UK GDPR: Frequently Asked Questions

Purpose:	To address frequently asked questions in relation to practical compliance with the GDPR
Scope of application:	All practising barristers to address the laws applicable in England and Wales
Issued by:	The Information Technology Panel
Issued on:	March 2023
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.**

Table of Contents

Introduction

1. This is a brief response to address some frequently asked questions (FAQs) in relation to practical compliance with UK GDPR. Data protection laws in both the EEA (the EU plus Iceland, Norway, and Liechtenstein) and UK are intended to ensure information about living individuals (within the definition of 'personal data') is used fairly and responsibly. To help ensure that, both EEA and UK data protection laws impose many obligations on those 'processing' personal data (and on controllers of such processing) and grant rights to those whose personal data is processed (the 'data subjects'). In summary, 'processing' includes doing almost anything with personal data, including storing, sharing, deleting, or using it.

2. The UK GDPR regime presently comprises two main pieces of legislation:

a) a version of the EU's General Data Protection Regulation, Regulation (EU) 2016/679 (the EU GDPR) incorporated into UK law (with various amendments made by Brexit legislation) following the end of the Brexit implementation (or 'transition') period at 11pm on 31 December 2020 (Retained Regulation (EU) 2016/679, the UK GDPR).
b) the parts of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement, as amended by Brexit legislation following the end of the Brexit implementation period (the DPA 2018).

3. When considering the general processing of personal data, both the UK GDPR and the Data Protection Act 2018 should be read together as both sets of provisions directly apply.

4. Although these responses to FAQs are in response to UK GDPR it should be noted that the UK GDPR is heavily derived from the EU GDPR and generally the terms and core concepts used in the UK GDPR have the same meaning as they do in the EU GDPR, although there are a number of key detailed differences between the two regimes. In summary, in a similar manner to the EU GDPR, the UK GDPR

applies to the processing of personal data and provides rights to those data subjects whose data is processed and imposes obligations on both controllers and processors of the personal data.

4. At the moment, the UK GDPR and the EU GDPR are very similar, but the UK's Data Protection and Digital Information Bill announced in 2022 is expected to introduce a number of data protection reforms and result in further divergence between the EU GDPR and UK GDPR. These FAQs will be reviewed in due course to account for this.

Privacy Notices (Articles 13-14)

Q1. When do I need to provide Article 13 and 14 notices?

Subject to the exceptions mentioned below, an Article 13 notice must be served on a data subject when you collect personal data from a data subject, and an Article 14 notice must be served on a data subject when personal data have been obtained otherwise than from that data subject.

Suggested general practice has been to include a link to your Privacy Notice in the signature block of your emails.

So far as timing is concerned:

- When an Article 13 notice is required, you have to provide the notice at the time when you obtain personal data from the data subject.
- When an Article 14 notice is required, you have to provide the notice within a reasonable period of obtaining the personal data, but at the latest within one month. If the data is used for communicating with the data subject, you have to provide the notice at the time of first communication. If the data will be given to someone else, you have to provide the notice before you do so.

There are exceptions as follows:

(1) No Article 13 or 14 notice is required if the data subject already has the information.
(2) The Data Protection Act 2018 (DPA 2018) introduces permitted exemptions which are set out in Schedule 2. Exemptions which are likely to be of most use to barristers are:

(i) Legal Professional Privilege (LPP):

DPA Schedule 2 paragraph 19 provides that no Article 13 or 14 notice is required in relation to personal data that consists of -

(a) information in respect of which a claim to legal professional privilege or, in Scotland, confidentiality of communications, could be maintained in legal proceedings, or
(b) information in respect of which a duty of confidentiality is owed by a professional legal adviser to a client of the adviser.

(ii) Self-incrimination:

DPA Schedule 2 paragraph 20 provides you need not comply with Articles 13 or 14 notices to the extent that compliance would, by revealing evidence of the commission of an offence, expose you to proceedings for that offence.

