Joint Data Controllers under the UK GDPR

Purpose:	To advise the profession in relation to being a joint data controller with solicitors' firms
Scope of application:	All practising barristers and chambers
Issued by:	The Information Technology Panel
Issued on:	May 2018
Last reviewed:	October 2022
Status and Effect:	**Please see the notice at the end of this document. This is not "guidance" for the purposes of the BSB Handbook I6.4.**

Introduction

1. The Bar Council's IT Panel has previously provided a note to the effect that barristers are not usually to be regarded as data processors acting on behalf of solicitor data controllers. This document addresses a different point, namely whether barristers and solicitors, who are each data controllers, are to be regarded as joint data controllers to whom UK GDPR Article 26 applies.

2. UK GDPR Article 26 is as follows:

> **Joint controllers**
>
> (1) Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the

controllers are subject. The arrangement may designate a contact point for data subjects.

(2) The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

(3) Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

3. The Data Protection Act 2018 defines joint controllers as follows:

58 Joint controllers

(1) Where two or more competent authorities jointly determine the purposes and means of processing personal data, they are joint controllers for the purposes of this Part.

(2) Joint controllers must, in a transparent manner, determine their respective responsibilities for compliance with this Part by means of an arrangement between them, except to the extent that those responsibilities are determined under or by virtue of an enactment.

(3) The arrangement must designate the controller which is to be the contact point for data subjects.

Joint controllership

4. The concept of joint data controllership is not new—it existed under the Data Protection Act 1998 (and indeed before).

5. Article 26 UK GDPR applies only where "two or more controllers *determine the purpose and means of processing*". Similarly, under the DPA 2018 joint controllers are those who "jointly determine the purposes and means of processing personal data".

6. The ICO has provided a checklist (available here) offering indicators as to whether two controllers are joint controllers:

- "We have a common objective with others regarding the processing.

- We are processing the personal data for the same purpose as another controller.
- We are using the same set of personal data (e.g. one database) for this processing as another controller.
- We have designed this process with another controller.
- We have common information management rules with another controller."

7. Other than in exceptional circumstances, the relationship between a barrister and that barrister's instructing solicitor in respect of a typical set of instructions or a typical brief will not meet these criteria. Instead, the barrister in question will (and will be professionally obliged to) form an opinion as to how the personal data should be used, how and where it should be stored, and as to the period for which it should be retained. **The barrister and the solicitor will therefore be processing a pool of data independently of each other, and will not be joint controllers.**

8. Any attempt to restrict the barrister's freedom of action in relation to the use of personal data could have the effect of preventing the barrister complying with Code of Conduct obligations, in particular with regard to the barrister's duty to the court (CD1, rC4 and rC16), and with regard to obligations to act independently in the best interests of the client, not to permit the professional client to limit the barrister's discretion as to how the interests of the client can best be served (CD4, rC3.5 and rC15.4), and to keep appropriate records (rC87.2).

COMBAR/CLLS guidance

9. The Commercial Bar Association, COMBAR, and the City of London Law Society, CLLS, published the following guidance in relation to joint controllers, concerning clause 19.5 of the revised version 3 of the COMBAR/CLSS terms of contract:

> "In some circumstances, the Solicitor and the Barrister may be joint controllers of personal data (perhaps with the Lay Client) within the meaning of article 26 of the GDPR. These circumstances may include the drafting of letters or witness statements, into which considerable input is received from both Solicitor and Barrister and which contains personal data of various data subjects. If the Solicitor and the Barrister are joint controllers, they are obliged to determine in a transparent manner their respective responsibilities for compliance with their obligations under the GDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in articles 13 and 14, by means of an arrangement between them. Clause 19.5 sets out an arrangement, placing individual responsibility on the Solicitor and

> the Barrister for the processing each undertakes, for the implementation of appropriate technical and organisational standards and as regards the exercising of the rights of the data subject. However, it places responsibility on the Solicitor to comply with articles 13 and 14 of the GDPR. These articles oblige the data controller to provide a "data subject" with certain information. This obligation does not apply to personal data that consists of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings (paragraph 19 of Schedule 2 to the Act)."

10. For the avoidance of doubt, this guidance is not inconsistent with what is stated above. The circumstances in which a barrister and solicitor may be joint controllers are likely to be rare. They might conceivably occur where a letter is drafted, or where a barrister is instructed to assist in the drafting of a witness statement with no ongoing involvement in the case thereafter. But where the barrister who assists in the drafting of a witness statement is to be instructed at trial, the barrister will need to be free to take independent decisions in relation to the use, retention and deletion of personal data. In addition, for the same data the barrister will be a data controller in the barrister's own right where acts of processing (such as retaining, storing and disclosing the data) are carried out for the barrister's own purposes, e.g. in relation to potential claims made against the barrister in the provision of legal services.

Article 26 Arrangement

11. If, in a rare case, joint controllership arises, there is no need for a formal written contract between the parties. Article 26 (by contrast with Article 28(3)) does not refer to a contract but only to "arrangement" between joint controllers.

12. The ICO guidance on what constitutes a "transparent arrangement" (available here) is as follows:

> "Joint controllers are not required to have a contract, but you must have a transparent arrangement that sets out your agreed roles and responsibilities for complying with the GDPR. The main points of this arrangement should be made available to individuals. We recommend that you include this in your privacy information."

13. The aim is to ensure that they are each aware of their respective responsibilities, and that the essence of the position is made transparent to the data subject(s), so far as possible.[1] Accordingly, if it is required at all, there is no reason why an Article 26 arrangement need do any more than state what the position would be in any event, namely that each data controller should remain individually

[1] These arrangements cannot be completely transparent to the extent that the obligation of confidentiality prevents disclosure of the fact of processing to non-client data subjects.

responsible for ensuring that its own processing is in compliance with data protection law. This is the approach taken by Clause 19.5 of the COMBAR/CLLS terms, which includes the following:

> "If and to the extent that the Barrister and the Solicitor are joint controllers (whether or not with anyone else) for the purposes of Data Protection Law, each shall, unless otherwise agreed, be individually responsible for ensuring that the processing each undertakes is in accordance with Data Protection Law, for ensuring so far as each is able the implementation of appropriate technical and organisational measures in accordance with Data Protection Law, and as regards the exercising of the rights of the data subject, but the Solicitor shall be responsible for the provision of information referred to in articles 13 and 14 of the GDPR if and to the extent that this provision of information is required by Data Protection Law."

14. Any arrangement which goes beyond this and purports to provide for indemnities or other terms which might alter the allocation of liability following a data breach on the part of one of the joint controllers, is potentially problematic and should be approached with caution. Barristers must, of course, have in mind their professional obligation to act independently in the best interests of the lay client. An agreement to alter the allocation of liability might, depending on the wording and on the circumstances, be incompatible with that duty of independence, and might have ramifications in relation to professional indemnity insurance (especially insofar as it requires a barrister to assume any liability which would not have arisen in any event by reason of common law, equity or statute.)

Important Notice

This document has been prepared by the Bar Council to assist barristers on matters of information security. **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.