptions for defence,[2] law enforcement,[3] regulatory functions,[4] national security,[5] health and safety,[6] honours,[7] the economy,[8] legal professional privilege,[9] information intended for future publication[10] and the effective conduct of public affairs.[11]

Thus, someone making a subject access request for information about their own dealings with a body may find that the information has been withheld under a DPA exemption regardless of any public interest in disclosure, however weighty. But similar information requested under the FOI Act may have to be disclosed on public interest grounds.

For example, the Information Commissioner has ruled on a request for access to a Prison Service manual setting out physical techniques of control used in dealing with young offenders. These included what was described as "the

---

[1] FOIA section 2(2)(b)
[2] FOIA section 26(1); DPA Schedule 7, paragraph 2
[3] FOIA section 31(1)(a), (b) and (d); DPA section 29(1)
[4] FOIA section 31(1)(g); DPA section 31
[5] FOIA section 24(1); DPA section 28(1)
[6] FOIA section 38(1) and Regulation 5(1) of The Data Protection (Subject Access Modification) (Health) Order 2000, Regulation 5(1) of The Data Protection (Subject Access Modification) (Social Work) Order 2000 and Regulation 5(1) of The Data Protection (Subject Access Modification) (Education) Order 2000
[7] FOIA section 37(1)(b); DPA Schedule 7, paragraph 3(b)
[8] FOIA section 29(1); and in relation to information process for corporate finance purposes DPA Schedule 7, paragraph 6(1)
[9] FOIA section 42(1); DPA Schedule 7, paragraph 10
[10] FOIA section 22(1); a more limited but potentially comparable provision in relation to examination marks is found in DPA Schedule 7, paragraph 8
[11] FOIA section 36(2)(c). More limited and specific provisions which might correspond to some of the circumstances in which s 36(2)(c) might be used can be found in DPA Schedule 7, paragraphs 5 and 7.

deliberate infliction of severe pain on children". The Youth Justice Board argued that disclosing this manual would allow detained young people to learn about and counteract the techniques and also lead to young people and staff being injured.

The Commissioner accepted that the information was exempt under two FOI exemptions, for information likely to prejudice the maintenance of security and good order in institutions of detention [12] and for information which could endanger the health and safety of individuals.[13] However, he found a significant public interest in disclosure, because of the deaths and injuries resulting from the use of such techniques; because of the lack of oversight and the significant moral and legal questions involved. Disclosure was ordered on public interest grounds, notwithstanding that two exemptions had been found to apply.[14]

That could not happen under an equivalent subject access request, for example by a young offender who had been injured by the abuse of these techniques. The individual's personal data might include the report of an investigation into the incident, perhaps revealing that the manual's safeguards had been ignored. This is likely be held to be exempt under the DPA on the grounds that disclosure would undermine the prevention or detection of crime by making it harder to prevent young offenders from assaulting staff. [15] The public interest case for disclosure would be irrelevant.

We think the public interest should be taken into account and that the DPA amended to require this.

No right to know when subject access exemptions have been used

Under the DPA, the individual making a subject access request has no right to know when information has been withheld. We think the FOIA approach should be adopted. Data controllers should be required to state whether information has been withheld and on what grounds, except where to do so would itself be damaging.

---

[12] FOIA section 31(1)(f)
[13] FOIA section 38(1)
[14] Information Commissioner, Decision Notice FS50173181, Youth Justice Board for England and Wales , 10 December 2009
[15] DPA section 29(1)(a)

At present, subject access requests may be responded to with a statement such as: "this is the personal data which we hold on you and are required to disclose". This deliberately obscures the question of whether other personal data is held but has not been disclosed. The Information Commissioner's guidance to data controllers encourages the use of such ambiguous statements:

> If all the information you hold about the requester is exempt, then you can reply stating that you do not hold any of their personal information that you are required to reveal.[16]

The result is to leave the requester uncertain as to whether no information is held or whether all information held is considered to be exempt. This may lead to unnecessary suspicion that information is being withheld, even when that is not the case.[17]

In this respect, the DPA falls significantly short of the FOIA, which generally requires that the requester be told when information has been withheld and under which exemption.[18] The FOIA does permit authorities to refuse to confirm or deny whether they hold information, but usually only where to give that confirmation or denial would itself be harmful.[19] The same approach should be required under the DPA.

