Subject Access Requests under the UK General Data Protection Regulation (UK GDPR)

Purpose:	To guide all barristers and chambers' data controllers on Subject Access Requests under the UK GDPR
Scope of application:	All practising barristers and chambers' data controllers
Issued by:	The Information Technology Panel
Last reviewed:	December 2022
Status and effect:	Please see the notice at end of this document. This is not "guidance" for the purposes of the BSB Handbook I6.4.

What is the UK General Data Protection Regulation?

1. The General Data Protection Regulation ("**UK GDPR**") is a European Regulation which came into effect in the UK from 25 May 2018. Since 1 January 2021, this has been modified and now the UK GDPR is in effect. This mirrors the GDPR in most significant respects, the most notable changes being the extent of the jurisdiction and that the only relevant regulatory body is the Information Commissioner. However, despite these changes the EU has confirmed that, at present, the current UK data protection regime is adequate.

2. This guidance assumes that you are a barrister in private practice and therefore a data controller (see below). As a data controller the ultimate responsibility for compliance lies with you. In some situations that responsibility may additionally be shared with the data processor.

3. If an employee, you may find this guidance helpful if you are complying with a Subject Access Request ("**SAR**"), i.e. a request from a data subject whose information you have, on behalf of an employer (who is a data controller). If so, you will need to adapt this guidance to your circumstances. What follows is intended to assist you in compliance with your data protection obligations in respect of a SAR, but is not legal advice.

4. Under the Data Protection Act 1998 you had an obligation to comply with Subject Access Requests. That obligation continues under the UK GDPR and the Data Protection Act 2018 ("**DPA 2018**") but has been modified.

Why is this relevant to me?

5. All barristers in self-employed practice who use a digital device for word processing, send emails or instead use a structured manual filing system for their work are highly likely to be data controllers.[1]

6. This is because the information which is stored on your computer (or in a structured filing system)[2] in the course of your work is likely to contain information about individuals (e.g. witness statements, expert reports, emails). This is personal data. You control what you do with that information (or what is done on your behalf, e.g. by your chambers staff, as data processors). This means that you are a data controller. You are also responsible for personal data processed on your behalf by your clerks, other staff or IT service providers, such as cloud storage facilities. Processing is a very wide term, and even covers simply storing the data.

7. The Information Commissioner's Office has provided guidance as to the SARs - aka the right of access[3].

8. The UK GDPR can be found here. See in particular: Arts. 5, 6, 9, 10, and 12 - 15.

What is a Subject Access Request (SAR)?

9. A subject access request is a request from or on behalf of an individual (not a company) which seeks to discover (1) whether and why you are processing the personal data of that individual (a data subject), (2) if so, to have access to that information and, (3) in addition, to be provided with additional information, which corresponds broadly to the information which should be provided in your privacy notice.

10. Requests may be made informally so it is important for you and your clerks to be able to consider if a SAR is being made when a request for information is made. It may be sensible to have a policy document or action points that they can refer to. This will also help you to check what you have to do and what the deadlines are. You may want to consider setting up and providing a specific, monitored email address to

[1] In addition, for the first time, the UKGDPR places obligations on data processors.
[2] The CA has recently considered this aspect under the DPA 1998 following an ECJ decision (see para. 30 below). Whether the same test applies under UKGDPR has not yet been determined, but it seems likely
[3] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UKGDPR/right-of-access/

channel such requests, such as dataprotection@chambers.co.uk, to make identification easier.

How do I tell if I have received a SAR?

11. 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 UK GDPR or explicitly identify itself as a SAR. Under the UK GDPR/DPA 2018 no fee can be charged unless the request is manifestly unfounded or excessive, such as a recent repeat request. In addition, the request may be sent to your Chambers rather than to you personally. In these circumstances it would be sensible for Chambers to be on the lookout for such requests and when received, to clarify who is the intended recipient of the SAR.

12. It is important that before responding you satisfy yourself that the request has actually been made by the data subject and not by someone illegitimately trying to obtain personal information concerning the data subject. If you are unsure whether the person making the request is the data subject you can ask for more information. However, you should only request information that is necessary to confirm who they are. The key to this is proportionality. You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when you receive the additional information. In some cases, a utility bill addressed to the data subject may be sufficient in order to confirm identity. But where the data requested concerns a person involved in a divorce case, for example, the data subject's spouse may have access to utility bills, or even a passport, and it may be necessary to obtain confirmation of identity in some other way.

13. Where the SAR is manifestly unfounded or excessive you can charge a reasonable fee taking into the cost of administration or alternatively refuse to respond. But be aware that you will bear the burden of proving this, if challenged. In assessing whether the request is excessive, you will need to consider the interval between repeat requests, the nature of the data, the purpose for which the data 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.

14. You should ensure that your staff and anyone processing data on your behalf are trained so that they can recognize a SAR when they receive one and know what to do, including the need to be satisfied as to the identity of the person making the request.

15. 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 SAR.

How long do I have to respond?

