General Data Protection Regulation

Bar Council Guide for Barristers and Chambers

Purpose:	To assist barristers and sets of chambers in their compliance with the GDPR
Scope of application:	All barristers and chambers
Issued by:	The Information Technology Panel
Issued on:	October 2017
Last reviewed:	December 2020
Status and effect:	**Please see the notice at the beginning of this document. This is not "guidance" for the purposes of the BSB Handbook I6.4.**

CONTENTS

APPLICABILITY OF THE GENERAL DATA PROTECTION REGULATION TO BARRISTERS AND SETS OF CHAMBERS

Important Notice

This advice has been prepared by the Bar Council to assist barristers on matters of data protection and information security. **It is not "guidance" for the purposes of the BSB Handbook I6.4, and neither the BSB nor bodies regulating data protection and 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 refer to the professional practice and ethics section of the Bar Council's website here.

Cyber attacks are now so common that there is a serious risk of an individual or set of chambers suffering an attack in the coming years. You don't want it to be you. It is important that you read this guidance and associated annexes, and that you take the necessary steps to minimise that risk and to comply with the GDPR. Serious financial penalties are significantly greater than before - a data breach could be very costly and could cause serious reputational damage.

The following Annexes to this Guide provide further assistance in considering your next steps, and are available on the Bar Council website:

- Annex 1 – What you should do next
- Annex 2 – Checklist of some points to consider

- Annex 3 – Extracts from the EDPB and Article 29 Working Party

Introduction

1. The General Data Protection Regulation ("GDPR") came into force in the UK on 25 May 2018. It has also been incorporated into UK law, with some modifications, as the UK GDPR, in the Data Protection Act 2018 ("**DPA 2018"**). By now you should have familiarised yourself with the new requirements and this guide can be used as a reminder and resource.

2. A number of aspects of the GDPR were left to national governments to specify. Schedules 1 to 4 of the DPA 2018 contain additional lawful grounds for processing and a number of exemptions to Articles of the GDPR.[1] This guide cannot cover every issue or detail of GDPR or DPA, but is intended to assist in compliance with the GDPR.

3. It should be noted that only Parts 1 and 2 of DPA 2018 are likely to be relevant to the ordinary practice of a self-employed barrister. Parts 3 and 4, i.e. ss. 29 to 113, apply to processing for law enforcement purposes and processing by the intelligence services.

4. **Every individual self-employed practising barrister is a data controller**. This means that every individual self-employed practising barrister must comply with these requirements. In order to comply with these requirements, individual barristers will need to give careful thought to a number of matters, including the period for which they retain emails and files relating to previous cases. **As a data controller the ultimate responsibility for compliance lies with you. In some situations that responsibility may be shared with the data processor.** This

[1] The ICO has published guidance on the DPA 2018 exemptions, at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/exemptions/.

Guidance is primarily concerned with the role of self-employed practising barristers as data controllers.

5. Each chambers is a data controller in respect of information about the management of chambers e.g. employment and assessment of staff and information about suppliers and marketing activities. Each chambers is very likely to be a data processor as a result of processing being carried out for barristers. There also may be circumstances where barristers carry out processing on behalf of Chambers e.g. management committees and recruitment.

6. Under the GDPR the key concepts and obligations on data controllers (such as barristers) include the following:

   (a) Principle of accountability – data controllers are responsible for, and must be able to demonstrate compliance with, data protection obligations.

   (b) Principle of transparency – personal data must be processed in a transparent manner, with data subjects being notified of processing.

   (c) Data minimisation – there are stricter rules relating to the extent of personal data which is kept, and to the period for which it may be kept.

   (d) Data breach notification – subject to limited exceptions, data breaches must be notified to the supervisory authority and data subjects.

   (e) Right to be forgotten.

   (f) Right of portability – data subjects will be entitled to receive a copy of personal data concerning them or have the data transferred to a third party.

   (g) Data Protection Officers and Data Protection Impact Assessments.

   (h) New liabilities for processors, which will include Chambers when processing information for barristers.

7. The ICO's "Data protection self assessment" check-lists provide a helpful tool for assessing your GDPR compliance. Some other points to check are listed in

Annexes 1 and 2. The Bar Council, the LPMA and the IBC collaborated in the commissioning a service and documentation to assist with barristers' and chambers' GDPR readiness which was notified to sets of Chambers. The ICO has published detailed guidance on the GDPR and DPA 2018, and reference should be made to this for additional guidance.

8. It may be useful (where possible) to ensure that a senior member of Chambers' staff has responsibility for GDPR compliance, both in the preparation for its introduction and once it has come into force. It is best to avoid designating that person as a "Data Protection Officer" unless the person has been formally appointed as a Data Protection Officer, because otherwise they could be deemed to have accepted that they have the necessary qualifications required by the GDPR for the named role, and to have undertaken the responsibilities of a Data Protection Officer as defined in the legislation.

9. The GDPR applies only "*to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*".

10. Information security is important in other areas beyond personal data to which the GDPR apply:

    (a) A barrister's obligation of confidentiality is not limited to personal data. Commercial clients will have an expectation that the barristers they instruct will adopt appropriate measures to protect the information which they disclose to the barrister, in accordance with best practices which prevail from time to time. For these reasons, it is in many respects prudent to treat commercial data in a similar way to personal data. It is possible that a commercial client or a solicitor's firm will want to carry out an information security audit of a set of chambers or a barrister.

(b) Although the GDPR does not usually apply to personal data kept on paper unless contained in a filing system, the security of paper documents is also important. Some reference is made in this guidance to the security of paper documents.

Recent developments

11. On 31 January 2020, the UK ceased to be an EU Member State and in accordance with the EU-UK Withdrawal Agreement (Withdrawal Agreement), entered an implementation period during which UK continues to be subject to EU law. During this period, the GDPR applies in the UK and the UK generally continues to be treated as an EU (and EEA) state for EEA and UK data protection law purposes. Any references to EEA or EU stated in this Guidance should therefore be read to also include the UK until the end of the implementation period.

12. The Withdrawal Agreement states that EU law shall be generally applicable to and in the UK during the implementation period. As such the UK is subject to EU data protection legislation, including the GDPR, until at least 31 December 2020. The Withdrawal Agreement also includes provisions in relation to the processing of personal data that will apply after the implementation period in certain circumstances. At the end of the implementation period the GDPR will be incorporated into the UK's domestic law as the 'UK GDPR' under the regulation-making powers in the European Union (Withdrawal) Act 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (the DPPEC Regulations), SI 2019/419 and certain other Brexit legislation. The UK will also make certain related changes to the DPA 2018.

13. The intention behind the UK GDPR regime is for the fundamental principles, obligations and rights that organisations and data subjects have become familiar with under the EU GDPR to stay the same. By creating the UK GDPR, the DPPEC Regulations will preserve the core EU GDPR standards in UK domestic law such

as the GDPR data protection principles, rights of data subjects and obligations for controllers and processors

14. The Government has indicated that it is committed to maintaining the high standards of the GDPR and that the rules set out in the GDPR will continue to apply to UK data controllers and processors (with minor amendments).

15. In a non-binding Political Declaration that accompanied the Withdrawal Agreement, the EU and UK indicated:

    (a) in view of the importance of data flows and exchanges across the future relationship, the UK and EU are committed to ensuring a high level of personal data protection to facilitate such flows between them.

    (b) the European Commission will start an assessment of whether the UK can be granted an adequacy decision as soon as possible after exit day, endeavouring to adopt decisions by the end of 2020 (if applicable conditions are met) and the UK undertake an equivalent exercise in respect of its own transfer restrictions.

    (c) the future relationship will not affect the UK or EU's autonomy over their respective personal data protection rules.

    (d) the EU and UK should also make arrangements for appropriate co-operation between regulators, slides subsequently issued suggest the European Commission see this as based on Article 50 (International co-operation for the protection of personal data). The slides expressly mentioned:

        i. exchange of information in the context of investigations
        ii. joint investigations
        iii. exchange of best practices, personnel, etc

16. The UK Government asked the European Commission to carry out an adequacy assessment in relation to both the GDPR and the Law Enforcement Directive. There has been no announcement of any decision as of November 2020

17. Barristers and UK businesses with an office, branch or other established presence in the EEA, or with clients in the EEA, will need to comply with both UK and EU data protection regulations after Brexit and may need to designate a representative in the EEA (see ¶204). The ICO has provided guidance on the consequences of Brexit in relation to data protection. This Guidance addresses transfers during the implementation period.

18. The UK government has indicated that after 31 December 2020 the Member States of the EU will be treated as having an adequate level or protection for data subjects. Similarly, all but 1 of the countries which the EU has designated as having an adequate level of protection will be treated by the UK as having an adequate level of protection.[2]

19. The EU has indicated that the UK will become a third country in the event of a "no deal scenario".[3] Accordingly, in those circumstances, the UK will need to obtain an adequacy decision from the EU to maintain data flows. Until that is obtained, if you are receiving data from the EU, the sender will have to make specific arrangements with you to guarantee the adequacy of the protection that your systems provide for data subjects (see the suggested mechanisms in footnote 2).

