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

David Smith
Deputy Commissioner
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

6 October 2011

Dear David

I have some serious concerns about the ICO's recently revised guidance "Access to Information Held in Complaints Files" (version 2, September 2011).

Whose personal data is it?

The guidance contains a section discussing when a person's opinion is the personal data of the person holding it, illustrated by a hypothetical probation officer's report on a client (on the 9th page). The first paragraph is correctly described as the client's personal data.

However, the second paragraph is described, without qualification and in its entirety, as the *probation officer's* personal data despite the fact that the key passage is quite obviously the *client's* personal data. The paragraph reads:

> "Given my 15 years' experience of dealing with clients like this, including my management of those on drug rehabilitation programmes, I am happy to conclude that my client no longer poses a threat to herself or to those around her and is unlikely to reoffend - provided access to the necessary support services is in place. My own approach is always to give clients the benefit of the doubt in cases like this, and usually this has worked out to the client's and the department's satisfaction." (*my underlining)*

The commentary continues:

> "This part of the report does tell us something about the probation officer himself – his professional approach and work-history. This part of the report is, therefore, the probation officer's own personal data."

This comment is addressed to the *whole* of the passage quoted above. The obvious, but wrong, implication is that the client has no right to see the passage that relates to her. Given the context (a discussion on how to treat opinions) the reader may assume that this is because the view is expressed as a professional opinion *("I am happy to conclude that...").* In fact, that is irrelevant, not least because the definition of "personal data" in section 1 of the DPA expressly states: *"personal data...includes an expression of opinion about the individual".*

The implication to those reading the guidance is that an individual's right to see their own personal data can be ignored, even when it is essential to their liberty, in order to protect what may be the relatively trivial privacy interest of the person recording the information. I am sure that this is not the ICO's actual position, but it is what this misleading passage appears to suggest.

Third party personal data

Another example refers to a hypothetical delivery man ("Mr Stevens") who refuses to take a washing machine into the customer's house via the back door, behaves in a threatening manner and then leaves the washing machine in the road. This account is later corroborated in a letter from a neighbour ("Mrs Oddman"). The guidance rightly says the neighbour's letter is her personal data and the personal data of the delivery man.

However, it continues:

> "Mrs Oddman's statement might have said that she hadn't seen anyone doing anything. In this case the information in the statement would be Mrs Oddman's personal data but not Mr Stevens' – even though it is held in a file about him."

I think that is questionable and potentially dangerous. If the witness had been in a position to observe an alleged incident but had observed nothing, it may mean that she had not paid attention. But it might just suggest that the incident did not occur. It could, for example, have been the result of a malicious complaint. If the neighbour says "I was there but saw no such incident" she may be saying by implication "the delivery man was not there at the relevant time". If that statement has been obtained in connection with a complaint against the delivery man and is held in his file it must be his personal data – and potentially available to him. To rule it out, as the guidance instructs, may be to withhold evidence that supports his case - the classic prelude to a miscarriage of justice.

The section 7(4) balancing test

On the following page, the guidance states that the neighbour's account confirming the delivery man's threatening behaviour is the delivery man's personal data but that "it would not be reasonable in the circumstances" to allow him to see it as:

> "given the nature of the incident, it is likely that the witness would expect her letter to be held in confidence by the supermarket. It would therefore be unfair to Mrs Oddman to disclose any of her letter to Mr Stevens."

I have concerns about this conclusion too.

The guidance is referring to section 7(4) of the DPA which requires the disclosure of personal information which also refers to another identifiable individual if (a) the other individual consents or (b) without consent, if such disclosure "is reasonable in all the circumstances".

The statutory criteria that come into play here under section 7(6) of the DPA require the data controller to take account of any "duty of confidentiality" owed to the third party. The data controller's *assumption* that the third party in the case study expected her report to held in confidence is not sufficient to establish a *duty* of confidence. In any event neither an expectation of confidentiality, nor an obligation of confidentiality, though extremely relevant, necessarily settles the matter. Section 27(5) of the DPA means that even a duty of confidence may not exclude the possibility of access.

The guidance makes no attempt to consider "all" the circumstances of the case. It makes an assumption about the third party's interests while entirely ignoring the data subject's interests. The delivery man could face dismissal for his conduct and might therefore need to know what he is alleged against him.

The data controller has received a complaint from the customer and corroboration from a neighbour. It could, as the guidance suggests, ask for her consent. But if it is refused, what happens? Would it be fair for it to take account of the corroboration but conceal its existence from the delivery man? Should the data controller consider whether it could be anonymised to prevent her identity being deduced? As the delivery man has already exhibited threatening behaviour, might there be a risk to anyone complaining about him? All these factors are relevant to whether disclosure is reasonable in "all the circumstances". The outcome might still be to withhold the information, but the question cannot be settled simply by considering the interests of only *one* of the parties.

The ICO's own "Guide to Data Protection" directly refers to the nature of this balancing test at paragraph 30:

> …although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights in respect of their own personal data. If the other person consents to you disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway. (my underlining)

The new guidance ignores this principle. (It deals with it only in the narrow context of cases where third party information has been supplied by the person making the subject access request, where there would be no point in withholding it anyway).

Where there is a potential conflict, the guidance suggests it should be resolved by asking for consent. It fails to acknowledge that section 7(4) expressly envisages the possibility of disclosure *without* consent.

In our experience, data controllers generally withhold *all* third party data from someone making a subject access request, without attempting to apply any balancing test. A data subject wishing to challenge this approach has to demonstrate, virtually from first principles, that the section 7(4) balancing exercise may require *their own interests* to be taken into account as well as those of the third party.

Section 7(4) was introduced as a result of the European Court of Human Rights 1989 decision against the UK in the Gaskin case. Graham Gaskin, who had been brought up in care, had applied for his social services records. He had been refused in every case where a contributor to, or a person mentioned in, the file withheld consent or could not be contacted. The European Court held that:

> the interests of the individual seeking access to records relating to his private and family life must be secured when a contributor to the records either is not available or improperly refuses consent. Such a system is only in conformity with the principle of proportionality if it provides that an independent authority finally decides whether access has to be granted in cases where a contributor fails to answer or withholds consent. (my underlining)

The essence of section 7(4) is surely that it provides a legal basis for addressing conflicting interests, which cannot be solved on the basis of consent. The guidance focuses on information held on *complaints* files, where such conflicts frequently occur. It is disappointing that the important possibility of disclosure without consent is not mentioned at all.

Yours sincerely

Maurice Frankel
Director