(iii) Confidential references:

DPA Schedule 2 paragraph 24 provides that no Article 13 or 14 notice is required if the listed GDPR provisions do not apply to personal data consisting of a reference given (or to be given) in confidence for the purposes of –

(a) the education, training or employment (or prospective education, training or employment) of the data subject,
(b) the placement (or prospective placement) of the data subject as a volunteer,
(c) the appointment (or prospective appointment) of the data subject to any office, or
(d) the provision (or prospective provision) by the data subject of any service.

(3) No Article 14 notice is required if:

(a) the provision of such information proves impossible or would involve a disproportionate effort,

(b) or in so far as the obligation to serve a notice is likely to render impossible or seriously impair the achievement of the objectives of that processing.

In the case of (3)(a) and (b) the controller must take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

The UK GDPR and the DPA 2018 contain exemptions from the UK GDPR (see ss. 10 and 15 and Schedules 1 and 2 DPA 2018). The exemption for LPP (para. 19 Sch. 2) restricts the application of the listed UK GDPR provisions to personal data that consists of information over which a claim to legal professional privilege could be maintained in legal proceedings, or information covered by a duty of confidentiality owed by a professional legal adviser to a client of the adviser. It means that in relation to cases on which a barrister is instructed, a barrister may need to serve a privacy notice in at least the following circumstances:

- when a barrister collects personal data from a client, for example when meeting a client in conference, receiving an email directly from a client, or when the barrister takes a witness statement from a client in a direct access case;
- when a barrister has obtained personal data relating to a data subject, and the personal data is no longer subject to an obligation of confidence (for example when a witness confirms in open court that his or her witness statement is true).

Article 13 and 14 notices will also be required in relation to personal data relating to pupillage, equality and diversity, staff recruitment, payroll, etc. insofar as those are done by the barrister as a data controller. This may apply to Heads of Chambers who are designated as the data controller for Chambers' processing activities.

Q2. In relation to providing Article 13 and 14 notices, what is the difference for direct access? Is it the case that the Data Protection Act 2018 exempts

barristers (in non-direct access cases) from the obligation to provide Article 13 and 14 notices, except when the proceedings end?

The rules are the same whether or not you are engaged on a direct access basis. But in practice, if you are instructed by a solicitor, initially you will not receive information directly from the lay client (save, for example, in conference). Article 13 will usually not apply to the lay client's personal data, though it will apply insofar as you receive the solicitor's own personal data, e.g. the solicitor's name and email address. However, it would be sensible to provide a privacy notice to the client with the acceptance of instructions to cover future direct disclosures. If you are engaged on a direct access basis, you are likely to receive the lay client's personal data directly from the lay client, so you will have to provide the lay client with an Article 13 notice in respect of that data.

Q3. When I am instructed by a professional client on behalf of a lay client, does this count as indirectly obtaining personal data from the lay client, and therefore engaging the need for an Article 14 notice?

See Q1 and Q2 above. You will usually not receive the lay client's personal data directly from the lay client, so you will not have to provide an Article 13 notice in respect of that data. You will have to provide an Article 13 notice to your solicitor, however, in respect of the solicitor's own personal data (unless they already have that information). However, you should provide the lay client with an Article 14 notice in due course, and it may be sensible to do this at the beginning of the relationship.

Q4. Is Article 13 for clients, and Article 14 for witnesses?

No. Article 13 is for people who give you their personal data directly. Article 14 is for people whose personal data you are given indirectly. If you have an instructing solicitor, the appropriate notice for both your lay client and for witnesses may be an Article 14 notice, but this depends on whether they give you their data directly or through someone else.

Much of the information to be provided in the Article 13 and Article 14 notices are the same. Remember that the LLP exemption may be of relevance - see Q1.

Q5. Do I need to go through all my old case files and start issuing Article 13 and 14 notices?

No. Article 13 and 14 apply only at the point when data is collected or obtained. So, in the majority of old cases (e.g. where you are not collecting and obtaining personal data, but merely storing for compliance reasons) Articles 13 & 14 will usually not apply.

Where you intend to further process the personal data for a purpose other than those that were disclosed when the personal data were initially collected, you must provide the data subject, **prior to that further processing**, with information on that other purpose and with any relevant further information as referred to in Article 13(2) and (3) or 14(2) and (4).

