Subject Access Requests under the Data Protection Act 1998

**Purpose:** To guide all barristers and chambers’ data controllers on Subject Access Requests under the Data Protections Acts

**Scope of application:** All practising barristers and chambers’ data controllers

**Issued by:** The Information Technology Panel

**Last reviewed:** November 2016

**Why is this relevant to me?**

All barristers in self-employed practice who use a computer for their work are highly likely to be data controllers. This is because the information which is stored on your computer in the course of your work is likely to contain information about individuals (e.g. witness statements, expert reports, emails) and you control what you do with that information. Even if you ask your clerks to keep and maintain records of individual solicitors (rather than firms) who have instructed you, on a computer owned by your chambers, you are likely to be a data controller in respect of this data.

Where the information is **only** kept on paper records, this can still be ‘data’ if it is in a ‘relevant filing system’. This is not the place for a detailed discussion of this thorny issue, on which the ICO has provided some guidance. In broad terms, a filing system will be a ‘relevant filing system’ if it is structured by reference to individuals or criteria relating to individuals and sufficiently structured or indexed that it is possible to discover whether and where personal information is being held in the system, without having to search through the files to find it.

As a data controller you have an obligation to notify your processing with the Information Commissioner’s Office. This involves completing some forms, which can be done online, on the telephone or by requesting the forms and filling them in) and paying the annual fee. The notification fee, unless you are a very large business (250 or more members of staff) with a large turnover (in excess of £25.9 million per annum), is £35.

If you have already notified your processing to the Information Commissioner you will have already made the decision that you are a data controller. There are a limited number of exemptions from notification, but usually, because of the nature of the processing being carried out, in practice, notification is required for self-employed barristers and for chambers.

---

1 Durant v FSA [2003] EWCA Civ 1746
It is better to assume that you are not exempt than to fail to notify, because to carry on non-exempt processing without notification is a criminal offence.

If you undertake judicial work, it is no longer necessary to notify in respect of processing carried on for the purpose of exercising judicial functions.

For more information on notification, please refer to the separate guidance on notification.

**What is a subject access request (SAR)?**

A subject access request is a request from or on behalf of an individual (not a company) which seeks to discover whether you are processing the personal data of that individual (a data subject) and if so, to provide a copy of the information. Requests are often made informally so it is important to be able to recognise a subject access request as such when a request for information is made.

**How do I tell if I have received a SAR?**

There is no statutory form for the request. It is therefore important to be aware that a request may not make any reference to the Act or explicitly identify itself as a SAR. However, the inclusion of the fee is usually a good indication, but it is important to be alert to an initial request which may be followed by payment of the fee. You should also ensure that your staff are trained so that they can recognise a SAR when they receive one and know what to do. If an individual simply makes a request for specific information relating to that individual then, subject to any obligations of confidentiality or privilege, you may decide simply to provide the information, without treating the matter as a subject access request.

**What if the SAR comes from a minor?**

The guidance provided by the Information Commissioner's Office suggests that the question of legal competence must be addressed on a case by case basis, but that minors over the age of 12 may be considered sufficiently mature to make a SAR. If you know the individual as part of your work, then you have to make a judgment as to whether they are mature enough to understand the nature and consequences of what they are asking (Gillick competence). If an adult seeks the information on behalf of the minor, then you will still need to confirm that the request is made with the child’s consent, unless they are too young to provide genuine consent. This can be particularly important in cases where there is a dispute which has caused a rift in the parental relationship.

**What do I do if I receive a SAR?**

The first thing to do is to acknowledge receipt of the request and ensure that it complies with the statutory requirements. There is no obligation to respond to a subject access request which is not made in writing (note that writing will include emails). However, it is sensible to inform the person of this requirement if a request is made orally.

You can choose whether to charge a fee. If you do, you should make it clear as early as possible after receiving the request that a fee is payable. If you do charge a fee then there is no need to

---

2 Data Protection (Notification and Notification Fees) (Amendment) Regulations 2009/1677, reg. 2
respond to the request unless and until the fee is paid. The statutory maximum for the fee is £10.

If, on considering the SAR, you reasonably require further information as to the identity of the data subject or to locate the information sought, you should inform the data subject, as soon as possible after receiving the request. Until you receive the further information you do not have to comply with the request³. However, it may be sensible to start considering what actions would be required for the collation of the information you need to respond to the request at this stage, if that is possible. If you know that the data subject is not legally competent, e.g. a person who is the subject of a mental health order or a minor, ensure that the request is made with the authority of the person who has conduct of their affairs.