20. In 2020 the CJEU struck down the EU-US Privacy Shield which enabled transfers of data to signed-up US companies.[4] No provision was made for existing transfers legitimised only on the basis of the Privacy Shield. This is currently causing significant disruption for businesses who wish to transfer personal data,

[2] https://www.gov.uk/guidance/using-personal-data-in-your-business-or-other-organisation-after-the-transition-period?
[3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12-infonote-nodeal-brexit_en.pdf
[4] https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

in particular to the USA. This is addressed in more detail below under Third country transfers (Arts. 44-49).

21. In any event, you will need to check your policy documents and privacy notices to ensure that they reflect the new position.

Definitions and abbreviations

22. Defined terms in the GDPR and used in this document include the following:

    (1) **'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;

    (2) **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

    (3) **'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(4) **'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(5) **'consent'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(6) **'personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(7) **'pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(8) **'data concerning health'** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

(9) **"special categories**" of data (corresponding approximately to "sensitive personal data" in DPA 1998) refers to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

23. The following abbreviations are used:

ICO – Information Commissioner's Office: The current regulator for data processing activities in England and Wales. The ICO will be the UK supervisory authority under the GDPR.

DPO – Data Protection Officer

DPIA – Data Protection Impact Assessment

Art. 29 WP - Art. 29 Working Party: This group was made up of the national data protection commissioners. After the implementation of the GDPR a new body, the EPDB, replaced the Art.29 WP, performing effectively the same function. The EDPB provides guidance on compliance with the Data Protection Directive and the GDPR at the EU level.

DPA 1998 – Data Protection Act 1998.

Types of personal data

24. As noted in the definitions above, 'personal data' means any information relating to an identified or identifiable natural person.

25. More prescriptive requirements apply to certain types of personal data:

    (a) "special categories" of data (under Art. 9, defined above)

    (b) personal data relating to criminal convictions and offences or related security measures referred to in Art. 6(1) (under Art. 10) (**"criminal convictions etc.")**.

Chambers as a data processor

26. DPA 1998 imposed obligations directly only on data controllers. However the GDPR also imposes obligations directly on data processors.

27. It is common for a set of chambers to provide IT facilities for use by or for the benefit of members of chambers, including:

(1) a server for use by individual barristers for storage of files

(2) an email server

(3) a network for accessing those servers

(4) a data connection to the internet

(5) fee, diary and record-keeping software

(6) client relationship software

(7) facilities for record-keeping and document management in relation to chambers management, pupillage, diversity and employment of staff.

28. A set of chambers which operates through a management company will be a data controller in respect of some matters, for example records relating to pupillage, employment of staff and marketing. Other sets of chambers operating under a different model may also be data controllers, depending on the set's formal constitutional arrangements. Alternatively this role may fall to the Head of Chambers on behalf of Chambers. To the extent that the Chambers is a data controller, the set must comply with the obligations which apply to data controllers.

29. As a result of the provision of some or all of the above facilities, many sets of chambers will fall within the definition of a "data processor" set out in ¶22 above. This means that chambers will have obligations as a data processor under Arts. 28 to 33 GDPR, and specific obligations relating to:

(a) record-keeping

(b) breach notification

(c) contractual arrangements with sub-processors, and

(d) (possibly also) appointment of a Data Protection Officer (¶193), and Data Protection Impact Assessments (¶201).

30. Some sets of chambers also arrange (a) IT support to manage chambers servers and to assist members with their own IT equipment, and (b) off-site file storage facilities (including cloud storage).

31. Arts. 28 and 29 deal with processing by a processor on behalf of a controller, so are of particular importance for Chambers processing data for barristers. Reference should be made to the full text of Arts. 28 and 29, but the main points include the following:

(a) Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

(b) The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

(c) Processing by a processor shall be governed by a contract or other legal act which is in writing (including in electronic form) and is binding on the processor with regard to the controller, and sets out specified details of the processing. The terms must include

i. that the processor will process data only on documented instructions from the controller, and

ii. that the processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

iii. that the processor at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless the law requires storage of the personal data.

(d) Where a processor engages another processor to carry out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor shall be imposed on that other processor by way of a contract or other legal act. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations. For example if Chambers uses an IT contractor, and that IT contractor fails to fulfil the data protection obligations, Chambers will be liable for the acts of the IT contractor.

(e) The contract or the other legal act may be based, in whole or in part, on standard contractual clauses.

(f) The processor and any sub-processor shall not process the data except on instructions from the controller, save where the law provides otherwise (Art. 29).

32. In order to comply with Art. 28, a document will be required (on paper or in electronic form) to set out the subject-matter and duration of the processing, the nature and purpose of the processing, the obligations of the controllers and the processor, and other matters referred to in Art. 28.1. This could either be a

contract or a document formally adopted at a chambers meeting. The ICO's expectations of the content of such agreements can be found here.

33. Chambers, in turn, will need to enter into contracts with IT support staff and other service providers (as sub-processors), containing the necessary terms. Each time chambers changes a service provider, chambers must inform barrister members of the change and give barristers an opportunity to object before the change is made. The circumstances in which data is processed on the Chambers Practice Management system will need to be defined so that the barristers are aware of and can control what happens to the data they are responsible for. This can be done in a separate document created potentially during the scoping/audit exercise which has been commissioned to assure compliance.

34. Your Chambers' Practice Management software may have features which make it possible to automate some procedures.

35. When a barrister leaves chambers, chambers (as a processor) must, at the choice of the barrister, 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.

Principles

36. The starting point for any data processing is compliance with the following principles (Art. 5 GDPR). These principles have some similarity to those under DPA 1998 but there are differences and also new concepts:

> 5(1) Personal data shall be:-
>
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Art. 89(1), not be considered to be incompatible with the initial purposes ('**purpose limitation'**);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Art. 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('**storage limitation**');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**').

5(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability**').

LAWFULNESS

Lawfulness: on what basis will processing be lawful?

37. In order to process personal data the processing must be lawful.

38. The GDPR sets out the possible bases for the lawfulness of processing in Art. 6 for ordinary personal data and Art. 9 for personal data in the special categories.

Lawfulness of processing of personal data not in the special categories

39. For personal data which is not in the special categories, at least one of the following bases for processing must be satisfied:

    (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

    (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

    (c) processing is necessary for compliance with a legal obligation to which the controller is subject;

    (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

    (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

    (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by 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.

40. Usually, (a) or (b) will provide the basis for processing of the personal data of clients for whom you are providing legal services, i.e. where you have contact (albeit possibly indirect through your professional client) with the data subject. In order for you to be able to rely on "consent", it must be informed consent and it must be indicated by a clear and affirmative action. Guidance on the meaning of consent under the GDPR has been provided by the ICO and also the CJEU.

41. Consent has, in the past, been used by UK data controllers in practice as either the sole basis for lawful processing or sometimes as a back-up to another lawful processing basis, as it was the easiest condition or mechanism for the data controller to achieve compliance (though it may not always have been the most

appropriate condition for data controllers to rely on). However, if you rely only on consent, you have to be aware that this may cause problems in a number of situations:

(a) Individuals may withhold their consent (although you should indicate in your privacy notice or contractual terms the effect of consent being withheld, e.g. that you will not be able to carry out your instructions without processing the client's personal data, if that is the case).

(b) Your client may decide to change representation and withdraw consent to your processing (Art. 7(3) GDPR). In such circumstances, you would have to rely on (b) and possibly (c) – which can only be satisfied if you, the controller, are under a legal obligation to process the data (e.g. retention for the purpose of satisfying regulations) or (f), for example if you wanted to retain the data for conflict-checking purposes or for use in the defence of potential complaints, legal proceedings or fee disputes.

(c) The reasons for which consent was originally sought and granted may have changed. This would mean that the data controller could no longer rely on the consent originally given.

42. It should be noted that under Art. 7(1) GDPR and Recital 32, data controllers have the burden of proving that consent was obtained. Art. 7(3) provides that the data controller must ensure that it as easy to withdraw consent as it is to grant it, and must inform the client of their right to withdraw consent (as do Arts. 13(2)(c) and 14(2)(d)). In practice this means that consent has to be informed and freely given. Pre-completed check boxes will no longer be effective.

43. In addition, when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. In most cases,

where the services directly concern the client, consent will be necessary for performance, but the purposes for which data is retained after the service has been performed will probably rely on lawful bases other than consent, such as Arts. 6(c) and/or 6(f).

44. A further downside to relying only on consent is that Art. 17 provides data subjects with the right to request erasure of their information (the 'right to be forgotten'), for example where consent has been withdrawn by the data subject (see from ¶95 below).

45. It may often be the case that it is not possible to obtain consent from all of the relevant data subjects and no lawfulness condition can be met. In those circumstances, e.g. disclosure to a mini pupil, the processing cannot be justified and the personal data should not be disclosed. (See the separate Guidance on mini pupils.)

46. If you keep drafts to consult only for research purposes you should consider deleting personal information from those drafts in line with the Data minimisation principle (¶110 below]).

47. Where you do not have contact with the data subject – in particular for the processing of third party personal data, (f) will normally be available unless the processing interferes substantially with the rights of such third parties. If relying on the "legitimate interest" basis it will be necessary to inform data subjects of the legitimate interest relied on, for example, the provision of legal or related services, conflicts, complaints, training of pupils etc. (unless the data is the subject of LPP or other exemptions from notification are applicable (see ¶93 below). It will be necessary to record the lawful basis of the processing, even if you do not disclose this to the data subject, in accordance with the principle of ACCOUNTABILITY. However, be aware that you may not be able to inform third parties of the processing where it is the subject of legal professional privilege or confidentiality obligations to your client.

