

BRITISH AND IRISH OMBUDSMAN ASSOCIATION

DATA PROTECTION GUIDANCE

1 INTRODUCTION

This guidance has been developed by the British and Irish Ombudsman Association (BIOA) in conjunction with the Information Commissioner's Office (the ICO). Its purpose is to set out guidelines to assist BIOA members in complying with their obligations under the Data Protection Act 1998 (the 'DPA').

It is not the intention of this guidance to reiterate the law on data protection, but rather to focus on issues of relevance for BIOA members. The guidance also contains a section on the respective roles of members and the ICO when dealing with complaints from the public which include breaches of the DPA.

The guidance is not mandatory and does not impose any legal obligations upon members. It is intended as a code of good practice for members in the United Kingdom.

BIOA welcomes the purpose and driving principles of the DPA and encourages its members to approach the rights and obligations it introduces in a spirit of openness and transparency.

2 LEGISLATIVE OVERVIEW

2.1 Origins and Principles of the Data Protection Act

The DPA has two main principles. First, it imposes obligations on members, as 'data controllers', to process personal data in accordance with a set of principles (known as the Data Protection Principles).

Secondly, the DPA confers rights on individuals, including the right to request personal data held about them by an organisation. This is known as the right to make a 'subject access request'.

When interpreting the DPA it can be helpful to remember that its latest form originated from a European Directive. This Directive was brought about to regulate the use of information in the light of advances in computerised technology. The Directive was intended to ensure the protection of individuals' rights to privacy first by imposing restrictions on the way information could be processed but also by allowing an individual the right to access information held by another about them in order to verify its accuracy.

2.2 The Right to Privacy and Obligations of Confidentiality

The rights set out above – rights to privacy and to access personal information – inevitably conflict where a scheme holds personal information about a complainant provided by an organisation under investigation. This conflict will be considered in more detail, but privacy and confidentiality are key concepts when balancing conflicting rights under the DPA.

Article 8 of the European Convention on Human Rights (the Convention) provides that everyone has the right to respect for their private and family life, their home and correspondence. This right can be fettered only to the extent that to do so is in accordance with the law and is necessary in a democratic society. It is unlawful for a public body to act in a manner which is incompatible with the Convention.

The law of confidence protects the disclosure of ‘confidential’ information. This is information which is not already in the public domain and which has a degree of sensitivity and value. It must also have been communicated in circumstances giving rise to an obligation of confidence, either expressly or impliedly¹.

2.3 An Ombudsman’s Governing Legislation

The obligations and rights introduced by the DPA must be interpreted in accordance with the framework governing each member. In particular, many statutory members will have provisions under their governing legislation regulating the disclosure of information.

For example, public sector members have a statutory prohibition on disclosure of information other than for the purposes of an investigation and/or investigation report. Other members may have slightly different provisions requiring them to preserve the confidentiality of information. Although the DPA overrides any statutory bar on disclosure of information, it is important to identify these provisions and take them into account.

Some statutory members also have provisions for disclosure of information if it appears to relate to complaints lodged with ombudsmen under other jurisdictions. Other members contain provision for an authority to serve notice on an Ombudsman certifying that disclosure of specified information would be contrary to the public interest. Other members have legislation which expressly permits or requires the disclosure of information in certain circumstances.

¹ There is a useful and more detailed guidance on the law of confidence on the Information Commissioner’s website in a document entitled: ‘*Awareness Guidance No 2: Information Provided in Confidence*’. Although the document is prepared in relation to the exemption for confidential information under the Freedom of Information Act, the principles it sets out are relevant in this context.

The governing framework and its relationship with the legislation is the starting point for each member in any consideration of the issues raised in this guidance. Members should take their own legal advice on the relationship between their own governing framework and the obligations imposed on them by the DPA

2.4 Data Protection and Freedom of Information

Members should bear in mind the interrelationship between the DPA and the Freedom of Information Act 2000 (FOIA), which is expected to come into force on 1 January 2005.

Requests for information can be made under the DPA or FOIA. Applicants do not need to identify the correct Act to make a valid request.

The DPA entitles living individuals to access personal information about them. This right only applies to information about the individual – so a member of the public is entitled to request personal information about themselves under the DPA but not about someone else or about matters not related to them.