If the SAR is not the first request you have received from this individual and complied with, you will have to consider whether the requests are identical or similar and whether a reasonable interval has elapsed between the requests. This is because there is no obligation to comply with repeated requests for the same or similar requests made at unreasonably close intervals⁴. In assessing whether the interval is reasonable you should consider the nature of the data, the purpose for which they are processed and the frequency with which the data are altered. For example, if the information is archived, historical data that has not been added to or changed since compliance with the previous request, this would suggest that there is no need to respond again. Nonetheless, it would be sensible to confirm that that is the situation.

How long do I have to respond?

You must comply with the request promptly and, in any event, within 40 days from the date on which the request is received, with the following exceptions. Where you need further information from the individual to satisfy yourself as to their identity and to locate information about them, and you have informed the person of this, the 40 day period starts to run from the time the requested information is provided. Similarly the period does not start until any fee is received⁵.

How do I comply?

You must tell the data subject whether you are processing any of their personal data.⁶ This requires a consideration of the information that is being processed.

If you are not processing any information about the data subject, you can answer the request in the negative and you will have complied with the DPA. However, you should note that processing is a broad term, and includes storing the information. It also includes obtaining information which it is intended will be stored as personal data.

If you are processing such data you have to:

1) Confirm that processing is being carried out.

³ S7(3) DPA  
⁴ 8(3) and (4) DPA  
⁵ S. 7(8) DPA  
⁶ S.7(1)(a) DPA
2) Provide a description of the data.
3) Indicate the purpose(s) for which such processing is being performed.
4) Indicate any Recipients or classes of Recipients (actual or intended) of the data.
5) Provide a copy of the information constituting the data in intelligible form. It must be supplied in permanent form unless this is not possible or would involve disproportionate effort.
6) Provide any available information about the source of the data. However, this may be subject to qualifications if it involves disclosure of personal data of a third party (see below).

The obligation under (1) and (2) will be met by providing the data. Note that the requirement is not for disclosure under the CPR. The obligation is to provide the information, not documents containing the information. Provided that you have accurately completed your Notification, (3) can be met by providing a description of the purposes akin to that included in your notification.

‘Recipients’ includes any legal person to whom the data are disclosed, and includes those processing data on your behalf (e.g. your clerks and administrative staff), but not those to whom it is disclosed if in response to an inquiry made in exercise of power conferred by law. However, as this involves the potential disclosure of personal data of third party individuals, it is subject to the considerations set out below. This potential problem can be avoided if you can describe the class of Recipients, for example, "staff".

The SAR relates to processing being carried out at the date when the request is received, so that data added after the date of the request does not have to be provided. However, if the information would be amended or deleted in the normal course and regardless of the receipt of the request, you do not have to provide it in the amended form or if it has been deleted. For example, if your normal data retention policy is such that data is deleted 39 days after receipt or creation, you do not have to supply such data. This assumes, of course, that you have a data retention policy!

When considering whether you are processing and what you have to disclose the following issues should be addressed:

1) What information about the person do I have?
2) Is it processed or intended to be processed automatically and therefore data?
3) If not, is it held in a relevant filing system and therefore data?
4) Is it personal data?
5) Is it exempted from compliance?
6) Does it include personal data relating to third party individuals?
7) What form does my response have to take?
8) What happens if the data subject is not happy with my response?

1) **What information about the person do I have?**

---

7 S. 70(1) DPA
8 S. 8(6) DPA
This question involves consideration, investigation and identification of the information which you have and which is being processed on your behalf by others. You need to identify this information in order to assess whether it constitutes personal data. At this stage you should not exclude from further consideration any information about the data subject which you have. If the information is not data or is not personal, this will become clear in the following steps.

2) **Is it processed or intended to be processed automatically and therefore data?**

Is the information identified above is held (or is to be recorded) on computer or on DVD/CD-ROM or some other computer-readable means, such as USB sticks etc? If so, it will be **data**. If, however, it was held on computer in the past, was printed out and is no longer held by you or on your behalf on computer or computer-readable media, it will not necessarily be data. Manually organised files are considered below.

3) **Is the information held in a relevant filing system?**

4) Even if the information is not processed automatically and is held on manual files it may still be **data**. If it is held in a “relevant filing system” as defined in the DPA it will be **data**. The Court of Appeal has considered this definition and concluded that information stored only on manual files which are not indexed in such a way that the information can be searched in a way equivalent to an automated search will not normally be covered.