48. Where the processing is in respect of activities related to your practice but not involving the provision of legal services *per se*, such as assisting pro bono organisations, you will need to consider lawfulness in the context of the purpose of that processing. Depending on the context it may be possible to rely on (e) as the lawful basis of the processing – on the basis that the processing is being carried out in the public interest.

49. In order to comply with the transparency principle (see TRANSPARENCY, from ¶59 below) you have to notify the data subject of the lawful basis of the processing, if a notification is required.

50. The ICO has provided guidance on the meaning of the word "necessary":

> 'Many of the lawful bases for processing depend on the processing being "necessary". This does not mean that processing has to be absolutely essential. However, it must be more than just useful, and more than just standard practice. It must be a targeted and proportionate way of achieving a specific purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means, or by processing less data.
>
> It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is objectively necessary for the stated purpose, not whether it is a necessary part of your chosen methods.'

51. This interpretation is consistent with the approach of the UK Courts to the equivalent term in DPA 1998: see *Cooper v National Crime Agency* [2019] EWCA Civ 16 [89-90] (Sales LJ); and *Aven v Orbis Business Intelligence Ltd* [2020] EWHC 1812 (QB) [66(2)] (Warby J.).

Lawfulness of processing of personal data in the special categories

52. The processing of the special categories of personal data defined in Art. 9(1) (see ¶22(9) above) is prohibited unless one of the following conditions for lawfulness is satisfied : (conditions which are not likely to be relevant have been omitted):

    (a) the data subject has given explicit consent, except where the law provides that consent does not override the prohibition on processing;

    (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

    (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

    (d) […]

    (e) processing relates to personal data which are manifestly made public by the data subject;

    (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

    (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

    (h) […]

    (i) […]

    (j) […].

53. For clients, (a) is likely to be the basis used, especially where litigation is not contemplated, but for third parties it is likely that (f) or (g) may be more

appropriate, although for some proceedings (e) may be appropriate where information has already been disclosed in Court or public documents, if that disclosure has been done by, at the request of or on behalf of the data subject. Ground (f), "the establishment, exercise or defence of a legal claim or whenever a court is acting in a judicial capacity", appears narrower than the related ground applicable to Article 10 (Criminal convictions etc, ¶57 below) as it does not clearly include advice in relation to non-contentious matters not involving a legal "claim". The Bar Council pressed for this to be widened when the Data Protection Bill was going through Parliament, but was unsuccessful. In November 2019 the ICO clarified the meaning of "legal claims" in detailed guidance on Art.9. The latest guidance states that "legal claims" goes beyond actual and prospective court proceedings, but it should be noted that other EU supervisory authorities may take a different view. The ICO Guidance states as follows:

> **"Legal claims**
>
> You must show that the purpose of the processing is to establish, exercise or defend legal claims. 'Legal claims' in this context is not limited to current legal proceedings. It includes processing necessary for:
>
> - actual or prospective court proceedings;
> - obtaining legal advice; or
> - establishing, exercising or defending legal rights in any other way.
>
> **Example**
>
> An employer is being sued by one of its employees following an accident at work. The employer wants to pass the details of the accident to its solicitors to obtain legal advice on its position and potentially to defend the claim. The information about the accident includes details of the individual's injuries, which qualify as health data. The purpose of the disclosure is to establish its legal position and to defend the claim.

Example

A professional trust and estate practitioner advises a client on setting up a trust to provide for a disabled family member. The adviser processes health data of the beneficiary for this purpose. Although there is no active legal claim before the courts, this is still for the purpose of establishing the legal claims of the trust beneficiary for the purposes of this condition.

Example

A hairdresser conducts a patch test on a client to check that they will not have an allergic reaction to a hair dye. The hairdresser records when the test was taken and the results. The hairdresser is therefore processing health data about the client's allergies. Although there is no actual or expected court claim, the purpose is to establish that the hairdresser is fulfilling their duty of care to the client, and to defend against any potential personal injury claims in the event of an adverse reaction.

You must be able to justify why processing of this specific data is 'necessary' to establish, exercise or defend the legal claim. The use of this data must be relevant and proportionate, and you must not have more data than you need.'

54. If (g) is to be relied upon, DPA 2018 (Schedule 1 Part 4) has additional conditions which must be complied with. These are that an appropriate policy document must be in place and, more importantly, the processing must be necessary both for the administration of justice (in this context) as well as for reasons of substantial public interest. You will have to look very carefully at the purpose of the processing to see whether it will fall within the conditions; e.g. submitting a skeleton argument or draft minute to the Court is likely to qualify for (g), but advising on quantum in a divorce settlement might not.

55. Guidance on what is required for explicit consent has been provided by the ICO. In short, explicit consent requires a very clear and specific statement of consent and former practices involving consent by default (e.g. pre-ticked consent boxes) will no longer be considered appropriate (see ¶42 above.)

56. Other reasons for processing may include processing for employment purposes (for staff members), pupil and tenant selection, equality and diversity, and marketing purposes. **For each category, the appropriate basis for processing will need to be identified, recorded and included in your privacy notice.**

Lawfulness of processing of personal data relating to criminal convictions and offences

57. Art. 10 imposes a prohibition on processing data relating to criminal convictions and offences except where permitted under national law. Schedule 1 paragraph 33 of the DPA 2018 permits such data to be processed

"if the processing-

(a) is necessary for the purpose of, or in connection with, any 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."

FAIRNESS

58. This is a highly fact specific assessment. It is not believed that the GDPR has changed the meaning of fairness under DPA 1998, which includes a balance of fairness to the data subject and fairness to the data controller.

TRANSPARENCY

59. Art. 13 sets out the information to be provided where personal data relating to a data subject are collected *from the data subject*. Art. 14, discussed in ¶70 below, deals with personal data which have been obtained otherwise than from the data subject (for example, personal data of the client provided by a solicitor or other agent, or relating to other members of the client's family, witnesses, or individuals on the other side in a case).

60. Art. 13 states as follows:

> '1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
>
> (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
>
> (b) the contact details of the data protection officer, where applicable;
>
> (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
>
> (d) where the processing is based on point (f) of Art. 6(1), the legitimate interests pursued by the controller or by a third party;
>
> (e) the recipients or categories of recipients of the personal data, if any;
>
> (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Art. 46 or 47, or the second subparagraph of Art. 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
>
> 2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
>
> (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
>
> (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
>
> (c) where the processing is based on point (a) of Art. 6(1) or point (a) of Art. 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
>
> (d) the right to lodge a complaint with a supervisory authority;
>
> (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well

as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Art. 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall 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 paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.'

61. Taking into account the exceptions to Art.13 in the DPA 2018 (see (¶74 below), Art. 13 will apply to a barrister carrying out work professionally in at least the following situations:

(a) acceptance of instructions from a new client in a direct access case;

(b) acceptance of new instructions from an existing client in a direct access case;

(c) receiving information from a client directly, e.g. in an email or during a conference.

(d) collecting contact details in order to communicate with another person (such as solicitors, expert witnesses, judges and court staff) by email, SMS message, fax, post, telephone or otherwise.

62. Art. 13 will also apply to a barrister or a set of chambers in at least the following situations:

(a) processing applications for tenancy, pupillage and mini-pupillage

(b) processing applications for employment of a potential member of staff

(c) equality and diversity data

(d) marketing lists.

63. In order to comply with Art. 13, the following information *will always* (or almost always) need to be provided when a barrister accepts instructions from a client (unless the client already has the information):

(a) the identity and the contact details of the barrister;

(b) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing (see LAWFULNESS, from ¶37 above) – the purpose will usually be "to enable me to provide legal services" or "to enable me to act as arbitrator, expert determiner, early neutral evaluator or mediator". However, additional purposes for individual barristers (as opposed to sets of Chambers) are also likely to include "for the purpose of conflict-checking, for use in the defence of potential complaints, legal proceedings or fee disputes, keeping anti-money laundering records, and/or exercising a right to a lien" (in relation to use in connection with complaints see the third example in the ICO Guidance quoted in ¶53 above);

(c) where the processing is based on legitimate interests pursued by the barrister or by a third party (Art. 6(1)(f)), the legitimate interests pursued by the barrister or a third party;

(d) where the processing is based on point (f) of Art. 6(1), the legitimate interests pursued by the controller or by a third party – see LAWFULNESS (¶37 above);

(e) the recipients or categories of recipients of the personal data - this may include:

i. courts and other tribunals to whom documents are presented;

ii. lay and professional clients;

iii. potential witnesses, in particular experts, and friends or family of the data subject;

iv. solicitors, barristers, pupils, mini-pupils and other legal representatives;

v. ombudsmen and regulatory authorities;

vi. current, past or prospective employers;

vii. education and examining bodies;

viii. business associates, professional advisers and trade bodies.

(f) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(g) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(h) where the processing is based on consent of the data subject (Art. 6(1)(a) or Art. 9(2)(a)), the existence of the right to withdraw consent to processing of personal data at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(i) the right to lodge a complaint with a supervisory authority;

(j) in cases where there is a barrister/client contract, the fact that provision of personal data is a contractual requirement, and the fact that the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data, i.e. that the barrister will not be able to provide the legal services.