FOIA allows the public to request any recorded information, including information about others, held by a public sector body. However, because this is a much wider right, there are more wide ranging exemptions.

Public sector schemes in particular should be alert to mixed requests, where an applicant requests information concerning themselves and general policy, or other individuals. In this case, their request for information about themselves should be dealt with under the DPA and the remaining information will fall under FOIA. There are different procedures for each².

However, members should note that, if the DPA does apply (i.e. if information is 'personal data') but is withheld under one of the exemptions to the DPA then there is no need to consider whether it should be released under FOIA (as 'personal data' about the person requesting the information is exempt from FOIA).

3 KEY CONCEPTS UNDER THE DATA PROTECTION ACT

3.1 What is Personal Data?

Personal data are data that relate to a living individual who can be identified either from the data itself or together with other information in an organisation's possession. Details of the sorts of information this might include are at Appendix 1.

In order to fall within the definition of 'personal data' the information must also:

² For example, the time for dealing with an FOIA request is 20 working days, while the time for dealing with a DPA request is 40 days.

- either be held automatically or recorded with the intention that it will be held automatically;
- (until January 2005 for public sector bodies) be held in a 'relevant manual filing system' (considered at 3.2 below) or recorded with the intention that it should form part of a relevant filing system; or
- be held as part of a special category of records known as 'accessible' records (considered at 3.3 below).

3.2 What is a Relevant Manual Filing system?

This is any manual set of information relating to individuals which is structured in such a way that specific information is readily accessible. There must be a filing system which must have a sufficiently sophisticated means of indicating at the outset of a search whether, and where, specific criteria can be readily located.

As a general guide, a relevant filing system will apply where a reasonably competent temporary administrative assistant, with no in-depth knowledge of a scheme's work or filing systems, would be able to extract information about an individual from a file. It would not apply where that person would require particular knowledge of the scheme's filing systems.

In most cases, it is unlikely that an investigation file will have a sufficiently sophisticated indexing system to satisfy this requirement. Therefore, the information contained within (provided it is not also held on a computer system) is unlikely to be personal data.

However, public sector members should note that, as from 1 January 2005, there will be no requirement for manually held information to be in a relevant filing system. At that point, the only requirement for information to be 'personal data' will be that it has the necessary 'personal' quality. Information held manually by private sector members will still need to be in a relevant filing system to be personal data (unless it is part of an 'accessible record').

3.3 What are Accessible Records?

These are health records, educational records and other 'accessible public records'.

Unlike health and educational records, these other 'accessible public records' are records held by particular public bodies for certain purposes and they are no longer accessible records once they are passed to the scheme.

Accessible records do not need to be held in a 'relevant manual filing system' to amount to personal data, although they must still have the necessary 'personal' quality.

4 DATA PROTECTION PRINCIPLES AND RECORD MANAGEMENT

The Act imposes eight principles of good record management on members processing personal data:

4.1 Conditions and purposes for processing

Conditions for processing: The first principle requires all processing of personal data to satisfy one of a set of conditions³. The conditions that an organisation should meet in processing personal data will vary according to the nature of the data and the reason for processing it. For statutory members, the most relevant condition is where the processing is necessary⁴ for the exercise of a statutory function. This condition applies to the processing of both ordinary and sensitive personal data.

For non statutory members there is a similar provision authorising the processing of ordinary personal data where this is necessary for the exercise of any functions of a public nature exercised in the public interest. There is not, however, any equivalent provision authorising the processing of sensitive personal data.

However, members should note that additional conditions are set out in the “Processing of Sensitive Personal Data” statutory instrument⁵, which includes a condition for processing in “the substantial public interest” when this is necessary to discharge a function designed to protect the public against dishonesty, malpractice, serious impropriety or incompetence of any person, or mismanagement in the administration of, or failures in services provided by, any body or association. In either case, the condition would apply where the function needed to be carried out without explicit consent being sought so as not to prejudice the discharge of that function.

Where none of the set of conditions authorising the processing of personal data apply, it is likely that consent will be required. Where consent is required, it must be freely given and cannot be assumed or implied. This means that there must be a positive action (such as a tick in a box or a signature). Care should be taken to ensure that consent is given voluntarily and that the complainant is fully informed about the purpose for which the information will be used. This should help to avoid situations where a complainant later contends that he/she did not consent to the use of information in a particular way.