16. You must respond to the request without undue delay and **in any event within 1 month** from receiving the SAR. If the complexity or number of requests received means that additional time is needed or further information is required you can take advantage of an extension of up to 2 months. If you need an extension, you still need to let the data subject know within 1 month, of any extension and the reasons for the delay.

17. Similarly, if you do not intend to comply you should notify the data subject within 1 month and give your reasons. You are still required to provide them with information about their right to lodge a complaint with a supervisory authority (see paragraph 22.g below).

How do I comply?

18. If, on considering the SAR, you are unable to identify the requester as a data subject, i.e. a person about whom you process data, you can simply respond with that information (see para. 21 below). You are not required to obtain additional information to identify the data subject in order to comply, although you should not refuse to accept additional information provided to identify the data subject, if it is offered.

19. If, however, you have doubts about the identity of the data subject, you may request the provision of further information to confirm the identity of the data subject.

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

21. If you are not processing any information about the data subject, you can answer the request in the negative and you will have complied. You should do so within 1 month. However, you should note that processing is a broad term, and includes mere storage of the information. It also includes the act of obtaining information which it is intended <u>will be</u> stored as personal data, even if it is not at that stage being processed automatically, e.g., handwritten notes that you routinely transcribe and save on a PC.

22. If you are processing such data you have to provide:

a. access to the data - this does not require disclosure of the document containing the data, just the data;

b. the purposes of the processing, e.g. providing legal services, accounting, education, contracts and enforcement;

c. the categories of personal data concerned, i.e. information about an individual relating to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, such as criminal convictions, health or financial status;

d. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

e. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period. This requires that you have a retention policy in respect of the personal data that you retain. For guidance on retention policies and periods see the Bar Council Guidance on Data Retention here;

f. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

g. the right to lodge a complaint with a supervisory authority (in England and Wales this is the Information Commissioner's Office);

h. where the personal data are not collected from the data subject, any available information as to their source;

i. the existence of any automated decision-making, including profiling, (referred to in Art. 22(1) and (4)) and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. It is unlikely that this will apply to the processing that you do in the course of providing legal services, and

j. where personal data is transferred to a country or organisation outside the EU, the safeguards in place to protect the personal data.

23. The data should be provided in a commonly used electronic form where the request is made in electronic form unless the data subject requests otherwise. Provision of the data will satisfy 22.a and 22.c above. You may need to consider how you are going to ensure that the information remains secure. Free secure email platforms are available, or you could consider sending an encrypted device, and separately providing the password.

24. Note that the requirement is not for disclosure under the CPR. The obligation is to provide the information, not documents containing the information. The requirement to provide the information in paras. 22.b and 22.d above are similar to the contents of the notification which was required under the DPA 1998.

25. '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 public authorities conducting an inquiry in accordance with national law[4]. However, as the provision of such information may involve the potential disclosure of the personal data of third-party individuals (e.g. if you name the persons to whom the data has been disclosed), it is subject to the considerations set out below. This potential problem can be avoided if you can describe, instead, the class of recipients, for example, "staff".

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

A. What information about the person do I have?

B. What information about the person is processed by data processors on my behalf, such as Chambers, an email provider, or a cloud storage service?

C. Is the personal data processed or intended to be processed by automatic means?

D. If not, is the information held in a structured filing system?

E. Is it personal data?

F. Is it exempted from compliance in whole or in part?

G. Do have to limit the disclosure I make because it includes personal data relating to third party individuals?

H. What form does my response have to take?

I. What happens if the data subject is not happy with my response?

A. What information about the person do I have?

27. 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

[4] Art. 4(9) UKGDPR.

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.

28. Finding data about an individual is easier and quicker if you have structured the storage of files to make this easier. You could, for example, set up your file storage by reference to the name of your client. If, however, the data subject is not a named client, you will need to use a search facility to search your systems by reference to their name or other identifier, e.g. email address.

29. Where you process a large amount of information about the data subject you should request that the data subject specify the information or processing activities to which the request relates.

B. Is the personal data processed or intended to be processed by automatic means?

30. If 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 a USB stick, it will be covered by the UK GDPR if it is also personal data[5]. 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.

C. Is the information held in a structured filing system?

29. Even if the information is not processed by automatic means and is held in a structured manual filing system it may still be personal data. "Filing system" is defined in the DPA 2018 as "any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis". In *Dawson-Damer v Taylor Wessing LLP* [2020] EWCA Civ 352, the Court of Appeal set out a 4-part test for identifying whether information was part of a filing system under the DPA 1998 and the Directive:

- are the files a "structured set of personal data"?
- are the data accessible according to specific criteria?
- are those criteria "related to individuals"?
- do the specific criteria enable the data to be easily (or "readily" as the 1998 Act puts it) retrieved?

[5] Art. 2 UKGDPR

The specific criteria must be related to the individuals whose information is concerned and those must enable ready access to the data. The Court of Appeal found that the "temp test" explained by the ICO in its FAQs to be of assistance:

> "Is there any rule of thumb I can apply to establish whether I have a relevant filing system?
>
> If you employed a temporary administrative assistant (a 'temp'), would they be able to extract specific information about an individual from your manual records without any particular knowledge of your type of work or the documents you hold? The 'temp test' assumes that the temp in question is reasonably competent, requiring only a short induction, explanation and/or operating manual on the particular filing system in question for them to be able to use it."