Q6. Do I need to provide Article 13 notices to solicitors?

Yes, unless they already have the information. You are processing their personal data (such as their name and contact details). Do note the definition of personal data under Article 4.1.

Q7. The IT Panel's GDPR Guide at para. 73 advises that "consent must be obtained indirectly" from lay clients. How will this be obtained?

You need a lawful basis for processing personal data, see the section on 'Lawfulness' in the GDPR Guide at paragraphs 23 - 43.

Paragraphs 29-30 of the Guide may not always be the most appropriate lawful basis for processing. If you do rely on consent (for example when giving advice on a non-contentious matter which does not fall within "legal claims") it may be more practicable to arrange for the solicitor to obtain the data subject's consent. This may especially be the case for data subjects other than the client.

Q8. Do I need to amend my acknowledgement letter to solicitors when they provide me with instructions? If so, is a link to my privacy notice online sufficient?

This will depend on the contents of your acknowledgement letter and information provided. The contact details of your solicitors (name and email address etc.) are personal data. You have to provide an Article 13 notice to a data subject at the time that you collect personal data from them and/or an

Article 14 Notice when you have obtained personal data of the data subject indirectly. You can do that giving them a link to your privacy notice, provided they can access that free of charge and easily. It may be easiest to incorporate a link to the notice in the signature block of your emails (when communicating by email), and to have the notice available on the Chambers' website.

In the contractual terms with your instructing solicitors, it is advisable that you should clearly state that you are a data controller in your own right (not a data processor or joint controller: see the Bar Council's note: 'Signing Controller-Processor Agreements with Solicitor Firms') and mention that you will be processing personal data in accordance with your Privacy Notice (which should be free of charge and easily accessible). See also, the Law Society's corresponding guidance.

Q9. What should be stated regarding possible disclosure of personal data to mini-pupils, secondees, interns etc., in terms of the content of a fair processing/privacy notice?

You must be transparent about what you intend to do with people's personal data. So, if you intend to disclose personal data to pupils, mini-pupils and others, you must say so in a privacy notice. Article 13(1)(e) and Article 14(1)(e) expressly state you must provide the data subject with information on the recipients or categories of recipient of the personal data, if any. You must also say on what Article 6 legal basis you intend to do so: for pupils it is probably in your legitimate interests to provide training to potential new recruits. For mini-pupils, the position is less clear and, it would be better to rely on your client's consent. When relying on the legitimate interests ground, you need to assure yourself that you are not overriding the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child, by disclosure or other processing. If you are processing special categories of personal data, you will also have to say on what Article 9(2) or DPA 2018 Schedule 1 Part 1 or 2 legal basis you rely. You will also need to ensure that any pupil/mini-pupil is a party to a controller/processor agreement under Article 28 (particularly mini-pupils and first-six pupils, as they will be processors on your behalf). This may be included in the confidentiality agreement you have in place with them.

Whether a pupil is a data controller (as opposed to processor) will depend on whether the pupil has sufficient control over the purposes and means of processing the personal data to be considered as a data controller independently of you (e.g. second or third six pupils carrying out work on their own behalf will be data controllers). See the Bar Council's note on Controller-Processor Agreement under GDPR.

Q10. Is it acceptable for barristers to simply refer all parties to the chambers privacy notice online?

It is possible for members of the same set of chambers to use a single chambers privacy notice, so long as each individual barrister complies with the requirement to notify data subjects of his or her identity and contact details. Every self-employed barrister is an individual Data Controller and must have their own privacy notice which they provide to each client when instructed. Other data subjects should also be provided with a privacy notice, subject to the exemptions set out under Q1 above. If all members of Chambers agree as to all the details of the privacy policy, including retention periods etc., then it may be possible for them to use the same privacy policy. If they cannot agree, each barrister should have their own privacy policy.

The barrister may adopt a short form of notice which contains a link to a longer notice which is used also by other members of chambers. Chambers as an entity should have its own privacy notice too.

