Information Commissioner's Office
Promoting public access to official information and protecting your personal information

Freedom of Information Act Awareness Guidance No 1

Personal Data

The Information Commissioner's Office (ICO) has produced this guidance as part of a series of good practice guidance designed to aid understanding and application of the Freedom of Information Act 2000. The aim is to introduce some of the key concepts in the Act and to suggest the approaches that may be taken in response to information requests.

The guidance will be developed over time in the light of practical experience.

Here we consider the exemption relating to personal information contained in personal data. The exemption is set out in section 40 of the Act.

A) WHAT DOES THE ACT SAY?

The exemption in Section 40 of the Act can be summarised as follows:

If the personal data is about the person requesting the information, then there is no right to know under the Freedom of Information Act. There is an absolute exemption to its release. However, any such requests should be treated as subject access requests under the Data Protection Act. This means that despite the exemption under the Freedom of Information Act, the applicant has a right to request his or her information under the Data Protection Act.

If the personal data is about someone other than the applicant, there is an exemption if disclosure would breach any of the Data Protection Principles. (This is the main issue explored in this guidance.) There are also some special rules to be applied in cases where the personal data are about someone who has formally objected to their disclosure. The term, "third party data," is used to describe personal information about someone other than the applicant.

Except in one very particular circumstance, referred to below, the exemption in section 40 is an absolute exemption.

B) WHAT IS PERSONAL DATA?

The term “personal data” is defined in the Data Protection Act, as amended by the Freedom of Information Act. “Personal data” is personal information about a living individual who can be identified. It may take any of the following forms:

- Computer input documents;
- Information processed by computer or other equipment (e.g. CCTV);
- Information in medical, social work, local authority housing or school pupil records;
- Information in refined structured manual records;
- Personal information held in any manual form by a public authority.

The last of these categories was introduced into the Data Protection Act by FOIA. For public authorities it means, in effect, that any information that relates to a living identifiable individual falls within the scope of the DPA regardless of how it is structured. However, in the case of this last type, which is sometimes referred to as category e data, there are some special rules designed to reduce the administrative burden which subject access requests are likely to place on authorities. These are explained in the next section. For private sector organisations, the definitions in the Data Protection Act do not include personal information held in unstructured filing systems.

C) SUBJECT ACCESS REQUESTS

Subject access requests must be made in writing. The definition includes requests made by email. There is no requirement to refer to the Data Protection Act and there will almost certainly be people who request information about themselves (i.e. personal data) while mistakenly citing the Freedom of Information Act. In any event, if the request is for personal data relating to the applicant, it should be treated as a request under the Data Protection Act.

If you calculate that you will be unable to respond within the 20 working day period provided by FOIA and that you may need the full 40 calendar day period allowed for under the Data Protection Act, you should let the applicant know.

Under FOIA, an applicant must simply state his or her name, provide an address for correspondence and describe the information requested. Only in exceptional circumstances will you be justified in seeking to verify the applicant’s identity - for instance if you suspect that a request is a vexatious one, submitted under an assumed name. Under the Data Protection Act, by contrast, you must avoid making disclosures of personal information which would breach the Act. In sensitive cases or where you suspect that the applicant is not who they claim to be, you will therefore need to check signatures or ask for proof of identity.

If you have doubt about the identity of the requestor you should treat the request as an application for third party personal data.

The usual subject access fee under the Data Protection Act is £10. Exceptions are a fee of up to £50 for medical records and a sliding scale for school pupil records. However, where the request includes unstructured personal information (category e personal data), the Freedom of Information Fees Regulations can be taken into account. These do not affect the fee that can be charged in most instances, but do place a limit on the amount of time an authority is required to spend in providing the information.

It is also worth remembering, particularly in the case of unstructured information, which may be hard to locate, that public authorities need not respond unless they are given any information which they reasonably need to find the information requested.

The Data Protection Act contains a number of exemptions from the right of subject access. These are explained in the "Data Protection Act 1998 Legal Guidance", also published by the Commissioner. The Commissioner has also published a large amount of information about subject access rights which is available from the data protection area of his web site or may be requested from the Information Line.

D) REQUESTS FOR THIRD PARTY PERSONAL DATA

Category e personal data is not subject to the majority of the data protection principles, but the exemption under section 40 allows them all to be considered when dealing with a request for information. Although releasing category e personal data would not in the majority of cases involve a breach of the data protection principles, we do strongly recommend, in considering requests for information containing personal data, that public authorities apply the protection principles to all personal data, including category e data.

The Data Protection Act contains 8 principles which, taken together, form the basic standard to which those processing personal data must operate. When an applicant asks for third party data, that request can only be refused if disclosure would breach any of the data protection principles.