³ Listed in Schedules 2 and 3 of the DPA

⁴ Schedule 2 para. 5(b), Schedule 3 para. 7(b). The Department for Constitutional Affairs, in a document entitled Public Sector Data Sharing (November 2003), clarifies that ‘necessary’ in this context encompasses matters that are ‘reasonably required or legally ancillary’, and is not limited to matters which are ‘absolutely essential’ to the accomplishment of a purpose.

⁵ SI 417

Purposes for processing: The second principle requires that data is only processed for limited and specified purposes and that it should not be further processed for any other incompatible purpose.

4.2 The need to notify individuals of the purpose of any processing

The first principle's requirement that processing be fair requires that individuals are notified of the purpose(s) for which personal data about them is processed, as well as details of any persons to whom it will be disclosed. This means that not only complainants but also witnesses to an investigation must be notified, if personal information is gathered about them.

This may be done in a variety of ways, such as through a standard letter to individuals or by insertion of a paragraph in a leaflet advertising a scheme's services, provided the leaflet is distributed to the individual in question. Members should attempt to provide this information at the point when the information is being collected, or as close as possible to this time.

There are exemptions from the duty to notify which broadly mirror the exemptions to the subject access right. The most likely exemption will be if it can be demonstrated in any given case that notification is likely to prejudice the discharge of a statutory function. This exemption will not discharge the duty to notify in all cases – but it will be relevant in cases where there is a real risk that notification would prejudice the outcome of an investigation.

Names contained on a risk register will usually be personal data. Members that operate a risk register should have a policy governing the way this information is processed. Members should consider notifying individuals of the existence of the register and the criteria which will determine whether their details are recorded on it. Thought should be given to whether individuals should be notified that they are on the register, and the circumstances where a scheme might be able to rely on an exemption from the notification requirements.

4.3 Information Gathering

The third principle requires members only to obtain personal data which is relevant, and not hold on to information unnecessarily. Therefore, personal data should not be collected or retained if it has no relevance to an investigation.

It is important to ensure that complainants and witnesses are aware of the basis on which information is gathered. In particular, members should consider informing individuals that any personal information that they provide about others could be disclosed in response to a subject access request (unless the information can be withheld under any of the exemptions).

If any individual does raise any reason why any evidence should not be disclosed then this should be clearly documented.

4.4 Accuracy and Updating

The fourth principle requires data controllers to take reasonable steps to ensure the accuracy of information that it holds. This duty applies to facts, not opinions. Individuals have the right to apply to the Courts to have any inaccurate personal data about them corrected.

When a scheme agrees that information is inaccurate then it must correct it and inform the complainant that this has been done. Members should consider whether this affects the outcome of the investigation.

Members should also consider whether it is practicable to destroy the inaccurate information. Sometimes it is important for a scheme to retain information which was previously provided, even if this is subsequently claimed or found to be inaccurate. The Act provides that the fourth principle will not be contravened in such case, provided the (inaccurate) information was accurately recorded in the first place, that reasonable steps were taken to ensure the accuracy of the data and that a record has been made of the correction.

In many cases, a member will be provided with two versions of events and may not be in a position to determine which is accurate. In such case it is important to record any alleged inaccuracy. If possible, this should be done in such a way that any person reading the information is aware of the alleged correction.

Complaints about the accuracy of, for example, a clinical opinion cannot be determined by the scheme and, in addition to noting the alleged correction, the complainant should be informed that his/her recourse is through the courts.

4.5 Retention

The fifth principle requires a data controller to keep information only for as long as is necessary. Members should give thought to how long case files are needed once an investigation is completed and should devise a retention policy accordingly.

4.6 Subject Access

The sixth principle incorporates the right of individuals to make a subject access request. Guidance on how to deal with such requests is at 5 below. Some of the difficulties in responding to a subject access request can be eliminated by good record management during an investigation. In particular:

- Information Provided by Third Parties: Often, information is volunteered 'in confidence'. Whilst there may be genuine reasons for accepting the information on this basis, it does not automatically mean that it will be exempt from disclosure (although it will usually be possible to rely on an exemption if the information is genuinely confidential, as discussed in 2.2 above). It is important that the scheme understands why the information is said to be confidential, and that the provider

of the information understands a scheme's obligations in relation to any possible disclosure of this kind of information.