Storage

Q11. Are pigeon holes still acceptable? Which documents are acceptable for pigeon holes, or other areas which are accessible to other members of chambers?

UK GDPR requires you to process data with a level of security appropriate to the risk, having regard to the nature of the processing, the state of the art, the likely consequences of disclosure, and other factors (Art. 32). You must take such things into account when you design and use your chamber's system (Art. 25). If you are satisfied that the location and access to your pigeon holes means they are appropriately secure, having regard to the information which they contain, i.e. where the pigeonholes are not accessible to anyone other than

members of chambers or others who have signed confidentiality agreements (e.g. pupils or staff etc.) then there should be no additional privacy issues, other than those already in existence (e.g. ABE interviews should be kept in a secure environment). Bear in mind that maintaining the confidentiality of your papers is also a requirement of the Code of Conduct, not just a UK GDPR issue.

Q12. Our cleaner has a key to our locked chambers rooms. Is this acceptable?

Providing your cleaner has been suitably vetted and has the appropriate confidentiality clause in their contract, then again this should not be a problem. But your risk assessment might suggest that some or all of your papers should be stored in a locked cupboard. Make sure your electronic devices are kept secure and encrypted so that they may not be accessed by unauthorised persons.

Q13. Is it acceptable for other members of chambers to have access to each other's rooms?

Please see the answer to (Q11& Q12 above).

Q14. What kind of agreement do we need to create with the company who holds our archived case files?

Under GDPR, the company you use will be a data processor. Standard templates for data controller/data processor contracts are available on the Bar Council's Practice and Ethics Hub here. You will need to make sure the processor agreements incorporate the points set out in Article 28 of the UKGDPR.

Q15. Can I take my laptop abroad with me?

There is no restriction on taking a laptop to a country within the EEA or to a country recognised by the European Commission as having an adequate level of protection for personal data. See here https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en for the list of these countries.

So far as other countries are concerned, the position is as follows. The ICO's Guidance on International Transfers states that for there to be a restricted transfer (i.e. a transfer to which UK GDPR Chapter V applies) there must be transfer to a receiver who is "a separate organisation or individual". It follows that there is no transfer of personal data outside the EEA when a barrister takes a laptop (or other device) containing personal data outside the EEA and brings it back to the UK, provided that no personal data is transmitted from the laptop to another organisation or individual or to a device belonging to another organisation or individual. The Bar Council's IT Panel has asked the ICO to confirm that this interpretation is correct. The ICO has confirmed that this is in line with the approach it would currently take. There is however a possibility that other EU supervisory authorities would consider there to be a transfer of personal data in this situation. You should also have in mind that an involuntary transfer of personal data outside the EEA might take place if the laptop is lost or stolen or if personal data is hacked via an insecure data network (such as an insecure internet cafe, hotel or airport network). While you are located in a country which is not an EEA country, or in a country without an adequate level of protection, you can still use your laptop to send emails containing personal data to the UK, to an EEA country, or to a country recognised as having an adequate level of protection, even though the personal data may be electronically routed through a non-EEA country or a country without an adequate level of protection; the ICO's Guidance states that transfer does not mean the same as transit.

The courtroom

Q16. Can I leave my papers, devices etc. in the robing room?

Not all robing rooms are secure and regardless of encryption or locks, should be regarded as a public space. Papers should preferably be left in a locked case and devices should always be encrypted. Unauthorised disclosure of personal data and confidential information is likely to be a considered as data protection breach, resulting in serious consequences, so careful risk assessment and care should be taken.

Q17. Can I leave my papers and devices in the courtroom? If not, what do I do with them?

Devices should be suitably encrypted. Providing that the courtroom is locked by court staff as you leave and not unlocked until you return, you should carry out your own risk assessment in deciding whether to leave information which may be confidential, commercially sensitive or which contains personal data in the special categories in the court room. Your confidentiality obligations may continue to apply, unless the documents have been referred to in public or otherwise made available to the public.

Data Retention

Q18. Does UK GDPR require deletion of personal data after a period of time?