The first principle requires personal data to be processed fairly and lawfully. In practice this will be the key issue when considering an application for third party data.

Disclosure would be unlawful if:

- There would be a breach of confidence. The duty of confidence is the subject of Awareness Guidance No 2**.** It is likely to arise where relatively sensitive information has been provided to an authority in the expectation that it would not be disclosed. Examples include medical information or personal financial details.
- There is law forbidding disclosure, for instance the Official Secrets Act.

The concept of “fairness” is harder to define, although in practice it ought not to be difficult to judge whether it would be unfair to someone to pass on their information without consent. The sorts of questions which should be asked include:

- Would the disclosure cause unnecessary or unjustified distress or damage to the person who the information is about?
- Would the third party expect that his or her information might be disclosed to others? Is disclosure incompatible with the purposes for which it was obtained?
- Had the person been led to believe that his or her information would be kept secret?
- Has the third party expressly refused consent to disclosure of the information?
- Does the legitimate interest of a member of the public seeking information about a public authority, including personal information, outweigh the rights, freedoms and legitimate interests of the data subject?

a) Private or Public Lives?

In thinking about fairness, it is likely to be helpful to ask whether the information relates to the private or public lives of the third party. Information which is about the home or family life of an individual, his or her personal finances, or consists of personal references, is likely to deserve protection. By contrast, information which is about someone acting in an official or work capacity should normally be provided on request unless there is some risk to the individual concerned.

While it is right to take into account any damage or distress that may be caused to a third party by the disclosure of personal information, the focus should be on damage or distress to an individual acting in a personal or private capacity. The exemption should not be used, for instance, as a means of sparing officials embarrassment over poor administrative decisions.

An issue which will often arise is whether the Data Protection Act prevents the disclosure of information about members of staff. Applying the criteria suggested above, if the information requested consists of job functions, grades or decisions which they have made in their official capacities, then disclosure would normally be made. On the other hand, information such as home addresses or internal disciplinary matters would not normally be disclosed. While it would be wrong to disclose bank account details of staff, it would be unlikely to be unfair to publish details of expenses incurred in the course of official business, information about pay bands, or, in the case of senior staff, details of salaries and other benefits. While this information clearly does relate to staff personally, there is a strong public interest in provision of information about how a public authority has spent public money.

These are not hard and fast rules. While names of officials in public facing roles would normally be provided on request, it may not be fair processing to provide the name of a member of staff in a junior role. There may also be good reason not to disclose the names of those in a public facing role if there is good reason to think that disclosure of that information could put someone at risk. It may be unfair processing to disclose the full names and work locations of those who carry out a role involving a risk of harassment or abuse. It may also be relevant to think about the seniority of staff generally: the more senior a person is the less likely it will be that to disclose information about him or her acting in an official capacity would be unfair.

b) Formal objections to disclosure

The Data Protection Act gives people the right to object in writing to the processing or disclosure of their personal data. Such written objections are often referred to as Section 10 Notices**.** An organisation receiving such a notice must comply unless there is some overriding justification for the processing. In some cases, although an organisation does not accept that there are valid grounds for objection, it may agree not to process or disclose data simply because those are the wishes of the person concerned.

If a request for the disclosure of information to which the third party has previously objected is received, the public authority must first consider whether releasing it would breach the data protection principles. If it is satisfied that the data protection principles apply and that the exemption is engaged, it then has to consider whether or not it is in the public interest to release the information. This is the only circumstance when requests that include personal data involve consideration of the public interest test.

E) PRACTICAL ISSUES

Many public authorities are used to dealing with subject access requests under the Data Protection Act and with the old definitions of personal data. Staff need to be aware of the fact the definitions have been broadened to include unstructured personal information.

It is a commonly held misconception that the Data Protection Act prevents the disclosure of any personal data without the consent of the person concerned. This is not true. The purpose of the Data Protection Act is to protect the private lives of individuals. Where information requested is about the people acting in a work or official capacity then there is less likelihood that the data protection principles would be breached.

You should develop a policy as to what information will be routinely disclosed about staff and what might be withheld. Your policy is likely to be more effective and you will avoid unnecessary alarm if this policy is developed in consultation with staff.

Public authorities hold a great deal of information about individuals with whom they have contact. They should consider making it known in what circumstances information about those individuals will be disclosed as a matter of course or in response to requests for information.

Further Information

If you need any more information about this or any other aspect of freedom of information, please contact us.

Phone: 08456 30 60 60
01625 54 57 45

E-mail: please use the online enquiry form on our website

Website: www.ico.gov.uk