---

[16] Data Protection Good Practice Note, Checklist for handling requests for personal information (subject access requests). Version 1.0, 09.01.07. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/checklist_for_handling_requests_for_personal_information.pdf

[17] Some years ago we took up this issue with Scotland Yard, which was responding to requests from people who wanted a copy of any criminal convictions against their name with the statement "*The Data Protection Act places an obligation on the Police when holding personal information on computer to provide a copy of that information (unless an exemption applies) to the individual concerned on request. From the personal details supplied in your request there is no information which the Chief Officer is required to supply under the provisions of the Act."* This led people to believe they were not permitted to see some conviction data recorded against their names. It naturally created suspicion that secret inaccurate information might be held. We understand that this practice was changed, following our representations. See: http://www.cfoi.org.uk/pdf/niscorrespondence.pdf

[18] FOIA section 17(1)

[19] Thus section 26(3) of FOIA permits an authority to refuse to confirm or deny whether it holds information if to do so would prejudice defence and if the public interest in refusing to do so outweighs the public interest in doing so (FOIA section 2(1)(b)).

Rights of appeal

Although the enforcement of both the DPA and FOIA involve the Information Commissioner's Office (ICO), the individual's appeal rights under the DPA are different from and significantly weaker than those under the FOIA.

(1) Notification of rights

The DPA does not require data controllers to inform requesters from whom information has been withheld of their appeal rights. This is expressly required under the FOIA[20] and should also be required under the DPA.

(2) Thoroughness of investigation

Most subject access complaints to the ICO are not fully investigated but dealt with by a less thorough process involving an assessment under section 42(1) of the DPA as to whether "it is likely or unlikely" that the Act has been complied with. Many of these are carried out purely on the basis of the information supplied by the complainant, without the ICO examining the disputed information. The outcome is likely to be a brief letter, whose findings are not legally binding.

When investigating an FOIA complaint the ICO nearly always examines the disputed information and requires the public authority to justify its handling of the request. Other than in certain circumstances, the requester is generally entitled to an enforceable decision notice[21] which sets out the ICO's detailed findings. The ICO has the powers to deal with subject access complaints in the same way,[22] but in most cases does not use them.

(3) Lack of access to Tribunal

Only the data controller, not the data subject, can appeal to the Tribunal. A data subject who is dissatisfied with the ICO's handling of their case can seek to enforce their rights in court[23] but cannot go to the Tribunal. But going to court

[20] FOIA section 17(1)
[21] FOIA section 50(2)
[22] Section 43 of the DPA allows the ICO to serve an Information Notice to obtain any information he reasonably requires from the data controller and section 40 allows the ICO to serve a legally binding enforcement notice on the data controller.
[23] DPA section 7(9)

involves the risk that they may have to pay costs if they lose – making such challenges rare.

By contrast, a data controller can appeal against an ICO enforcement notice to the Tribunal, where it normally only has to pay its own costs.[24] This highly asymmetrical arrangement clearly favours the data controller over the data subject. It contrasts with the FOIA arrangements, where either the requester or the public authority can appeal to the Tribunal against a decision notice.[25]

It has also lead to an imbalance in case law. There is now a substantial body of decisions, from the ICO, Tribunal and even courts, on the interpretation of the FOIA but very little such material on the DPA. This is dealt with further below.

Lack of transparency

The ICO receives far more subject access complaints than FOI complaints – yet publishes virtually nothing about how it deals with them. In 2009-2010, the ICO received over 9,300 complaints or requests for advice about subject access.[26] Yet no information about the outcome of these complaints is available. Neither the assessments themselves nor summaries of them are published, and there appear to be no statistics about the outcomes of subject access complaints. Occasionally an ICO annual report publishes a few lines on each of 2 or 3 cases but even this is not regularly done. The ICO does produce *guidance* on subject access. But the vast amount of *casework* takes place entirely in private and is not publicly accessible.

As a result, there is no public accountability for the substantial resources that the ICO devotes to this critical function. The quality of its work is shielded from public scrutiny, so there is no way of knowing how well complaints are dealt with. Finally, there is no opportunity for data subjects or data controllers to learn

[24] Costs would only be awarded if the Tribunal considered that a party had acted unreasonably in bringing, defending or conducting the proceedings. The Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009, rule 10(1)(b)
[25] FOIA section 57(1)
[26] The ICO states that 33,234 requests for advice and complaints relating to personal data were received and that subject access accounted for over 28% of complaints. (Annual Report for 2009-2010, pages 33 and 34)

from the vast quantity of past casework or to judge how specific issues which they may be facing have previously been dealt with.

The contrast with the position under the FOIA is remarkable. On average the ICO publishes at least a dozen detailed FOIA decisions a week, most running to over 20 A4 pages in length. Yet over the whole 23 year period during which subject access has been in force[27] it is doubtful whether the ICO has published the equivalent of more than a handful of A4 pages on its subject access casework.

This has practical consequences. The combined effect of ICO and Tribunal decisions means that there is now substantial clarity on questions such as when authorities must disclose the names of public officials under the FOIA.[28] There is virtually no comparable case law on most subject access issues.