The fifth GDPR data protection principle requires personal data to be kept in a form which permits identification of data subjects for no longer than is necessary (Article 5(1)(e)).

In order to ensure that personal data are not kept longer than necessary, you must establish time limits for erasure or for a periodic review. You should retain only the information required for the purpose. Information may need to be held for different periods of time depending on its nature and the purpose of the retention. You should also ensure that you are in compliance with any professional codes of conduct and sectoral regulation.

Q19. What does "no longer than necessary" mean, in relation to the need to retain data for conflict checks?

There is no specific guidance on the appropriate period to be considered for conflict checks. It is necessary to consider both the length of the period and the amount of personal data which is retained. If you decide that after X years you will retain only the brief details stored on the chambers fee system, a longer period will be appropriate than if you decide to retain more extensive information such as all the case papers whether in paper or electronic format.

Q20. What do we do about insurance, generally and also in relation to data retention?

On the one hand you may have a legitimate interest in retaining personal data for an appropriate period of time in order to be able to deal with complaints or

claims. On the other hand your insurers cannot expect you to retain personal data for a longer period of time if that would be contrary to GDPR. The appropriate period will not be the same for every barrister, and you must form your own view on this point. See paragraphs 97 to 115 of the Guide. The BMIF have indicated that generally a minimum 12-year retention period should be observed.

Data sharing agreements

Q21. When is a data sharing agreement required?

Data protection law distinguishes between

- a '**controller**': a natural or legal person public authority, agency or other body which (either alone or jointly with others) **determines the purposes and means** of processing personal data; and
- a '**processor**': a natural or legal person public authority, agency or other body which **processes personal data on behalf of the controller**. See the definitions in Article 4 of the UK GDPR.

The UK GDPR also defines the concept of 'joint controllers', which are subject to additional specific obligations under Article 26. Controllers that are not joint controllers are commonly referred to as 'independent' controllers. The Information Commissioner's Office (ICO) has produced a detailed code of conduct for controllers that share personal data . Under the UK GDPR, although there are no specific mandatory arrangements which must be put in place where personal data is shared by one controller with another controller unless they are 'joint controllers' (as defined in Article 26 of the UK GDPR); each controller will need to consider what steps and arrangements are required, or would be prudent, in the circumstances. However, it is necessary for controllers to enter into a written agreement with the processor in compliance with Article 28 UK GDPR to comply with certain minimum obligations. Controllers have a number of obligations where they use a processor, which include undertaking an appropriate level of due diligence and ensuring they can prove they have undertaken sufficient steps to check the processor is competent, as well as conducting appropriate ongoing checks on the processing and the processor once it has commenced. The processor will also have obligations under law and contract. Processors are required to comply with a number of obligations under the UK GDPR in relation to the

manner in which they process personal data. These include a direct (rather than solely contractual) obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the relevant risks. Such measures might include pseudonymisation, encryption, the ability to restore data in a timely manner and regular testing.

Please see the Bar Council's notes: (1) Joint Data Controllers under the GDPR and (2) Signing Controller-Processor Agreements with Solicitors' Firms.

The Data Sharing Code of Practice (DPA 1998 Data Sharing Code) which was originally published by the ICO as part of its obligations under the previous Data Protection Act 1998 (DPA 1998) (now repealed) is yet to be updated, but may be of limited assistance.

Q22. What are the differences between a data sharing agreement and an Article 28 agreement?

An 'Article 28' agreement is one form of 'data sharing' agreement: i.e. an agreement specifically between a controller and a processor stipulating how the data will be processed in accordance with the controller's rules and compliance measures under the UK GDPR.

Q23. Are joint data controllers the same as data controllers in common? When might barristers be joint data controllers?

No: See Bar Council note here.

Q24. Is it acceptable for chambers to embed their controller-processor agreements into their constitutions?

Yes.

Q25. If not a joint controller or controller-processor agreement, do I need any kind of data sharing agreement with instructing solicitors?

Please see the Bar Council's note on Controller-Processor Agreements with Solicitor Firms.

Q26. After receiving instructions, do I need to wait until both lay and professional client have agreed to my privacy notices before I can act?