64. In order to comply with Art. 13, the following information *may* need to be provided, depending on the circumstances, when a barrister accepts instructions

from a client in a direct access case or obtains personal data from a third party such as a witness:

(a) the identity and the contact details of the barrister's representative within the EU; After Brexit, a UK-resident barrister operating across borders may need to have a representative located within the EU, and similarly, an EU-resident barrister will need a UK representative - see Representatives of controllers (¶204 below);

(b) the contact details of the barrister's data protection officer, where applicable (this will rarely, if ever, apply to a barrister, as it is unlikely that a barrister or sets of chambers will need to appoint a DPO – see separate guidance on DPOs (¶193) and DPIA (¶201);

(c) where applicable, the fact that the barrister intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Arts. 46 or 47, or the second subparagraph of Art. 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available – see Third country transfers (¶170 below).

65. At the time when personal data are obtained by the data controller, the data controller must inform the data subject of "the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period" (Art. 13(2)(a)). Recital (39) says this: "In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review".

66. These provisions mean that each barrister will firstly need to consider how much personal data needs to be processed, how much needs to be retained, and for what period it needs to be retained. This may be difficult to assess at the start of

any case when the relevance of information has not yet become apparent. In such cases, it may be sensible to adopt a retention period and system appropriate for any case in which a standard retention period can be fixed and then re-assessed at fixed periods thereafter. The process and retention period may differ depending on the purpose for which the data is retained.

67. The re-assessment procedure which is adopted should ensure that after a given period of time has elapsed, the personal data will be (a) deleted, or (b) reviewed and either deleted or marked for further review after a further period of time. This is discussed in more detail in ¶123 below.

68. It is not anticipated that any barrister is likely to undertake profiling or automated decision-making, but if you or Chambers does so it should be aware that additional obligations apply to such processing.

69. Where the barrister intends to further process the personal data for a purpose other than that for which the personal data were collected, the barrister must provide the data subject, prior to that further processing, with information on that other purpose and with any relevant further information of the kind referred to in Art. 13(2).

70. Art. 14 deals with personal data obtained otherwise than from the data subject (for example personal data of a client obtained from a solicitor or other instructing agent or relating to other members of the client's family, witnesses, or individuals on the other side in a case).

71. Subject to an important exception in Art. 14(5)(b), Art. 14 requires the data controller to provide to the data subject similar information to that referred to in Art. 13:

    (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

72. The main reason for Art. 14 is presumably to deal with the situation where personal data is transferred in bulk from one data controller to another with a view to exploitation for commercial purposes. However the language of Art. 14 is wide enough to apply to barristers receiving personal data of individuals indirectly. This may include personal data of the client obtained from a solicitor or other instructing agent or of the lay client's family members, witnesses or individuals on the other side in a case.

73. Art. 14(5) contains limitations on Art. 14 as follows:

> 'Paragraphs 1 to 4 [of Art. 14] shall not apply where and insofar as:
>
> (a) the data subject already has the information;
>
> (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Art. 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
>
> (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
>
> (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.'

74. The DPA 2018 (Schedule 2 paragraph 19) restricts the operation of Arts. 13 to 15 GDPR (and the general principles of Art. 5) where the personal data "consists of

information in respect of which a claim to legal professional privilege … could be maintained in legal proceedings" and in relation to "information in respect of which a duty of confidentiality is owed by a professional legal adviser to a client of the adviser". This will in many cases make it unnecessary to comply with Art. 13 for third parties and Art. 14, in particular where the data relates to an individual who is involved in a case on the opposing side. However, it will be necessary for the information required by Arts.13 and 14 to be passed on to the lay client, usually via the professional client.

75. Sub-paragraph (d) of Art. 14(5) will apply to the personal data of persons other than a lay client in most cases where a barrister is provided with personal data in the course of providing legal services, as the Code of Conduct requires barristers to keep information confidential, and the information must be kept confidential in order to protect the client's right to legal professional privilege. In this situation an Art. 14 notification will not be required for such persons.

76. Sub-paragraph (d) will not apply to witness statements and other documents for use in court if they are not or are no longer confidential, for example pleadings which have been served or witness statements of witnesses which have been referred to in open court. For documents of this kind it is necessary to consider sub-paragraph (b). The DPA 2018 contains nothing to alter the position on this point.

77. It might be reasonable to take the view that it would involve disproportionate effort for a barrister to notify every data subject mentioned in a disclosed document that the barrister is in receipt of their personal data, especially if this notification has already been carried out by the instructing agent. In many situations the barrister will not have contact details for the data subject.

78. In appropriate cases, the data minimisation requirement may require that an application be made under CPR 31.22(2) for an order restricting or prohibiting the use of a document which has been disclosed under CPR Part 31 and read by

the court or referred to at a public hearing. However, there are some circumstances where protection from disclosure is not justified – as in *Khuja v Times Newspapers* [2017] UKSC 49.

79. Where a barrister obtains personal data indirectly (e.g. not in relation to the provision of legal services), the position will depend on the circumstances. For example, if a potential employee has identified a third party to provide a reference, the reference will contain personal data obtained indirectly about the potential employee. In those circumstances, it seems likely that the Art. 14 obligations will apply.

80. Barristers will need to form their own view as to the application of Art. 14(5)(b) and (d). If the barrister decides that notification would involve disproportionate effort, it would be sensible to record the reasons for so deciding (this is consistent with the principles of Accountability and Transparency).

81. If you decide that notification would involve disproportionate effort, you will still need to comply with the final sentence of Art. 14(5)(b). This requires appropriate measures to be taken protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available. This could be dealt with by displaying a privacy notice on your or your chambers' website. This notice will need, amongst other things, to state the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

Privacy Notices

82. Chambers and barristers privacy notices should already have been updated to comply with the requirements of the GDPR.

83. Art. 12 requires the controller to take appropriate measures to provide any information referred to in Arts. 13 and 14 and any communication under Arts. 15 to 22 and 34 relating to processing to the data subject in a concise, transparent,

intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. This should in particular be noted by barristers who hold personal data relating to children.

84. Privacy notices will be required in the following contexts, providing the information required by Arts. 13 and 14:

(a) to clients on the acceptance of instructions, including, in particular, direct access clients who will not also be instructing a solicitor – this will need to include a reference to using material in the course of proceedings, whether by service on opposing parties, filing in court, or otherwise;

(b) to the public, on the chambers' web site or the barrister's own website, informing clients, data subjects other than clients (including anyone who communicates with a barrister by electronic means such as email, SMS message, and twitter, such as solicitors, expert witnesses, judges and court staff);

(c) to candidates for tenancy, pupillage and mini-pupillage;

(d) to applicants for positions as an employee;

(e) to users of the chambers web site or a barrister's own website.

85. The ICO has provided guidance on privacy notices generally, and the additional information required under the GDPR.

Contractual Terms for clients

86. It is strongly desirable for Data Controllers (barristers) to include in their contractual terms of engagement with instructing solicitors, international lawyers and lay clients a mechanism by which explicit consent is obtained to processing and/or by which a client provides confirmation that it has obtained any necessary consents in relation to personal data it supplies, in addition to relying on one of the other lawful processing conditions under Art. 6(1) or Art.

9(2) see ¶¶40 to 46 and 56 above. Some solicitors have requested barristers and sets of Chambers to enter into agreements which describe barristers as data processors. This is almost always not appropriate as part of a barrister's normal practice, and the Bar Council and the Law Society have published guidance on this point.

87. Where the lay client is instructing via professional clients, such consent will need to be obtained indirectly.

88. As obtaining and retaining consent may be problematic it will be prudent for data controllers to consider whether another lawful basis for processing (such as Art. 6(1) (b), (c) or (f)) would be more appropriate to rely on in any particular case, in addition to obtaining explicit consent under the contractual terms of engagement. Where you have a pupil or plan to use a devil, it is necessary to inform the client of the fact that disclosure is likely to take place, but you should give the client the option to refuse, as this is their confidential information.

89. In addition, it will be necessary to amend privacy notices which are referred to in the contract terms to comply with the GDPR, in particular, to provide the information required by Arts. 13 and 14 as described above from ¶59.

Rights of Data Subjects[5]

Subject Access Requests (Art. 15)

90. Subject to questions of Legal Professional Privilege (considered in ¶92 below), this is covered by a separate detailed guidance document.

[5] These refer to the rights which fall within TRANSPARENCY. Additionally, data subjects have rights to rectification and restriction of processing which are addressed under ACCURACY from ¶130).

91. As with all data subject rights (Arts. 15 - 22), the time limit for responding is 1 month, although an extension of up to 2 further months may be available depending on the complexity or number of requests. Within 1 month you have to respond providing information on what action has been taken in response to the request or notify the data subject that the period has been extended with the reasons for the delay. There have been cases of Subject Access Requests being made by impostors, so it is important to verify that the request has been made by or with the authority of the data subject – see the separate guidance document here.

Legal professional privilege and third party sources

92. DPA 1998 expressly exempted personal data which is covered by legal professional privilege from the data to be provided pursuant to a section 7 subject access request (DPA 1998, Schedule 7, paragraph 10). The ICO recognised that personal data was exempted from the right of subject access if it consisted of information for which legal professional privilege (or its Scottish equivalent) could be claimed in legal proceedings in any part of the UK.