In some cases confidential information will be filed separately, or 'off file'. For the purposes of the Data Protection Act this will not avoid the need to disclose the information – exactly the same principles will apply.

- Recording Internal Information: Care should be taken in the way that information is recorded, particularly internal minutes and notes, which should be kept as factual as possible. Where possible, reference should be made to the complaint and not the complainant.
- Internal Advice: expert witnesses and internal advisers should be made aware that personal data contained in their reports and comments – including comments recorded in notes of telephone conversations – may need to be disclosed if a subject access request is made. Reports should be prepared on that basis. Investigators should be aware that personal data contained in their note of instruction may also need to be disclosed.
- Drafts: Personal data contained in a draft may need to be disclosed if it is not also contained in a final report. However, if the only changes between a draft and a final report are not personal data then there is usually no reason why the draft needs to be disclosed.
- WP: personal data includes information held electronically as well as manually and this can be overlooked when responding to a request. Therefore, members should set up a system for ensuring that all automated documents relating to a case can be easily accessed.

4.7 Security

The seventh principle imposes an obligation on employers and employees to keep personal data about others secure. Members that do not already do so should therefore take measures to ensure that information is kept secure. The seventh principle specifically states that these measures need not be merely technical, but can be organisational as well.

4.8 Transfers outside the EEA

The eighth principle prohibits the transfer of personal data outside the European Economic Area without first ensuring adequate protection of the data. This does not appear to have implications for ombudsmen's work although the ICO will give advice in any case where this might occur.

5 RESPONDING TO A SUBJECT ACCESS REQUEST

Individuals have the right to make a subject access request for information that constitutes their “personal data”. When a member receives such a request, there are a number of considerations that can affect their response:

5.1 Is information ‘personal data’?

Members should remember that not all information held in a complainant’s file will be ‘personal data’. The elements required to satisfy this definition are set out at 3.1 and Appendix 1. The decision of *Durant v FSA* has significantly narrowed the scope of information satisfying this definition. This is especially so for private sector schemes for whom, even after January 2005, any manual files holding information about a complaint must be a ‘relevant filing system’ in order for the information they contain to be personal data.

Inevitably, a scheme will obtain information about a complaint or complainant which does not satisfy the definition of ‘personal data’ under the Act.

Where this occurs there is no obligation to release the information. However, BIOA encourages members to deal with requests for information in as helpful a way as possible and suggests that the information should be released unless there is a valid reason for withholding the information.

Examples of what might amount to reasons for withholding information which is **not** personal data include:

- a) where the information is subject to a statutory bar on disclosure
- b) where the information was provided in confidence and disclosure may give rise to an action for breach of confidence
- c) where disclosure will breach an individual’s rights under, for example, Article 8 of the Convention
- d) where disclosure is likely to cause serious physical or mental harm to the individual or another
- e) where the disclosure concerns internal documents which, if disclosed, will lead to unnecessary argument as to the merits of a decision or process which would prejudice the complainant’s willingness to accept the conclusion of an investigation.
- f) An organisation has 40 calendar days in which to respond to a subject access request. Information that is personal data should be provided, unless a relevant exemption applies.

5.2 Exemptions to the right of subject access

The right of access to personal data is subject to a number of exemptions, and there are conflicting rights to be considered. The main ones for members are set out below.

5.2.1 Third Party Information (s.7)

A data controller need not provide information which relates to a third party unless:

- a) the third party has given his/her consent; or
- b) it is reasonable in all the circumstances to release the information without consent.

Personal data will relate to a third party if it identifies that party either directly or indirectly or where the third party can be identified as the source of a document. In this situation there could be a conflict between the applicant's rights to information and the third party's rights to privacy and confidentiality. Members will need to balance these conflicting rights.

If the third party is an organisation (as opposed to an individual) then there is no need to apply this balancing test. Often, however, a scheme will receive information provided by an organisation which contains information relating to an individual employee of that organisation. If this is the case, members will need to weigh the conflicting rights of that person and the applicant. A member may still seek the views of the organisation about the disclosure of the information, but ultimately they will be balancing the rights of the individuals concerned. The rights of the organisation as a whole are not relevant to s.7. However, they may be relevant under the s.31 exemption.