D. Is it personal data?

30. The definition of "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This can include, for example, name, address, IP address or an opinion about a person.

31. If you are in doubt as to whether the information constitutes personal data, you should take professional advice.

E. Is the data nevertheless exempted from compliance?

32. There may be circumstances in which compliance may be limited or excused. The ambit of the exclusions and limitations is set out in DPA 2018, which now refers to the UK GDPR. The current position is as follows.

33. Art. 15 UK GDPR provides for subject access requests. Section 15 DPA 2018 identifies where all the exemptions and derogations from the subject access rights provided by UK GDPR, which include SARs, can be found. These are located in the Schedules 2 – 4 of the Act. The following summarises the main exemptions, but there are many other exemptions which may apply to your specific circumstances, for which you may need to take expert advice. The right does not apply in the following circumstances:

a. where disclosure of the information is (a) is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), (b) is necessary for the purpose of obtaining legal advice,

or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights, to the extent that the application of those provisions would prevent the controller from making the disclosure. (Sch. 2 para 5(3) DPA 2018). As can be appreciated this is a very narrow exemption and is unlikely to be of much relevance because it is confined to necessary disclosures.

b. Where disclosure of the data is required by an enactment, a rule of law or an order of a court or tribunal, to the extent that Art. 15 would prevent the controller from making the disclosure (Sch. 2 para 5(2) DPA 2018). This recognises the supremacy of law and court orders over the limitations on disclosure provided in Art. 15 UK GDPR.

c. to the extent that compliance would involve disclosing information relating to another individual who can be identified from the information (this also applies to identifying the source of the information) (Sch. 2 para. 16). This exemption does not apply if the third-party consents to disclosure or if it would be reasonable to disclose without that consent. Reasonableness is to be assessed in all the circumstances including: (a) the type of information that would be disclosed, (b) any duty of confidentiality owed to the other individual, (c) any steps taken by the controller with a view to seeking the consent of the other individual, (d) whether the other individual is capable of giving consent, and (e) any express refusal of consent by the other individual. In specific circumstances, set out in DPA 2018 Schedule 2 Part 3 para.17, reasonableness is presumed, e.g. health professionals.

d. where the data consists of information which is the subject of legal professional privilege (Sch. 2, para. 19 DPA 2018);

e. personal data processed for the prevention or detection of crime, the apprehension or prosecution of offenders, to the extent that the application of those provisions would be likely to prejudice any of those matters (Sch. 2 para. 2 DPA 2018).

f. to the extent that compliance would reveal evidence of the commission of an offence (by that person) and expose the person to proceedings for that (self-incrimination exemption). This does not apply to data protection offences or to offences of making false statements otherwise than on oath. However, data disclosed in compliance with Art. 15 UK GDPR is not admissible against the person in proceedings for an offence under DPA 2018.

34. There are a number of other exemptions in DPA 2018, which relate to other circumstances, e.g. negotiations, confidential references, journalism, artistic and literary purposes, research etc. which may be relevant to peripheral activities. DPA 2018 should be consulted in relation for a complete list and the conditions that apply.

35. The UK GDPR does not cover personal data processed by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. DPA 2018 does cover this processing in Part 3. However, the definition of "competent authority" in s. 30 DPA 2018, means that this applies to the police or other investigating authorities rather than barristers carrying out their normal activities.

F. Does it include personal data relating to other (third party) individuals?

36. The personal data of the data subject may include references to other individuals. If you get a SAR you will need to decide whether you can disclose the personal information of third parties, which is not privileged information. If it is privileged information, obviously you cannot disclose it, unless it is the privilege of the person asking for it.

G. What form does my response have to take?

37. Your obligation is to provide the data in a commonly used electronic form if the SAR was made by electronic means, unless a different form is asked for by the data subject. As pointed out above, you may need to consider if the mechanism you plan to use ensures that the information remains secure during transit. Free secure email platforms are available or you could consider sending an encrypted device or CD-ROM, and separately providing the password.

H. What happens if the data subject is not satisfied with my response?

38. If the data subject considers your response inadequate there are likely to be three avenues open to them. They may complain to the ICO, to the Courts or to the BSB.

39. Failure to comply with a SAR without a justification is a breach of the UK GDPR and the DPA 2018 which may expose a data controller to administrative action by the ICO which can include administrative fines up to a maximum of £17,500,000 and/or to pay compensation to the data subject.

I. What if the SAR comes from a minor?

40. The guidance provided by the ICO under the DPA 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.

41. Under the UK GDPR, there are specific requirements in relation to consent of children to the provision of information society services which suggests that the minimum age of consent which can be set by a national government is 13. The UK has chosen 13 as that age.

42. More generally, if you know the individual child 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 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 a family relationship.

Sources of Guidance

43. 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 as to interpretation of the GDPR, but not the UK GDPR, where that differs.