93. There is no equivalent express exemption in the GDPR, though Art. 15(4) states that the right to obtain a copy of personal data under Art. 15(3) shall not adversely affect the rights and freedoms of others. Schedule 2, Part 4, para, 19 DPA 2018 contains an exemption from parts of Arts. 13, 14 and 15 for personal data to which LPP applies. Sch. 2 Part 3 para. 16 also includes an exemption from Arts. 15(1)-(3) where disclosure would involve disclosing information relating to another individual. This appears to be very similar to the provisions of s. 7 DPA 1998.

94. It could happen that in the course of exercising its enforcement powers the ICO obtains material which is covered by LPP. Page 22 of its Regulatory Action Policy states that the ICO does not require access to such material. However page 18

states the opposite. The context suggests that page 18 should say "We do **not** require access to …". This was raised with the ICO in 2019, and it was indicated that this would be addressed in Spring 2020. An update is awaited.

Right of erasure = right to be forgotten (Art. 17)

95. You may have heard of the existence of this right or have seen references to it in the results of Google searches.

96. This right enables a data subject to have the information held about them erased in particular circumstances. The most relevant limitation on the exercise of this right is that it does not apply where processing is necessary for the establishment, exercise or defence of legal claims. This means that if a witness or the other party seeks to exercise this right as a tactic during proceedings, it can be refused. See ¶53 above on the meaning of "the establishment, exercise or defence of legal claims".

97. It can only be exercised if:

(a) the personal data are no longer necessary for the purpose for which they were collected or processed

(b) the data subject withdraws consent and there is no other legal ground for the processing;

(c) the data subject objects to automated processing - this is not likely to be relevant to barristers or Chambers

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services to a child (this too is unlikely to apply to processing by a barristers or Chambers).

98. It also does not apply to the extent that processing is necessary for:

(a) exercising the right of freedom of expression and information;

(b) compliance with a legal obligation under Union or Member State law to which the controller is subject which requires the processing, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) reasons of public interest in preventative health or occupational medicine;

(d) archiving or scientific or historical research or statistical purposes in the public interest;

(e) for the establishment, exercise or defence of legal claims.

99. If the data have been made public and the controller is obliged to erase the data, then the controller must take proportionate measures to inform other controller of the data subject's request to erase that data.

100. Deleting data from backups raises complications. The ICO's guidance on the right of erasure says this:

> 'You must be absolutely clear with individuals as to what will happen to their data when their erasure request is fulfilled, including in respect of backup systems.
>
> It may be that the erasure request can be instantly fulfilled in respect of live systems, but that the data will remain within the backup environment for a certain period of time until it is overwritten.
>
> The key issue is to put the backup data 'beyond use', even if it cannot be immediately overwritten. You must ensure that you do not use the data within the backup for any other purpose, i.e. that the backup is simply held on your systems until it is replaced in line with an established schedule. Provided this is the case it may be unlikely that the retention of personal data within the backup would pose a significant risk, although this will be context specific. For more information on what we mean by 'putting data beyond use' see our old guidance under the 1998 Act on deleting personal data (this will be updated in due course).'

Right to data portability Art. 20

101. This new right enables a data subject to receive or have transmitted to a third party their personal data in a structured commonly used and machine-readable format in certain situations. This will usually apply where a data subject wants to transfer their case to a new representative. It does not create an obligation for controllers to adopt or maintain processing systems which are technically compatible with other controllers.

102. It only applies where:

(a) the processing is based on consent or on a contract; and

(b) the processing is carried out by automated means.

103. The exercise of the right is without prejudice to the Right to be forgotten (¶95 above.

104. It does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (see Art. 20(3) and Recital 68 GDPR).

105. The exercise of this right also has to be balanced against the rights of others under the GDPR. The effect of this is that if the right applied, the transmitted data would have to be modified (e.g. redacted) to remove references to third parties to avoid disclosing their data.

106. The initial time limit for responding is 1 month, as described in ¶91 above, although an extension of up to 2 further months may be available depending on the complexity or number of requests. Within 1 month you have to respond providing information on what action has been taken in response to the request or notify the data subject that the period has been extended with the reasons for the delay.

PURPOSE LIMITATION

107. This principle requires that data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

108. Under DPA 1998 a data controller had to notify the purposes for which they were processing data to the ICO, which information was placed on a register, and that register was accessible to the public. Through that mechanism registered data controllers discharged the obligation to disclose the purposes of their processing. This mechanism is no longer in place. Notification of such purposes is now carried out by the data controller serving notices under Arts. 13 and 14, or possibly by means of accessible privacy notices on websites.

109. However, the principle of purpose limitation remains. You can only process data for specific, legitimate, identified purposes and you are required to identify those purposes to data subjects. (See LAWFULNESS, from ¶37 above, for legitimacy of purposes and TRANSPARENCY, from ¶59, for the form of notifications).

DATA MINIMISATION AND STORAGE LIMITATION (Art. 25)

110. Art. 25 deals with steps to be taken to minimise the amount of data which is used and stored:

> "1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

> 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

111. This requires additional steps to be taken where it is appropriate and feasible to do so, having regard to the state-of-the-art and the cost of implementation. Such steps may include in current proceedings pseudonymising third party data, and in historical cases data minimisation (that is to say taking steps to minimise the amount of data being stored) e.g. removing as data as soon as possible once the proceedings have concluded and the data are no longer required for conflict checking purposes, or to respond to a potential complaint. For example, in a case concerning clinical negligence where the names of patients other than the client are not relevant it may be necessary to anonymise the names of other patients who have undergone a similar procedure, by replacing their names with identifying codes such as A1, A2. It should be possible to arrange that solicitors carry out this task before providing the documents to barristers, as this is consistent with their data protection obligations under GDPR. If however, the case is taken on a direct access basis then it may be necessary for the barrister to carry out this task, which will need to be factored into any costs estimates.

112. Art. 25.2 expressly requires data controllers to ensure that *by default* only personal data which are necessary for each specific purpose of the processing are processed, and states that this obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

113. The words "by default" imply that some steps will need to take place routinely without needing to be initiated by the data controller on each occasion. This is

likely to be onerous without appropriate tools or processes, and is considered further below.

114. Personal data which is kept in a form which permits identification of the data subject must not be kept for longer than is necessary for the purpose for which the personal data are processed (Art. 5(e)). Accordingly, it is unlikely to be justifiable to keep *all* personal data *indefinitely*.

115. Individual barristers will need to consider what data they need to retain for the purpose of their own practice, and should record their conclusions in a data retention policy. Also, in order to comply with Art. 13(2)(a), barristers must when accepting instructions inform clients and other data subjects of the period for which personal data will be stored, or if that is not possible, the criteria used to determine that period. The guidance in ¶124 below may be helpful.

116. For case files in civil matters it is likely that a barrister will need to keep personal data for at least a year after the maximum relevant limitation period measured from a defined endpoint, for the purpose of defending or taking legal action.[6] Some possible endpoints are the latest of the end of all appeal periods for a case or the date of the last payment or the date or writing off fees on the case. Bear in mind that a limitation period may exceed (or be alleged to exceed) 6 years, for example where the facts relating to the negligence were not known to the claimant, where a claim is made by a person who has been liable for a claim to contribution, where minors or other persons who lack capacity are involved, or where fraud is alleged. In criminal cases, it may be relevant to consider the

[6] The ICO's guidance on International Transfers considers the meaning of "legal claims" (quoted at ¶53 As with all data subject rights (Arts. 15 - 22), the time limit for responding is 1 month, although an extension of up to 2 further months may be available depending on the complexity or number of requests. Within 1 month you have to respond providing information on what action has been taken in response to the request or notify the data subject that the period has been extended with the reasons for the delay.). It says "You cannot rely on this exception if there is only the mere possibility that a legal claim or other formal proceedings may be brought in the future." It is arguable that "legal claims" has a wider meaning in the context of Art.9 than in the context of Art.49.

possibility of an appeal out of time or the period of imprisonment for any convicted defendant.

117. BMIF set out its approach to document retention in its Chairman's report dated 26 July 2018. It would be appropriate for barristers to take this into account in deciding how long documents should be retained for, but there may be other considerations which should also be taken into account.

> 'The question of retention of documents and information is very important in the context of claims against Members. All Members know from their own practices that contemporaneous documents or information will almost always be regarded as the best evidence of what happened, and of people's motivations, in the past and will normally be preferred over oral witness evidence on the relevant issue. This applies just as much to claims against barristers. The availability of such documents and information is of invaluable assistance to the Managers and those lawyers instructed to defend Members as they evaluate the merits of claims and determine how best to safeguard the interests of both the Member subject to any particular claim and Bar Mutual.
>
> As such, Bar Mutual believes that Members should be treated as having good reason to retain such documents and information. With this in mind, I would urge Members to continue to retain notebooks and (as regards documents that are more likely to be retained in soft copy) emails and, importantly, their attachments, attendance notes and documents they have drafted and to do so for at least fifteen years (which is the long-stop limitation period under section 14B of the Limitation Act 1980). Those whose practice involves infants and protected parties (in particular, those acting for claimants in catastrophic personal injury disputes) should consider adopting an even longer retention period.'[7]

118. You should seek to limit the personal data you retain beyond the limitation period to data which can be retained for an objectively justifiable legitimate interest.