Where possible, members should anonymise third party information. See also the Commissioner's guidance entitled *Subject Access Rights and Third Party Information* for further guidance on how to apply the balancing test.

5.2.2 Negotiations (Sch 7, para 7)

Personal data does not need to be disclosed if it is contained within records of a scheme's intentions in relation to negotiations with the individual, where and to the extent that releasing this information would prejudice the negotiations.

For example, personal data could include a record of a potential compensation figure, and the premature release of this information could compromise the negotiations taking place. Personal data relating to other elements of the dispute could have a lesser impact on the negotiations. Schedule 7 Paragraph 7 would provide an exemption to the extent that disclosure would prejudice the negotiations. In this example that might mean that the compensation figure would not be disclosed, but other information, that was non-prejudicial, would be disclosed.

5.2.3 Health Information

Special rules apply to requests for the disclosure of information about the physical or mental health of an individual. This information must not be supplied without first contacting an 'appropriate health professional' for an opinion on whether disclosure would be likely to cause serious harm to the physical or mental condition of the individual or another, unless the individual has previously seen the information.

An 'appropriate health professional' is the health professional who is currently or was most recently responsible for the clinical care of the individual in connection with the requested health information.

An opinion on whether disclosure would harm the individual can only be relied on for six months, after which a further opinion must be obtained.

Care should be taken in relation to the disclosure of medical records of children or adults without capacity to handle their own affairs. Information should not be disclosed to others if it was initially provided in the expectation that it would remain confidential.

There is a similar partial exemption for education, adoption and/or social services information where disclosure would cause serious harm to the physical or mental health of the individual or another, or would reveal that the individual is at risk of child abuse.

5.2.4 Legal Privilege (schedule 7, para.10)

Information need not be supplied if a claim to legal professional privilege could be made in respect of the information in legal proceedings. This includes legal advice that is given where litigation is in process or is contemplated (for example, legal advice where a judicial review is threatened). It can also cover communications between an ombudsman and his/her legal advisor for the dominant purpose of seeking or giving legal advice. An example would be advice on whether a complaint comes within a scheme's statutory jurisdiction.

Members should note that legal professional privilege will not apply to information or comments provided by a legal advisor which are not for the purpose of legal advice, such as comments on policy matters or on the presentation of an investigation report (as opposed to advice on a legal issue relevant to the investigation). The question of when legal privilege applies is complex and members should consult their own legal advisors in relation to any legal advice on a file.

The ICO has produced a useful guidance note, 'Legal Professional Privilege' (Awareness Guidance No 4) which is available on its website. Again, although the guidance has been prepared in relation to the Freedom of Information Act, its summary and examples of what is privileged information are useful and relevant.

5.2.5 S.31 exemption : regulatory activities

Information is exempt from subject access **to the extent which**, in any case, disclosure would be likely to prejudice the proper discharge of certain designated regulatory activities. Before reviewing the application of this exemption to the activities of member schemes (see paragraph 5.2.5.1), it is helpful to examine two concepts which are relevant to the question of when prejudice is likely:

‘Likely to prejudice’: in order for prejudice to be ‘likely’, there must be a real risk that it will occur. This does not, however, mean that the prejudice needs to be more probable than not.

‘In any case’: although it may be possible to make some generalisations, and to establish presumptive policies on that basis, this phrase requires consideration of the likelihood of prejudice in relation to each individual case. The exemption is not intended for blanket application to any category of information. A member could be processing personal data and might, by dint of their regulatory framework, be able to rely on the exemption at section 31. However, the prejudice test would need to be applied in relation to each piece of personal data. The exemption cannot be used as a basis for withholding all of the personal data on a file without this process of consideration.

Depending on the nature of the processing, it is possible that disclosure of some personal data will be prejudicial to a member scheme’s function, but the remainder will not. The remainder will therefore need to be provided, unless any other exemption applies.