5) **Is it personal data?**

Even if the information is ‘data’ within the DPA, it is not necessarily "personal data". In order to be personal data the information must be data which relates to an individual from which they can be identified or which together with other information in your possession would enable such identification.

In **Durant v FSA** the Court of Appeal held that this definition should be construed narrowly, and that it is likely in most cases that only information that names or directly refers to the data subject will qualify. This means that not every reference to the data subject will be personal data; the information must affect the privacy of the data subject in their personal or family life, their business or professional capacity. However, this is a narrow exception and taking too broad an interpretation of the Durant test is not favoured by the Information Commissioner’s Office (ICO).

If the information is biographical in a significant sense, that is, going beyond the recording of the data subject’s involvement in a matter or an event that has no personal connotations or if the information has the data subject as its focus rather than some other person with whom he may have been involved this will probably be personal data. If you are in doubt as to whether the information constitutes personal data, you should take professional advice. The ICO has also provided guidance on this issue.

---

9 S. 1(1) DPA
10 S. 1(12) DPA
11 Durant v FSA [2003] EWCA Civ 1746, ¶50
6) **Is the data nevertheless exempted from compliance?**

There are certain circumstances in which compliance may be limited or excused. Many of the following categories of exemptions will not apply, but in each case you will have to consider whether the provision of data would compromise any of these activities for you or your clients:

a) National security - if the exemption is required for the purpose of safeguarding national security. In this context "required" is to be interpreted consistently with the European principle of proportionality.

b) Prevention and detection of crime, apprehension and prosecution of offenders, assessment or collection of tax or duty or imposition of similar nature, only to the extent that it is likely to prejudice such matters.

c) Regulatory activity (e.g. for protecting the public from financial loss from misconduct or negligence in financial services e.g. banking and insurance, from the conduct of bankrupts or from misconduct in other professions and includes an exemption for personal data processed for the purposes of discharging any function of the Legal Services Board), but **only to the extent that** compliance would be likely to prejudice the proper function of such activity.

d) Data processed only for journalistic, artistic or literary purposes, but only if compliance is incompatible with those purposes.

e) Data processed only for statistical or historical purposes, but only under certain conditions.\(^{12}\)

f) Data which the data controller is required to make public by law.

g) References given in confidence by you for the education, training or employment of the data subject.

h) Where disclosure of the personal data would be likely to prejudice the combat effectiveness of the armed forces.

i) Personal data processed for assessing a person's suitability for judicial office or for appointment as a QC or the conferment of an honour by the Crown.

j) Personal data processed for the purpose of management forecasting or planning for a business or other activity only to the extent that such compliance would prejudice the conduct of the business or other activity.

k) Personal data processed for corporate financial services only to the extent that compliance could or it is believed that it could affect the price of an instrument which exists or may be created or if it exemption is required to protect an important economic or financial interest in the UK.

---

\(^{12}\) S.33 DPA
l) Records of your intentions relation to any negotiations with the individual are exempt to the extent that compliance would prejudice such negotiations

m) Personal data consisting of information recorded by candidates during an examination are exempt from the SAR

n) Legal professional privilege - to the extent that a claim to such privilege could be maintained in legal proceedings

o) Self-incrimination - you need not comply with the request to the extent that such disclosure would reveal evidence of an offence (other than under the DPA) and thereby expose you to proceedings for that offence

p) Personal data which is processed for the purposes of assessing any person’s suitability for the offices listed in the schedule to The Data Protection (Crown Appointments) Order 2000 (SI 2000/416) is exempted from compliance with the SAR.

q) Personal data processed only for the purposes of your personal family or household affairs are exempt from compliance with the SAR.

r) Health, education and social services records (see below)

s) Personal data the disclosure of which is restricted by specific enactments are exempted from compliance with the SAR\(^\text{13}\)

t) If the exemption is required for the purpose of avoiding an infringement of the privileges of either House of Parliament.

u) Data processed for domestic purposes

There are more complex requirements with respect to Health, Social Services and Education records. It is not possible to provide an explanation in respect of those provisions in this summary. Those who are likely to hold such personal data are advised to consider the detailed provisions of the following statutory instruments:

a) The Data Protection (Subject Access Modification) (Health) Order 2000/413

b) The Data Protection (Subject Access Modification) (Social Work) Order 2000/415

c) The Data Protection (Subject Access Modification) (Social Work) (Amendment) Order 2005/467

d) The Data Protection (Subject Access Modification) (Education) Order 2000/414

e) The Education (Pupil Information) (England) Regulations 2005/1437

Note that s. 27(5) DPA, provides that:

\(^{13}\) Personal data shall be processed in accordance with the rights of data subjects under this Act.
"Except as provided by this Part, the subject information provisions shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information."