A privacy notice is a notice served by a data controller on a data subject. It does not need to be acknowledged by the data subject, but if you are sending it to your lay client via your solicitor you may want to ensure that you keep a record of an acknowledgement that it will be passed on.

If you consider that you need a data subject's consent to process their data (for example when you are advising in a non-contentious matter which is not a "legal claim" and you need to process e.g. health data in the Special Categories), then you need to obtain the data subject's consent in accordance with UK GDPR Arts. 4(11) and 7. This applies to all data subjects, not just clients.

Software

Q27. Is backing documents up to the iCloud, or Microsoft One Drive GDPR compliant?

Data should not normally be stored outside of the EEA or in jurisdictions without an existing adequacy decision made by the European Commission (as provided under Article 45) ('permitted jurisdictions').

One of the key protections under the UK GDPR is a restriction under its Chapter V on the transfer of personal data to:

a) any country or territory outside the UK (known as a 'third country'), or
b) an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries (an 'international organisation').

The restriction on such transfers is to ensure the protection granted to personal data in UK travels with the data wherever it goes. The restriction also applies to 'onward transfers', for example if personal data is transferred from the UK to a recipient in country A and then 'onward' transferred to country B or to another recipient in country A.

However, the UK GDPR also expressly acknowledges that international flows of personal data are necessary for the expansion of trade and international co-operation. Therefore, such restricted transfers are permitted if:

a) an adequacy regulation applies, meaning UK authorities have concluded that the third country adequately protects personal data
b) the transfer uses one of a specific set of transfer tools or appropriate safeguards referred to in Article 46 of the UK GDPR
c) or certain limited derogations apply

To check whether the jurisdiction has an adequacy decision granted see the ICO's guidance on International Transfers.

- Unless you are satisfied that the server you are using is situated in a permitted jurisdiction and that the company who owns the server will not store a copy of the data outside the permitted jurisdictions, you should not use this type of cloud service, unless you can comply with Chapter V of the UK GDPR, permitting transfer outside the EEA.

You should only transfer personal data outside the UK or EEA in compliance with Chapter V of the UK GDPR.

Although the European Commission had made a partial adequacy decision in relation to transfers to the USA under the EU-US Privacy Shield Framework, this has since been withdrawn and declared as being an invalid transfer mechanism, following the Court of Justice ruling in the case of *Schrems II*.[1] The UK Government has legislated to confirm that the Privacy Shield mechanism does not exist under the UK GDPR. Therefore, the USA is not recognised by the European Commission or the UK Government as providing an adequate level of protection under the GDPR.

In the absence of an adequacy regulations under section 17A of the Data Protection Act 2018 or of appropriate safeguards pursuant to Article 46 GDPR, you will need to satisfy one of the derogations for specific situations under Article 49 GDPR.

Equality & Diversity

Q28. Chambers collect E&D special category data for the following purposes:

[1] *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems (Case C-311/18*

- **Recruitment: pupillage; mini pupils; established practitioners; staff**
- **Workplace monitoring: BSB required reporting (every 3 years) and work allocation monitoring**

What do chambers need to do in relation to recruitment and workplace monitoring, and how long should they retain data?

DPA 2018 Schedule 1 paragraph 8 provides a lawful basis for processing certain categories of data, subject to specified exceptions, where the processing is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained. The categories are as follows:

Category of personal data:	**Groups of people (in relation to a category of personal data):**
Personal data revealing racial or ethnic origin	People of different racial or ethnic origins
Personal data revealing religious or philosophical beliefs	People holding different religious or philosophical beliefs
Data concerning health	People with different states of physical or mental health
Personal data concerning an individual's sexual orientation	People of different sexual orientation

This is a "substantial public interest" ground. Consent is not required.

Data controllers who process the above personal data must have in place an appropriate policy document: see Schedule 1 paragraphs 5 and 39. This document must (a) explain the controller's procedures for securing compliance with the principles in Article 5 of the UK GDPR (principles relating to processing of personal data) in connection with the processing of personal data in reliance on the condition in question, and (b) explains the controller's policies

as regards the retention and erasure of personal data processed in reliance on the condition, giving an indication of how long such personal data is likely to be retained.