Some possible examples of where the exemption might apply in the context of member schemes’ work are:

- a) Requests made by the complainant during the process of an investigation where negotiations for local resolution are underway and where the disclosure of data is likely to prejudice the successful outcome of such negotiations.⁶ This might exempt, for example, comments about the complainant made by the body under investigation where the investigator considers that the disclosure of such comments risks making the complaint less open to resolution.
- b) Requests made during the process of an investigation where the disclosure of data would be likely to prejudice the successful completion of an investigation. Members would need to demonstrate that the disclosure of information would be likely to undermine the confidence of any of the parties and make them unwilling to co-operate during the remainder of the investigation. This would particularly apply to information provided by a third party where that party, for legitimate

⁶ Please also see 5.2.4 (negotiations exemption) above. Some (although not all) personal data in this scenario may also be exempt under Schedule 7 paragraph 7.

reason, objects to its release and where further information is needed from the party in question. An example might be where the information is likely to be used against the third party in related legal proceedings or where disclosure is likely to result in physical harm or other detriment to the third party.

- c) Requests for personal data where the time and effort involved in responding would divert resources from the investigative function and so prejudice the Ombudsman's ability to conduct a proper investigation. This would involve an analysis of time and resources. This argument might particularly apply to cases where the individual is a persistent complainant or where he/she is already in possession of much of the information requested (such as letters to and from the individual).
- d) Certain categories of data which are provided in confidence. Data will not be exempt simply by virtue of the fact that they are expressed to be provided 'in confidence', particularly if there is nothing confidential or sensitive about them. However, an expression of confidence will be a strong indicator that s.31 might apply, particularly in the following situations :
 - where personal data is provided in confidence by an organisation under investigation to an investigator who regularly investigates that particular organisation. In such case, the investigator would need to demonstrate that disclosure would undermine the relationship between the parties and so prejudice the willingness of the organisation to provide information relevant to that, or future, investigations;
 - where personal data is provided in confidence and disclosure is likely to result in physical harm or other detriment to another party; or
 - where personal data is provided by a party under investigation and is likely to be used against that party, for example in future litigation.
- e) Information contained in violence warning markers or risk registers to the effect that a complainant is potentially violent.
- f) Personal data contained in internal memoranda and notes of internal deliberations, if it could be established that disclosure is likely to prejudice the investigative function by, for example:
 - inhibiting the necessary expression of opinion (for example, during the conduct of an investigation); or
 - resulting in unnecessary argument as to the accuracy of such memoranda and/or opinions expressed therein.
 - An example might be a note of a case conference, attended by investigators and experts, where differing opinions are put forward as to the strength of a

case, if it can be shown that the disclosure of personal data would be likely to create unnecessary arguments about the merits of the discussion and thereby prejudice the complainant's satisfaction with the outcome of the investigation.

- Another example might be personal data contained in legal advice which does not qualify for legal privilege, if it can be shown that its disclosure would again lead to argument over the merits of the case and prejudice the complainant's willingness to accept the conclusion of an investigation.

In each situation a member must be able to demonstrate the prejudice to their regulatory function.

5.2.5.1 The Application of section 31

BIOA members provided submissions describing their processing in the course of producing this guidance to assist consideration of the application of section 31. The range of activities and processing present within the BIOA membership precludes the ICO giving any blanket statement as to the use of the s.31 exemption.

In order to determine whether a member scheme's activities could fall within the exemption, it is helpful to break down the wording of the section. Subsections 4 and 5 of section 31 are limited and relatively specific. For example, sub-section 4 restricts itself to functions designed to give protection to the public from maladministration and failures by public bodies, and conferred by enactment on the Parliamentary Ombudsman and other specified schemes. Sub-section 4A applies specifically to the Financial Ombudsman Service. Sub-section 5 relates to the discharge of functions conferred on the Office of Fair Trading to protect the public, to prevent distortion of competition, or to prevent abuse of a dominant market position.

For those members not falling within any of the above, sub-section 2 of the section has a more general scope and, in broad terms, applies to information processed by a body if;

- its functions are statutory, governmental by nature or are of a public nature and exercised in the public interest; and
- those functions are designed for specific regulatory purposes. These include:
 - protecting members of the public against financial loss caused by dishonesty, malpractice, impropriety or incompetence etc on the part of financial institutions or limited companies;
 - protecting the public from financial loss caused by the conduct of bankrupt individuals;
 - ensuring the good administration of charities;

- securing health & safety in the work-place

In addition, where none of the above apply, section 31(2)(a)(iii) has a wider residual ambit – applying to functions designed to protect the public against dishonesty, malpractice, impropriety or incompetence of “persons authorised to carry on any profession or other activity”.