This means that the exemptions provided for in the DPA and the secondary legislation are a complete code of the exemptions from compliance. There is no recourse to any other rule of law or enactment to avoid compliance.

7) **Does it include personal data relating to other (third party) individuals?**

The personal data of the data subject may include references to other individuals. Although the data subject has a right to be provided with their personal data, this right has to be balanced against the rights of third parties in respect of their personal data. This is set out in ss. 7(4) - (6) and s. 8(7) DPA. The effect of these provisions is that you do not have to comply only to the extent that the personal data contains information relating to another individual who can be identified from that information unless the third party has consented to disclosure or it is reasonable in all the circumstances to disclose it without consent.

Considerations about personal data of third parties may also affect the obligation to provide information about recipients and sources of the personal data of the data subject seeking access.

When considering whether it is reasonable to disclose in the absence of consent, the following factors (as well as any other relevant factors) should be considered:

a) any duty of confidentiality owed to the other individual,

b) any steps taken by the data controller with a view to seeking the consent of the other individual,

c) whether the other individual is capable of giving consent, and

d) any express refusal of consent by the other individual.

Where, for example, an email contains not only the personal data of the data subject but also personal data of a third party, you must consider whether it is reasonable to disclose the personal data of the data subject, if the disclosure would be likely to enable the data subject to identify the third party. In making this assessment you should consider what information you know or reasonably believe is in the possession of the data subject which may enable them to identify the third party and what is the likely impact of the disclosure.

This does not excuse you from providing as much of the personal data of the data subject as is possible without the identifying material.

8) **What form does my response have to take?**

Your obligation is to provide the data in permanent and intelligible form, not the documents containing the data. This is not a disclosure-type exercise. However, it may be simpler to
provide redacted copies of documents rather than retype the data in hard copy. If it is impossible or involves disproportionate effort to provide the hard copy or if the data subject consents you may provide the data in another form, e.g. electronic or ‘soft’ copy, provided it is in an intelligible form. It may be advantageous to retype the data if the nature of the document (even in redacted form) discloses information about third parties which may lead to their identification.

9) What happens if the data subject is not satisfied with my response?

If the data subject considers your response inadequate there are two avenues open to them. They may complain to the Information Commissioner that you have failed to comply with their request or they can apply to the Court for an order under s. 7(9) DPA requiring you to comply.

If the Information Commissioner considers that subject access should have been given he may serve an information notice to determine if you are complying with the data protection principles (DPP). Failure to comply with the SAR is a breach of the 6th DPP 14. Usually the ICO will seek to resolve the issue through negotiation, at least initially. If this fails, it may serve an enforcement notice requiring you to comply. Failure to comply with an enforcement notice is a criminal offence. If you disagree with the information notice or the enforcement notice you can appeal them to the Information Tribunal. The burden of justifying the notices rests on the Information Commissioner. In addition, if the ICO considers that the breach of the DPA is serious it may impose a monetary penalty.

If the application is made to the Court, the Court can consider the information which you hold on the data subject without providing it to data subject in order to assess whether you have complied. However, it cannot order its disclosure to the data subject unless and until it decides that you have failed to comply with the SAR.

Sources of Guidance

This is necessarily a brief overview of the various complex provisions, and is no substitute for getting professional advice. Further guidance may be obtained from the following sources:

- The website of the Office of the Information Commissioner contains much useful guidance
- The statutory materials can be found online
- The European Commission also provides guidance

Important Notice

This document has been prepared by the Bar Council to assist barristers on matters of IT. It is not “guidance” for the purposes of the BSB Handbook 16.4, and neither the BSB nor bodies regulating information security nor the Legal Ombudsman is bound by any views or advice expressed in it. It does not comprise - and cannot be relied on as giving - legal advice. It has

14 The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 (SI 2000/419)
been prepared in good faith, but neither the Bar Council nor any of the individuals responsible for or involved in its preparation accept any responsibility or liability for anything done in reliance on it. For fuller information as to the status and effect of this document, please refer to the professional practice and ethics section of the Bar Council's website here.