Retention periods

Normally you should retain personal data only for as long as necessary for the purpose for which it was obtained. This includes E&D diversity data. If the information can be pseudonymised or anonymised, this should be carried out.

You may need to keep the data as received, for a short period of time, to meet statutory or professional compliance obligations or in case there is a complaint about the application process.

So, for example, rejected job applicants' details may reasonably be kept for 6 months unless it was clearly communicated to the applicant that there is policy to keep CVs for longer.

You may find the previous ICO guidance on 'The employment practices code' useful.

Q29. How long should we keep sexual harassment data? What about other sensitive E&D issues?

This depends on the nature of the personal data, the circumstances in which it was obtained, and the purpose for which it is being retained, amongst other things. You should only retain this data for so long as it is required either for disclosed purposes, such as for defending against potential claims or for addressing complaints, or for the prevention and detection of an unlawful act. It may also be necessary to retain the data where the processing is a precursor to the disclosure to a competent authority.

For E&D issues – see Q28 above.

Data Protection Officers

Q30. Does this apply to any set of chambers other than a criminal set?

Yes, if you are processing Special Category data on a large scale, you must appoint a DPO (Article 37(1)(c)). Even when there is no requirement to appoint a DPO under UK GDPR & DPA 2018, it may be prudent for a designated member of staff to be responsible for data protection matters. If that person is

not actually a DPO they should not use that title as it implies that they have the necessary qualifications and carry out the duties of a DPO under GDPR.

Q31. When are data protection officers required? What is a large scale?

Recital 91 to the GDPR, referring to similar wording in Article. 35 relating to Data Protection Impact Assessments (in a different context), says this in relation to the expression "large scale":

"The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory."

Applicability

Q32. My clerks and IT staff in chambers are handling all our GDPR compliance. Is there anything I actually need to do specifically as a practising barrister?

Please refer to the extensive guidance available on the Bar Council IT Hub. As a barrister in self-employed practice, you must ensure you comply **personally** with the requirements of the UK GDPR as each self-employed barrister is an individual data controller and should be individually registered with the ICO as such. You cannot delegate the responsibility for data protection compliance in your own individual practice to anyone else, including your clerks, ultimately you are the data controller and it is your responsibility.

Q33. I am an employed barrister. How far does this apply to me – am I still a data controller, and is the GDPR something for my employer to deal with rather than myself?

Generally, your employer will be the data controller, not you. Your employer should have a Data Protection Policy which complies with the GDPR, which you will be required to comply with.

Q34. I am a pupil barrister. What are my obligations?

Your obligations are the same as those for any other self-employed person, though you may undertake a greater proportion of your work as a data processor (for your supervisor or another member of chambers) rather than as a data controller. If you are in your first six or otherwise carrying out work for another member of chambers, you will most likely be considered to be a data processor rather than a data controller in respect of the work you carry out in respect of their clients. As such you will need to sign a data controller/data processor agreement with your pupil supervisor(s) in relation to that work: this will probably be arranged through Chambers at the start of your pupillage. If you are a second/third six pupil it may be that you are an independent data controller, even though you have a pupil supervisor, so you should comply with your obligations as a data controller, seek appropriate training and make sure you are registered as such with the ICO.

Q35. Do Heads of Chambers have specific obligations in relation to data protection?

The Head of Chambers will be a data controller in their own right for the processing of personal data for their own practice. Depending on how your chambers is set up, the Head of Chambers may also be nominated as the Chambers' data controller. This also means that in that latter role, the Head of Chambers will act as a data processor for the other members of chambers using the data processing services supplied by Chambers to the members, for example, where the Head of Chambers rather than a service company employs chambers' staff, or provides facilities such as communications, case management software, or internet, for other members.

Q36. What happens when I move chambers?