These provisions are wide and are likely to be applicable to many, perhaps all, of the case-work activities of members. Members should be aware, however, that a literal interpretation of section 31 could raise two types of question. First, have the member scheme’s dispute-resolution functions, which focus on service and similar failures, been designed to protect against “dishonesty, malpractice or other seriously improper conduct...or unfitness or incompetence”? Secondly (where s31(2)(a)(iii) is in issue) have individuals falling within the jurisdiction of a scheme been “authorised” to carry on their profession or other activity?

The answers to these questions may mean that some members would not be able to take advantage of section 31 on a literal interpretation of its wording - whether in relation to the data they are processing in specific cases, or in their processing at all. However, bearing in mind the EU origins of the Act and the need to adopt a purposive approach to its interpretation, the Commissioner is minded to take a broad approach as to the range of bodies which may seek to rely on the provisions of section 31. He would not ordinarily anticipate taking enforcement action against a BIOA member on this issue – provided that they have been approved for membership of BIOA in line with the Association’s criteria and can demonstrate that their activities are broadly “regulatory” by nature. Members will still need to demonstrate the likelihood of prejudice on a case by case basis.

Members should, however, note that the exercise of enforcement discretion on the part of the Commissioner would not stop an individual bringing these issues to the courts and it is possible that a court would support a strict interpretation of these provisions.

Members may wish to undertake their own risk assessment of their approach to all aspects of section 31.

5.2.6 Other exemptions include:

Personal data processed for the purpose of preventing or detecting crime, or the assessment of any tax or duty of a similar nature (s.29).

Personal data processed only for research purposes, provided that is the sole purpose and the data are not used to support any other measures or decisions (s.33).

6 HYBRID COMPLAINTS

Details of how to deal with hybrid complaints (complaints which straddle the jurisdictions of a member scheme and the ICO) are set out in Appendix II.

16 November 2004

Appendix I : Personal Data

When is data 'personal' data?

Personal data are data relating to a living individual who can be identified from the data. When deciding whether information 'relates to' an individual it is helpful, in cases where it is not obvious, to consider whether the information affects the individual in either a personal or professional capacity. This might be because the information is either:

- a) biographical in a significant sense; or
- b) has the individual (as opposed to some other person or event) as its focus.

Any expression of opinion about the individual or any indication of the intentions of any person in respect of the individual will be personal data.

Is a person's name on a document 'personal data'?

Not necessarily. It is more likely that an individual's name will be 'personal data' where the name appears together with other information about the individual such as his or her address or telephone number.

What sorts of information are likely to be 'personal data'?

Provided the information in question can be linked to an identifiable individual, the following **are** likely to be examples of personal data:

- An individual's salary or other financial information (including information about a person's bank statements, tax liabilities and spending preferences).
- Information about an individual's family life or personal circumstances.
- Information about an individual's employment or profession.
- Any opinion about an individual (as opposed to an opinion about a complaint) or his or her state of mind.

There is also a special category of information called 'sensitive personal data'. This includes information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, membership of a trade union, physical or mental health, sexual life or details about the commission (or alleged commission) of any offence. Special conditions apply to authorise the processing of any sensitive personal data. These are considered in more detail at 4.1.

Often, whether or not information is 'personal data' will depend on the nature of the complaint. For example, a complaint about care provided by a hospital will usually involve information about a person's health and this information will be personal data.

On the other hand, a complaint about a delay or failure to follow a certain procedure will mean that the focus of the investigation is on process – i.e. the process followed by an organisation.

Members should note that information about *a process itself* is not personal data to the complainant. Information about the *effect of the process* on the complainant (for example, any physical, personal or financial repercussions) is likely to be personal data.

Of particular relevance to this issue is the recent case law “Durant vs. FSA”, in which a complainant was seeking to obtain records regarding a complaint that had been referred to the FSA. The judges in this case concluded that information regarding the complaint was not by definition personal data of the complainant, and that personal data should be more closely related to the individual concerned.

What sorts of information are *not* likely to be ‘personal data’?