119. Barristers may wish to retain emails and other files in order to:

---

7 https://www.barmutual.co.uk/fileadmin/uploads/barmutual/2018_documents/BMIF_s_Chairman_s_Report_-_July_2018.pdf

(a) refer back to them in future cases which raise similar legal, factual or procedural issues;

(b) carry out conflict checks in future cases - the extent to which this requires the retention of personal data will depend on the nature of your practice; and

(c) keep records of money-laundering checks.

120. It may be possible to achieve these purposes without retaining the entirety of emails and other files. Attachment to emails, which may include instructions, witness statements and correspondence and could contain a great deal of personal data should be stored separately in the relevant case folder. This will enable you to manage and find information more easily, should you receive a subject access request or when assessing the data retention timescales for files.

121. Arts. 5(1)(e) and 25.1 require that personal data is retained only when there is a necessity to retain that personal data. Necessity in this sense means "proportional to the need". Where documents are retained only as precedents e.g. opinions, pleadings etc. the names could be removed. For the future you may want to consider using defined terms which can easily be searched for, and removed as part of the suggested retention process which is described in ¶124 below.

122. Procedures will be required both (a) to assist barristers in deleting the data which they store themselves and (b) for deleting personal data (including briefs and advices) stored on the Chambers Practice Management system. These points are being discussed with the suppliers. In the latter case there are complications where more than one barrister in Chambers has been instructed on a case. Such procedures should be recorded in a policy document so that it is clear not only to barristers and Chambers but also in the event that the ICO assesses the processing in the course of an investigation.

123. Barristers conducting direct access work or giving advice on transactions may have to retain records for money-laundering checks. It is best to keep these in separate files. These records must be kept for five years beginning from the date a business relationship ends, and also from the date a transaction is completed.

124. There are some practical steps which can be taken which make it easier to implement a procedure for reviewing/erasing data.

(a) Consider what data and documents you will need to retain and the reason why you need to retain them. Think about how you will store files in a manner which makes it possible and easy to delete data which you do not need to retain.

(b) It would be sensible to organise your work (including emails, advices, drafts, instructions and other documents) into case-specific sub-folders and to ensure, so far as possible, that emails for cases do not contain substantive advice, but rather that substantive advice is stored separately. The following folder structure could be helpful in order to facilitate the deletion of emails, while retaining the core case documents which you may need to retain for conflict checking:

(i) "work"

(ii) the year in which instructions were first received

(iii) either "special" or "other", in order to distinguish cases involving personal data involving special categories of personal data or criminal conviction etc.,

(iv) the name of the client or matter.[8]

(c) Any emails or files which the barrister may wish to retain, because they record the results of time-consuming legal research or for other reasons,

[8] For example: "Inbox/Work/Year/Special/*NameOfClient*"

should be redacted as to the identifying details of the data subjects and can then be stored separately. This process will be simplified if you keep it in mind when preparing your advice – think about structuring the advice in a manner which facilitates the redaction of personal data.

(d) When instructions are accepted, a period of time should be recorded as the initial retention period for that matter. That period is likely to vary depending on the nature of a practice but is unlikely to be less than the maximum limitation period for any claim made in respect of work done on that case. Precisely identifying when the period should start is difficult, but it is suggested that the period should date from the latest of

(i) the date on which the last item of work is recorded as having been carried out,

(ii) the date on which the fees have become fully paid, and

(iii) the date on which the last amount of fees was written off.

These dates may correspond to the date when a case is marked as 'Closed' on the Chambers Practice Management system. The period up to the review date is referred to as the "retention period".

(e) The client (or other data subject) can be told that the retention period will be reviewed when the work has been completed and the retention period may be adjusted at that time, and that personal data will be retained for at least the retention period.

(f) At the end of the period the barrister will review the data held for the case. Personal data will be deleted or minimised, or (if there is good reason for doing so) a further retention period will be designated and recorded.

(g) A procedure will be required for recording retention periods and triggering a review by the barrister at the end of the retention period. This function

could be automatically added to Chambers practice management software or at least to the Chamber's case entry process. At the end of the retention period the software will flag up the need to review the retention period. A log of the date when the review is completed should also be maintained for the purpose of demonstrating compliance with the retention review protocol.

125. It may be advisable to have and use a separate email account for personal emails and for logging on to websites for non-professional purposes. Amongst other things, this will make it easier to delete emails of more than a certain age without also deleting personal emails.

126. Quite apart from express regulatory requirements, there are practical reasons for not retaining data from old cases indefinitely:

(a) It considerably reduces the impact in the event of a data breach, for example following an intrusion as a result of opening a phishing email or ransomware attack. No barrister or set of chambers wants to be famous as the barrister or set of chambers whose data is leaked.

(b) In the event of a data breach, the fact that excessive data has been retained, and therefore put at risk, is a factor which the ICO can take into account when considering whether to impose a fine and the amount of that fine.

(c) In the event of a data breach, there will be many fewer data subjects who may need to be notified (see ¶167).

(d) It is easier to find specific data in response to a subject access request or when searching for data for other purposes.

(e) It reduces the amount of data storage space required, which means that systems are likely to operate more efficiently.

(f) If data is retained for a very long period it is more likely to be inaccurate and out of date, which exposes you to risks of data subjects making

applications for correction of data, restriction of processing or erasure of data.

127. If you do decide that you need to keep personal data from old cases for a long period, it is important to keep it in an encrypted form (or another equally secure form), both as a security precaution and in order to benefit from the exemption in Art. 34(3)(a) from the requirement to notify data subjects in the event of a data breach (see ¶167 below). In order to be sure that the data cannot be accessed by a hacker, the encrypted data needs to be kept encrypted at all times except when the data is being accessed. If the data is kept in a folder which is kept unlocked all the time when the computer is being used, there is risk that the unencrypted data may be accessible to a hacker.

128. Further information on points to take into account when preparing a data retention policy (including points to have in mind when assessing an appropriate retention period), and in relation to measures for safeguarding data from previous cases is available in the Bar Council IT Panel's document dealing with this point [link]

129. The procedure for deleting personal data will need to include deletion of personal data of clients and others from devices used by pupils or members of staff at the time when they leave chambers. See the draft Bring Your Own Device policy [link], which you will need to adapt for your own circumstances.

ACCURACY

Right to rectification and restriction of processing (Arts. 16, 18, 19)

130. As under DPA 1998, a data subject has the right to have inaccurate data held by a data controller, rectified without delay. Where it is incomplete the data subject may have it completed by adding a supplementary statement.

131. Similarly, a data subject can seek a restriction on a data controller's processing of their information (not including storage) in limited circumstances:

(a) where the accuracy of the data is contested – for a period which enables the controller to verify its accuracy;

(b) where the processing is unlawful (e.g. consent has been withdrawn and there is no other lawful basis for retaining the data);

(c) where the controller no longer needs the data but the data subject requires it for the establishment, exercise or defence of legal claims (-see ¶53 above on the meaning of "legal claims");

(d) in some circumstances where there has been an objection to automated decision making – but this is unlikely to be relevant to processing likely to be carried out by a barrister or Chambers.

132. Where processing has been restricted:

(a) a controller must inform a data subject before a restriction is lifted;

(b) processing must only be carried out with the consent of the data subject or for the establishment, exercise or defence of legal claims or for the protection of a third party's rights or where it is in the important public interest of the EU or a member state.

133. Where there has been rectification or a restriction or erasure of data, the controller is required to communicate that fact to recipients unless it is impossible or involves disproportionate effort. The controller is also required to inform the data subject about those recipients at the data subject's request.

INTEGRITY AND CONFIDENTIALITY

134. Arts. 24, 28, 29 and 32 set out a number of obligations dealing with the integrity and confidentiality of data. Arts. 28-29 are addressed in Chambers as a data processor, see from ¶26 above.

135. Art. 24 – Responsibility of the Controller:

> '1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
>
> 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.'

136. Art. 24.1 imposes obligations on individual barristers as a data controller (a) in relation to the processing they carry out in their own practice and (b) in relation to matters affecting them as a member of chambers, for example where there is collective provision of IT facilities (email, server storage, network, internet), fees and diary software, client relationship software, pupillage, diversity, and employment records for staff by Chambers.

137. Chambers which provide network, internet, email and file storage facilities for their members will be acting as data processors for that data as well as operating as data controllers in their own right. As data processors, Chambers will need to adopt appropriate security precautions and other procedures in order to comply with Art. 32 (see from ¶147 below).

138. As well as the personal responsibility for their own processing, an individual barrister may also be held personally responsible for a failure by Chambers staff to adopt proper precautions, including IT support staff, in their role as a data processor of the personal data for which the barrister is a data controller. Non-compliance does not require negligence on the part of the individual barrister. However the degree of responsibility of the individual barrister will be one of the factors which determines the level of any financial penalty or other remedial measures imposed (see the discussion of Fines (Arts. 83-84) from ¶206 below).

139. The level of precautions required depends on the circumstances. A higher level of security is required where there is a greater probability and risk of severity of harm. For example, a greater level of security will be required for an email setting out details relating to a client's health or previous convictions or confidential information than an email confirming the time of a court hearing.

140. Where proportionate to the processing activities, it will be mandatory to implement an appropriate Information Security policy: see Art.24.2. This will require the development and adoption of an appropriate Information Security policy, if the policy you are currently using does not comply with GDPR. The Bar Council's recommendations [link] can be used as a starting-point, but may need to be supplemented by additional requirements in order to meet the particular circumstances of individual barristers and sets of chambers.