When a barrister leaves Chambers, Chambers (as a processor) must, at the choice of the barrister, retain, delete or return all the personal data which relate to the barrister's cases after the end of the provision of services relating to processing, and delete existing copies unless Union or UK law requires storage of the personal data. This will also require that data is deleted from back-up and archive storage media. These requirements should be considered at the time that the controller/processor agreement is agreed between the data

controller, i.e. barrister, and the data processor, i.e. the set of chambers – see Article 28.

A barrister may elect to have all the data moved to their new Chambers for fee collection or may elect to have the former Chambers carry on this task. If the latter, then the former Chambers will need to retain the barrister's personal data (as data controller) as well as the personal data in respect of which the barrister is a data controller (as data processor).

Q37. Are we processing the personal data of instructing solicitors, as well as that of our lay clients?

Yes – see Q3 above.

Q38. What must arbitrators, adjudicators and mediators do to comply with the GDPR?

In common with other businesses and organisations that obtain the personal data of data subjects, arbitrators, adjudicators and mediators are data controllers. They must comply with the UK GDPR and applicable data protection laws (e.g. laws relating to the seat of the arbitration). In general terms, they must comply with similar obligations to the obligations which apply to barristers, as they are data controllers and/or processors depending on the situation. The Guide provided for barristers can be found here.

An important difference between arbitrators/adjudicators/mediators on the one hand and barristers on the other hand is that communications between a party and an arbitrator/adjudicator/mediator are not protected by legal professional privilege. Such persons cannot rely on the exceptions in DPA schedule 2 paragraph 19 relating to (a) information covered by legal professional privilege and (b) "information in respect of which a duty of confidentiality is owed by a professional legal adviser to a client of the adviser".

If you are a barrister and a mediator/arbitrator, you should include these additional purposes (mediation/arbitration) as appropriate on your privacy notice for compliance with Articles. 13 and/or 14 (see Q1 above).

Q39. Would sharing case information informally with colleagues in chambers amount to processing of personal data under the UK GDPR? If so, do barristers need to have controller-processor agreements in place?

Sharing information in chambers even in informal discussion among your colleagues in chambers would amount to processing, where there is a disclosure of personal data. Hence it would be advisable to discuss cases without mentioning personal data, in order that UK GDPR does not apply, you do not break your professional confidentiality obligations and your colleagues would not be placed in a difficult position in future with regard to conflict-of-interest checks.

Q40. How detailed must the barrister's legitimate processing assessment be?

If you are intending to rely on legitimate interests as the lawful ground for processing personal data, you have to conduct a balancing exercise: your legitimate interests must be weighed against the fundamental rights and freedoms of the data subject. GDPR Recital (47) refers to carrying out an assessment when relying on this ground, i.e. you will need to conduct a legitimate interests assessment.

This is a 3-stage test:

- **Purpose test** – is there a legitimate interest behind the processing?
- **Necessity test** – is the processing necessary for that purpose?
- **Balancing test** – is the legitimate interest overridden by the individual's interests, rights or freedoms?

See the ICO's guidance here.

Legitimate interest as a basis may be the most appropriate basis when:

- the processing is not required by law but is of a clear benefit to you or others
- there is a limited privacy impact on the individual
- the individual could reasonably expect you to use their data in that way, and
- you cannot, or do not want to, give the individual full upfront control, i.e. consent.

The legitimate interests basis cannot be relied on in relation to Special Categories personal data (Article 9). If you process such data, you cannot therefore use legitimate interests as the basis for all your processing. None of the lawful bases takes precedence over the others, and you should always rely

on the one that is most appropriate to the circumstances having considered the purpose of the processing.

Accountability is the seventh UK GDPR data protection principle as set out in Article 5(2). This states that the controller shall be responsible for, and be able to demonstrate compliance with, the UK GDPR data protection principles set out in Article 5(1). Despite the fact that legitimate interests is likely to be the most common ground for processing your clients' personal data, it would be prudent to have some form of physical record to demonstrate that you have conducted a genuine legitimate interests assessment. Bear in mind that it is unlikely that you will be able to rely on consent in relation to data subjects who are not your client, without compromising your duty of confidentiality to your client.

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.