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

Purpose: To guide all barristers and chambers’ data controllers on Subject Access Requests under the GDPR

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

Issued by: The Information Technology Panel

Last reviewed: October 2017

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 General Data Protection Regulation?

1. The General Data Protection Regulation (GDPR) is a new law that will replace the Data Protection Act 1998 in the UK from 25 May 2018. The government has confirmed that the UK’s decision to leave the EU will not affect the commencement of the GDPR.

2. There are a number of aspects of the GDPR which are left to national governments to specify. The government has proposed a Data Protection Bill. Accordingly, what follows is intended to assist in compliance with the GDPR. However, as a data controller the ultimate responsibility for compliance lies with you. In some situations that responsibility may be shared with the data processor.

3. Under the Data Protection Act 1998 as a data controller you had an obligation to comply with Subject Access Requests. That obligation continues under the GDPR but has been modified. In the interim you should have regard for the guidance previously provided in respect of the Data Protection Act 1998.

---

Why is this relevant to me?

4. All barristers in self-employed practice who use a computer or a structured manual filing system for their work are highly likely to be data controllers. In addition, for the first time, the GDPR places obligations on data processors.

5. This is because the information which is stored on your computer (or in a structured filing system) in the course of your work is likely to contain information about individuals (e.g. witness statements, expert reports, emails). This is personal data. To a large extent you control what you do with that information. This means that you are a data controller. You are also responsible for personal data processed on your behalf by your clerks or other staff.

6. The Information Commissioner’s Office has provided some guidance as to the right of access.

7. The GDPR can be found here. See in particular Arts. 10, 15 and Recitals 57 and 63.

What is a subject access request (SAR)?

8. A subject access request is a request from or on behalf of an individual (not a company) which seeks to discover (1) whether 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 to be provided in your privacy notice [see link] and paragraph Error! Reference source not found.

9. Requests may be 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?

10. 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 Regulation or explicitly identify itself as a SAR. Under the GDPR, unlike under the DPA, no fee can be charged unless the request is manifestly unfounded or excessive, such as a recent repeat request.

11. 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.

---

2 The ICO suggest that this is a wider definition than under the DPA and may include chronologically ordered sets of manual records containing personal data. (https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/introduction/)

You will bear the burden of proving that the SAR is manifestly unfounded or excessive. In assessing whether the requests are excessive, you will need to consider the interval between repeat requests, 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.

12. You should ensure that your staff are trained so that they can recognise a SAR when they receive one and know what to do.

13. 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.

**How long do I have to respond?**

14. 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.

15. 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 20.7 below).

**How do I comply?**

16. If, on considering the SAR, you are unable to identify the requester as a data subject 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.

17. 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.

18. 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.

---

4 Recital 57 GDPR
19. 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 storing the information. It also includes obtaining information which it is intended will be stored as personal data.

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

20.1 access to the data;

20.2 the purposes of the processing, e.g. providing legal services, accounting, education;

20.3 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.

20.4 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;

20.5 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 GDPR.

20.6 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;

20.7 the right to lodge a complaint with a supervisory authority;

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

20.9 the existence of 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

20.10 where personal data is transferred to a country or organisation outside the EU, the safeguards in place to protect the personal data.
21. 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 20.1 and 20.3 above.

22. 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 20.2 and 20.4 are similar to the contents of the notification which was required under the DPA.

23. ‘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 EU or national law\(^5\). 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”.

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

- What information about the person do I have?
- Is the personal data processed or intended to be processed by automatic means?
- If not, is the information held in a structured filing system?
- Is it personal data?
- Is it exempted from compliance?
- Does it include personal data relating to third party individuals?
- What form does my response have to take?
- What happens if the data subject is not happy with my response?

A. **What information about the person do I have?**

25. 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.

---

\(^5\) Art. 4(9) GDPR.
26. Where you process a large amount of data 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?

27. 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 USB sticks it will be covered by the GDPR if it is also personal 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.

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

28. 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. The specific criteria for the identification of such filing systems have not been included in the Regulation, so the ambit of this definition is uncertain.

D. Is it personal data?

29. 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.

30. 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?

31. There may be circumstances in which compliance may be limited or excused. The ambit of the exclusions and limitations is set out in Data Protection Bill, but this is obviously uncertain. At present the position is likely to be as follows.

32. Art. 15 (1) – (3) – the subject access rights - are excluded where information is required to be provided by law or in connection with legal proceedings, but only to the extent that the disclosure under Art. 15 would prevent such disclosure. This is the subject of representations by the Bar Council.

---

6 Art. 2(1) GDPR
33. Art. 15(1) – (3) are also excluded where compliance would involve disclosing information relating to another individual.

34. Art. 15(1) – (3) – do not apply to data which consists of information which is the subject of legal professional privilege or to the extent that disclosure would reveal evidence of the commission of an offence, not including offences under the Data Protection Bill or s. 5 Perjury Act 1911.

35. There are a number of other exemptions in the Data Protection Bill, which relate to other circumstances, e.g. negotiations, confidential references etc. which may be relevant to peripheral activities. The Bill should be consulted in relation for a complete list.

36. The 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.

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

37. The personal data of the data subject may include references to other individuals. The provision of a copy of the personal data of the data subject should not adversely affect the rights and freedoms of others.

38. As set out above, as with the DPA, the Data Protection Bill provides for an exemption from the subject access rights where disclosure would reveal information about another individual, who can be identified from the information.

G. What form does my response have to take?

39. 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.

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

40. If the data subject considers your response inadequate there are likely to be two avenues open to them. They may complain to the ICO or to the Courts.

41. Failure to comply with a SAR without a justification is a breach of the GDPR which may expose a data controller to administrative action by the ICO and/or to pay compensation to the data subject and/or an administrative fine not exceeding 20M Euros.
I. What if the SAR comes from a minor?

42. 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.

43. Under the 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.

44. 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 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 a family relationship.

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 I6.4, 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 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 see here.