141. The measures adopted should be reviewed and updated periodically or when the circumstances of the processing materially change, e.g. where a new IT system is implemented which materially alters the circumstances such as the introduction of a cloud solution.

142. Art. 24.3 provides that the adherence to approved codes of conduct may be used as an element by which to demonstrate compliance. The Bar Council's recommendations on Information Security do not amount to an approved code of conduct, but may be of assistance in demonstrating compliance. Failure to comply with the guidance may be taken into account as an aggravating factor by the ICO in the case of a personal data breach and in the assessment of whether to apply a monetary penalty and the amount of that penalty.

143. There are also a number of international IT security standards, such as those based on FIPS 800-53 (published by NIST) and those based on ISO 27000 or ISO 20001. They may not be wholly appropriate for individual barristers or small sets, but larger chambers may wish to consider whether to follow such an

international standard as assisting in demonstrating compliance. More detailed guidance is available in the CCBE Guidance paper.[9]

144. Individual barristers will typically make use of a number of data processors to enable them to manage their practice. These will include the set of chambers to which the barrister belongs and in many cases will also include email and cloud storage service providers.

145. Art. 28 sets out the requirements for formal arrangements between data controllers and data processors, and has been dealt with under Chambers as a data processor (¶12). These requirements will also apply to other data processors used by individual barristers and by sets of chambers. Don't forget that first six pupils (and second six to the extent that they are not working on their own cases) and devils are also data processors. It would be sensible to have a pro forma processing agreement for use with pupils and devils – see also the separate guidance on devilling [link].

146. As stated in ¶31 above, barristers and chambers may only use providers (including cloud storage providers) whose terms contain obligations (a) only to process personal data on documented instructions of the controller, and (b) to delete personal data after the end of provision of services. It is not advisable to use services where data is analysed by the service provider's servers, and retained indefinitely, for the purpose of displaying targeted advertising (such as Gmail). The terms of some mass-market cloud storage providers may also not be

9 http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommentations/EN_ITL_20160520_CCBE_Guidance_on_Improving_the_IT_Security_of_Lawyers_Against_Unlawful_Surveillance.pdf

consistent with this obligation (particularly if they are US-based or owned by US entities)[10].

147. Art. 32 - Security of processing

> "1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
>
> (a) the pseudonymisation and encryption of personal data;
>
> (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
>
> (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
>
> (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
>
> 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

148. Art. 32 provides greater detail about mechanisms which can increase the security of the data processed. It begins by stating explicitly that technical and organisational measures must be appropriate for ensuring a level of security appropriate to the risk and the cost.

149. In relation to their own practices, individual barristers should consider, and where appropriate, comply with the Bar Council's recommendations for Information Security [link]. These recommendations deal with many of the

[10] The export of any work-related personal data to a US organisation can no longer be justified by reliance on Privacy Shield, the approval for which was struck down by the CJEU.

matters set out in Art. 32 - such as password security, encryption of data, keeping backups, antivirus, firewall, keeping operating systems up-to-date, disposal of hard disk drives, cloud storage, cross-border transfers, and handling of hard copy papers.

150. The following techniques may be used to improve security of systems, in order to comply with Art. 32:

(a) password-protected access to devices and the IT network, using strong passwords and password managers, ;

(b) pseudonymising personal data (e.g. personal data to be referred to in open court);

(c) encrypting data on smartphones, tablets, portable storage devices and laptops (recommended, where practicable, in the Bar Council's existing guidance);

(d) depending on the nature and amount of the personal data stored and the physical security of the location, encrypting desktops in chambers, desktops at home, servers, and files stored off-site;

(e) secure disposal of redundant hard disk drives and other storage devices;

(f) using up-to-date anti-virus software and firewalls, and applying operating system updates;

(g) policies and procedures for the use of personally-owned devices by pupils and staff, including deletion of data when they leave chambers (known as BYOD – "bring your own device") – see the Bar Council's draft BYOD policy [link];

(h) depending on the nature and amount of the personal data stored and any specific instructions of clients, using encrypted email for sensitive data,

and/or sending links to encrypted files stored in the cloud instead of sending attachments – see guidance on cloud storage [link];

(i) when making back-ups of data, using facilities which would not be at risk in the event of a ransomware attack: synchronised folders, whether on- or off-site, may be as much at risk as local folders, so it is best to use storage media which are not permanently connected to the internet, or off-site and/or offline storage facilities which allow access to previous uncorrupted versions of data;

(j) minimising the risk of a ransomware or other attacks, and the consequences of such attacks, (for example by regular information security training of barristers and staff);

(k) procedures providing for regular auditing of facilities, equipment and procedures;

(l) policies and procedures for the use of fax;

(m) policies and procedures for hard copy papers.

A non-exhaustive checklist of some of the matters to be considered is attached as Annex 2.

151. Sch. 2 paragraph 5 of the DPA 2018 contains an exemption permitting personal data to be *disclosed* for the purpose of or in connection with legal proceedings, for the purpose of obtaining legal advice or otherwise establishing, exercising or defending legal rights (to the extent that disclosure would otherwise not be permitted). This is similar to DPA 1998 s. 35. It has a limited scope as it applies only to *disclosure* which is necessary.

ACCOUNTABILITY

152. Art. 24 places a personal responsibility on every data controller to ensure that appropriate technical and organisational measures are implemented and also includes an additional requirement to document their compliance.

153. The obligation to document compliance is a new obligation in the GDPR.

Record-keeping (Art. 30)

154. Art. 30 contains detailed requirements relating to record-keeping. These do not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Art. 9(1) or personal data relating to criminal convictions and offences referred to in Art. 10.

155. Many barristers will be exempt from the requirement to keep records because of the 250 employee exception. However some barristers may be required to keep records in accordance with Art. 30 because they regularly process either data within the special categories or criminal convictions. Barristers should form their own view or obtain specialist advice.

156. Whether this applies to your processing may depend on the nature of your practice – criminal barristers and chambers are likely to be processing data relating criminal convictions etc.; barristers who practice in criminal, family, medical negligence and/or personal injury may process data in the special categories (see Definitions and abbreviations, ¶22 above), as this covers data about health. Employment barristers may process data about trade union membership.

157. If a barrister's processing does fall within Art. 30 then their Chambers will also have to keep records appropriate to a processor as set out in ¶154 above.

158. Chambers' record-keeping would need to cover only the processing activities it carries out for its barristers, as opposed to the processing activities carried out by individual barristers which do not use Chamber's processing (e.g. storage of data on a personally owned home computer, storage of data in the cloud by an individual barrister using the barrister's own cloud storage account or personal email account).

159. In cases where Art. 30 does not require record-keeping, it will still be helpful to have records of some activities in order to be able to demonstrate compliance in accordance with Art. 24.1. Points which it would be helpful for individual barristers to be able to support with evidence include:

(a) adoption and implementation of a data retention policy – this will require a copy of the policy itself, and a record of the date of its adoption;

(b) details of any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken (Art.33.4).

(c) the dates on which personal data is reviewed and deleted, and the reasons for deciding to retain personal data after the initial retention period;

(d) a copy of all privacy notices and a record of their review dates;

(e) a list of the recipients (or classes of recipients) of a data subject's personal data (in order to be able to comply with a Subject Access Request and Art. 15(1)(c), and with Art. 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing);

(f) the reason for deciding not to provide a data protection notification under Art. 14 (¶¶73 to 77 above);

(g) confirmation of the secure disposal of a hard disk drive or other storage device containing data, and the method of disposal used;

(h) participation in information security training - depending on your CPD plan this may count towards your CPD.

160. If Art. 30 does apply the **controller** has to record the following information in writing, which can be in electronic form:

> '(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
> (b) the purposes of the processing;
> (c) a description of the categories of data subjects and of the categories of personal data;
> (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
> (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Art. 49(1), the documentation of suitable safeguards;
> (f) where possible, the envisaged time limits for erasure of the different categories of data;
> (g) where possible, a general description of the technical and organisational security measures referred to in Art. 32(1).'

161. If Art. 30 does apply the **processor** has to record the following information in writing, which can be in electronic form:

> '(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
> (b) the categories of processing carried out on behalf of each controller;
> (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Art. 49(1), the documentation of suitable safeguards;
> (d) where possible, a general description of the technical and organisational security measures referred to in Art. 32(1).'

162. The records have to be retained and provided on request to the supervisory authority, which will be the ICO.

Notification of data breaches (Arts. 33-34)

163. The definition of a personal data breach is substantially unchanged from DPA 1998 definition. It obviously covers breaches originated from outside the data controller's system, for example, personal data accessed by means of hacking or phishing, but it also covers breaches which may come from within chambers, for example the access to and disclosure of personal data (whether deliberate or accidental) by unauthorised members of staff, pupils or mini-pupils.

164. In the event of a personal data breach, Art. 33(1) imposes obligations on the data controller to notify the breach to the supervisory authority "without undue delay" and, if feasible, within 72 hours of becoming aware of the breach. If notification is made after 72 hours, reasons for the delay must be given. Art. 33(3) stipulates that the notification should at least:

> '(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
>
> (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
>
> (c) describe the likely consequences of the personal data breach;
>
> (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.'

165. Art. 33(4) imposes on the data controller an obligation to document the facts and effects of any personal data breaches and any remedial action taken. This is an aspect of the principle of accountability and is more than a mere formality as the

purpose of this documentation is to enable the supervisory authority to verify compliance with Art. 33.