The following are examples of information which *will not* normally be personal data:

- Mere reference to a person’s name, where the name is not associated with any other personal information;
- Incidental mention in the minutes of a business meeting of an individual’s attendance at that meeting.
- Where an individual’s name appears on a document or e-mail indicating only that it has been sent or copied to that particular individual, the content of that document or e-mail does not amount to personal data about the individual unless there is other information about the individual within it;
- A factual analysis of a complaint (unless that analysis contains personal information such as health or financial information);
- Comments from the investigating team about the nature of a complaint or the manner in which the complaint is being/should be dealt with;
- Information relating to any of the investigating team, including names and any comments on the way an investigator is handling a complaint (although this may well be personal data relating to the investigator in question).

What about a note of a conversation with a complainant about a case?

A note recording personal or professional information about the complainant will be personal data. However, a note of a conversation about the progress or handling of a complaint is unlikely to be personal data.

What about a document which mentions the complainant?

Only information which relates to the complainant in his personal or professional life, or which focuses on the complainant or is biographical in a significant sense is personal data. If the document mentions the complainant in the context of focusing on another issue it will not be personal data.

If the document comments on allegations made by the complainant about the way an organisation has conducted itself (i.e. an explanation of the reason for taking a particular course of action) this will only be personal data if the explanation relates in some particular, individual sense to the complainant. An outline of an organisation’s standard procedure would not be personal data.

Appendix II: Hybrid Complaints

1 What is a 'hybrid' complaint?

A hybrid complaint is one which raises issues which straddle the jurisdictions of a member scheme and the ICO.

For example, a scheme might receive a complaint which includes an alleged failure to provide information as part of a wider complaint. Similarly, the ICO might receive a complaint about failure to provide access to information which includes elements of maladministration.

Often, it is difficult to judge how best to deal with these complaints. The following principles are suggestions only. Each case will vary according to the particular circumstances.

2 Basic principles

Members should aim to resolve complaints fairly and efficiently, without passing them needlessly between different bodies.

However, the data protection legislation can be complex and it is not the function of each scheme to give data protection assessments. Members should therefore feel able to consult or refer complaints to the ICO where appropriate.

3 Complaints received by members

Complaints **solely** about breaches of the Data Protection Act should be handled by the ICO. Members should explain this to the complainant and provide assistance to the complainant in passing the complaint to the ICO. This may mean referring the complaint to the ICO on the complainant's behalf, if the complainant consents or, if more appropriate, providing the ICO's contact details for the complainant to contact the ICO directly.

Hybrid complaints are more complex. Some members do not have the jurisdiction to consider data protection issues. If this is the case, the scheme should explain this to the complainant and, as above, should assist the complainant in forwarding the data protection aspect of the complaint to the ICO. Other members have jurisdictions which allow them to consider data protection issues. In such case, if complaint includes a simple data protection issue (such as a complaint about a delay in providing personal data), the data protection aspect can often be dealt with by the scheme along with the wider complaint. However, the scheme should usually liaise with the ICO's staff to ensure that this is the most appropriate course and that the complaint does not involve any complex matter that the ICO should handle. Members should liaise with the ICO Compliance department. In this case, the complainant should be notified that he/she will have the right to refer the matter to the ICO if he/she is dissatisfied with this particular aspect of his/her complaint.

If a complaint includes complex matters of data protection law (for example, where a body is citing the application of an exemption), in addition to other aspects which are clearly within the scheme's jurisdiction, then the data protection aspect of the complaint would usually be dealt with separately by the Information Commissioner's Office. Members should provide as much assistance as possible to the complainant in passing the complaint to the ICO. Again, if the complainant consents, this may mean referring the matter to the ICO on behalf of the complainant. It would then be for the complainant to pursue the matter with the ICO directly.

In all cases, complainants should be notified of the ICO's contact details.

The complainant ultimately has the right to complain to the Parliamentary Ombudsman in relation to any alleged maladministration on the part of the ICO.

4 Complaints received by the Information Commissioner's Office

Complaints clearly within the Commissioner's jurisdiction which involve no other issues will be dealt with by the ICO.

Hybrid complaints will normally be dealt with on the same principles as above, namely that the ICO will deal with the data protection aspects and the scheme will deal with the maladministration complaints. The ICO should either advise the complainant to raise the complaint of maladministration with the relevant scheme (to be dealt with separately) or refer the complaint directly to the scheme (provided consent has been obtained).

5 Liaison

There will inevitably be cases which are not clear cut. In cases of doubt, discussions between the scheme and the ICO should take place to decide the best way of handling the particular case.