For example, where an individual's data includes personal data about a third party, it must be released even if the third party has not consented if disclosure without consent "is reasonable in the circumstances".[29] The ICO has issued brief guidance on this topic, but has never published details of how it actually approaches the matter in practice – though it must have addressed the issue in hundreds of assessments. Most data controllers appear to ignore the requirement and withhold all third party personal data for which consent to disclose has not been given. The ICO's failure to document its decisions on the issue is likely to have contributed to the disregard of this provision.

[27] The right of subject access was originally established by the Data Protection Act 1984 and came into force in November 1987.
[28] Tribunal decisions specifically addressing this point include: EA/2007/0072, Department for Business, Enterprise and Regulatory Reform & Information Commissioner & Friends of the Earth; EA/2008/0065, Creekside Forum & Information Commissioner & Department for Culture, Media and Sport.
[29] DPA section 7(4)(b)

OTHER ISSUES

Disclosure of anonymised data

The Information Tribunal has ruled that statistics or other data derived from personal data remain personal data even if disclosed to the public in a fully anonymised form from which no individual can be identified.[30] If this ruling is upheld, it would have serious implications for the operation of the FOIA.

The ruling relates to the definition of "personal data" in section 1 of the DPA:

> "personal data" means 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

The Tribunal's view in this case was that, so long as the data controller retains information which allows it to identify the individuals to whom the statistics relate, the statistics remain personal data. The anonymised data cannot then be disclosed in response to an FOI request unless the disclosure complies with the data protection principles.

For ordinary personal data, this may not present an obstacle. If the data is so well anonymised that the public (including people who may be familiar with the individuals concerned) cannot identify them, disclosure is likely to fair and thus comply with the data protection principles.[31]

But where the anonymised data derives from sensitive personal data, the position is different. The DPA prohibits the release of such data unless a condition from Schedule 3 of the Act is satisfied.[32] In the case dealt with by the Tribunal, which involved abortion statistics, the Department of Health had a statutory duty to publish these statistics, thus satisfying a Schedule 3

---

[30] Information Tribunal, EA/2008/0074, Department of Health & The Information Commissioner & The Pro Life Alliance.
[31] Such a disclosure is likely to comply with the balancing test in paragraph 6 of Schedule 2 of the DPA, since the rights of the data subjects cannot be prejudiced by a disclosure from which they cannot be identified.
[32] DPA Schedule 1, paragraph 1(b)

condition.[33] Where no such duty exists, authorities which do not wish to disclose may argue that they have no Schedule 3 basis for doing so. This might, for example, affect FOIA requests for anonymised information about the types of injuries suffered by victims of road traffic accidents or by British troops serving in Afghanistan or for the amount of compensation paid to patients injured by medical negligence – all of which presumably involve statistics extracted from personal data about individuals' health.[34] Similar examples may involve statistics drawn from other kinds of sensitive personal data (eg numbers of staff dismissed after committing criminal offences).

The Tribunal's decision in the above case is currently under appeal to the High Court. However, given that the dispute involves the interpretation of an earlier House of Lords ruling,[35] the matter may not be resolved without further appeals, potentially extending over years.

We think the matter should be dealt with by an amendment to the DPA establishing that the disclosure, in response to an FOIA request, of fully anonymised data derived from personal data or sensitive personal data does not contravene the data protection principles. We believe this would be permitted by the Directive as it stands, particularly in light of Recital 72 which states that the Directive "allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive".

Schedule 3 conditions

Sensitive personal data can only be disclosed under the FOIA if a condition from Schedule 3 of the DPA is satisfied and the nature of these conditions means that in most cases this is not possible. We question whether such a rigid restriction is appropriate.

For example, the definition of "sensitive personal data" includes information about the commission of an offence by the data subject. Thus, although an

[33] Paragraph 7(1)(b) of Schedule 3 of the DPA.
[34] This information is derived from personal data about the health of individuals, and is sensitive personal data under section 2(e) of the DPA.
[35] Common Services Agency v Scottish Information Commissioner [2008] UKHL 47

individual may have been convicted of an offence, following the presentation of evidence in open court, an FOIA request for any details of that evidence is likely to be refused under section 40 of the Act. This may lead public authorities to refuse requests for details relating to the offence, even though they were given in evidence in open court during a prosecution which the requester would have been free to attend in person, during which he or she could have taken notes of the evidence. The information would also be exempt if the details had been reported by the media and could still be obtained from back copies of newspapers available online.

In one such case, the Information Commissioner commented on the anomaly which requires him to uphold an exemption for such information even though much of it is already in the public domain, and invited the Ministry of Justice "to address the problem, including the possibility of remedial legislation".[36] We believe such legislation should be introduced.

---

[36] Decision Notice FS50158274, Cabinet Office, 2 March 2009, paragraph 73.