166. Art. 33 also imposes an obligations upon a data processor to notify the data controller "without undue delay" on becoming aware of a personal data breach (Art. 33 (2)). This will apply where, for example, Chamber's systems are compromised and barristers save their data to a Chambers server.

167. Art. 34 deals with notification to data subjects. Where a personal data breach is "*likely to result in a high risk to the rights and freedoms of natural persons*" communication of the breach to the data subjects without undue delay is **mandatory**. Although the reporting threshold is high - referring to likelihood of a ***high*** risk to rights and freedoms, this threshold may be met – but this will depend on the nature of the personal data involved in the breach and the circumstances of the breach. The EDPB has approved the Art. 29 WP guidance on what amounts to a high risk for the purpose of the GDPR (see Annexe 3 and the Guidelines on Data Protection Impact Assessment). The following examples may meet that threshold:

(a) Loss or disclosure of a large amount of personal health data about children involved in a criminal case.

(b) Loss or disclosure of the names, addresses, national insurance numbers and dates of birth of a number of individuals may lead to a risk of identity theft.

On the other hand if the breach consists of the destruction of data which is a duplicate, this is unlikely to meet the threshold.

168. Art. 34(3) exempts the controller from being required to report a personal data breach to the data subject providing that at least one of three conditions is met. These are:

(a) (in effect) that the data were encrypted;

(b) that the controller has taken subsequent measures which ensure that the high risk to rights and freedoms is no longer likely to materialise; and

(c) that it would involve disproportionate effort to notify. However in such a case there is substituted an obligation to inform data subjects in an equally effective manner, such as by way of public advertisement.

169. The relatively small scale of most barrister's practices and most chambers may make it unlikely that (3) could safely be relied upon, and, in any event, it is difficult to see why barristers would prefer public advertisement to a personal communication. Further, if the breach is a disclosure, the nature of the data (especially that protected by Legal Professional Privilege) is such that it may be difficult to see what could be done ex post facto to ensure that risks to the data subjects' rights is unlikely to materialise. See also EDPB-endorsed guidance from the Art. 29 WP on personal data breaches (add to Annex 3 and Add Link https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052).

170. One strategy which may exempt a barrister from the data subject notification requirement would be to ensure that all files containing personal data are encrypted.

171. There is also a potential conflict between the obligation to notify data subjects of a personal data breach and the obligation of confidentiality. Where the data subject is a witness or on the other side in litigation or potential litigation, it may not be possible to notify them without disclosing your client's confidential or legally privileged information. In these circumstances, it may not be possible to comply with the obligation to notify. Neither the GDPR nor the DPA 2018 contain an exemption for privileged information in this situation. It may be prudent to ask the ICO or the Bar Council for guidance, taking into account the particular circumstances.

172. The time limit of 72 hours for notification to the ICO is very tight, especially if a data breach occurs just before or over a weekend. Individual barristers and chambers should therefore to consider establishing internal procedures to ensure compliance with the provisions of Arts. 33 and 34, including the preparation of an incident response plan. A draft pro forma incident plan can be found here [link].

Third country transfers (Arts. 44-49)

173. As mentioned in the Introduction above, during the implementation period the GDPR applies in the UK and the UK generally continues to be treated as an EU (and EEA) state for EEA and UK data protection law purposes. Any references to EEA or EU stated in this Guidance should therefore be read to also include the UK until the end of the implementation period.

174. Art. 44 sets out the general principle in relation to transfers of personal data to countries outside the EEA. A transfer of personal data may take place only if the conditions laid down in Chapter V GDPR are complied with by the controller and processor, including for onward transfers of personal data from the third country to another third country (or the processing is exempted from compliance pursuant to Sch. 2 Part 5 DPA 2018: journalism, artistic, academic or literary purposes). The ICO has published guidance on Chapter V.

175. GDPR Chapter V applies only to transfers of data. It does not apply where data is only in transit via non-EEA countries. The ICO has confirmed the view of the IT Panel, that it will not be a transfer if data held on a device under the control of a data controller is taken by the data controller to another country, which does not provide adequate protection. However, care should be taken to ensure that the data is not disclosed when in that country, as this would amount to a transfer.

176. Data transfer compliance will remain a significant concern for chambers and barristers working directly with international clients, lawyers and multinational organisations.

177. In contrast to the regime under the DPA 1998, under the DPA 2018 and the GDPR, transfer restrictions will apply both to data controllers and data processors when data is transferred to a third country or an international organisation. In addition, transfer restrictions will apply both to the initial transfer, and to any 'onward transfer'.

178. The ICO Working Party and the EDPB all have indicated that it is best practice to take the following layered approach to restricted international transfers of personal data:

- first consider whether there has been an adequacy decision confirming that the third country or international organisation provides an adequate level of protection, if not then
- the data exporter should consider putting in place appropriate safeguards such as one of the mechanisms included in Articles 45–46 of the GDPR
- finally, in the absence of the above, use one of the specific derogations of Article 49(1)

179. There are a number of mechanisms under which data transfers are permitted to 'a third country or an international organisation' such as where the Commission has provided an adequacy decision, specified appropriate safeguards are in place or where certain derogations apply

180. Under the GDPR, only the European Commission will be entitled to decide on the adequacy (or inadequacy) of a third country (or specified sector), territory or international organisation based on the elements set out in Article 45(2) and such decision will be subject to the examination procedure referred to under Art. 93(2). Once made, the effect of such a decision is that personal data can flow from

the EEA to that third country or international organisation as if it was an intra-EEA transfer.

181. The Commission has recognised certain countries and territories as providing sufficient level of protection for personal data to allow controllers to transfer data to them without further data export safeguards. A list of the Commission's current approved countries and territories may be found from its website [11].

182. Although the US is not recognised by the Commission as providing an adequate level of protection; on 12 July 2016, the Commission adopted an adequacy decision[12] that concluded that US organisations which are registered under the EU-US Privacy Shield (the Privacy Shield) did provide an adequate level of protection for personal data transferred from the EU to such US organisations. On 16 July 2020, this decision was set aside by the CJEU in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems[13]. Hence the Privacy Shield is no longer valid. The CJEU ruled that the standard contractual clauses ("SCC") for the transfer of personal data to processors established in third countries remained valid. However, the decision also makes clear that this was only on the basis that the SCC required disclosure of the risks to the data subject and the use of additional measures to ensure that an adequate level of protection was provided to data subjects. The EDPB has very recently started consulting on additional measures which may be used with the SCC to provide an adequate level of protection (see here). Industry sources have proposed the use of additional data security and minimisation techniques such as zero knowledge encryption, and pseudonymisation to legitimise transfers.

[11] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[12] Commission Decision (EU 2016/1250: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN

[13] https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

183. If there is no adequacy decision, transfers can occur under appropriate safeguards, provided that enforceable rights and effective legal remedies for data subjects are available as specified in Art. 46. However, it is likely that only SCC will be appropriate. Notably, there is no requirement for specific Data Protection Authority approval to implement a number of these safeguards, including:

(a) Legally binding instruments between public authorities (unlikely to be relevant for most barristers and Chambers)

(b) Binding Corporate Rules (BCRs) which provide the means by which a multinational organisation can transfer personal data intra-group from the EEA to a territory outside the EEA. They are not an appropriate remedy for transfer of personal data outside of an organisation's group. These are unlikely to be a useful mechanism for barristers or Chambers unless the Chambers has an annex in a non-EU country.

(c) Model Clauses from the Commission. These have yet to be developed under GDPR, but earlier versions produced under DPA 1998 are available which may be a starting point.

(d) The Supervisory Authority's adopted Standard Contractual Clauses ("SCC"). The ICO has indicated it intends to promulgate its own version of these clauses for use in the case of a no-deal Brexit.

(e) GDPR approved sectoral codes of conducts. At present there are no plans for such codes of conduct in the legal services sector.

(f) Through an approved certification mechanism such as a data protection seal or mark which has been issued by specified certification bodies or a competent Data Protection Authority, along with 'binding and enforceable commitments' of the third country controller or processor to apply safeguards, including as regards data subject rights. These have yet to be developed under GDPR for use in the legal sector.

184. The ICO may authorise specific clauses for use in controller/processor and controller/controller contracts or provisions in administrative arrangements between public authorities (provided that these arrangements include enforceable and effective data subject rights).

185. While the GDPR includes new mechanisms and safeguards that did not exist under DPA 1998, many are yet to be developed, such as the certification process. The ICO has an approval mechanism for certification bodies but has yet to authorise any certification bodies.

186. Under DPA 1998, it was possible to self assess the risks of the transfer if none of the formal 'adequacy solutions' (the equivalent to 'appropriate safeguards' under the GDPR) were in place. Under the GDPR, a data controller is required to carry out an assessment of the adequacy of protection for any particular transfer but must do so within the framework of Arts. 44 - 49. Following, Schrems II, in the absence of an adequacy decision, the options for legitimising transfer are far more limited. The assessment is limited to the consideration of which tools can be used to legitimise the transfer, and the identification of the additional safeguards required to enable SCC to be used.

187. If it is deemed that there is inadequate protection, or insufficient safeguards, international transfers will still be permitted if certain conditions are satisfied. While similar to those permitted derogations in DPA 1998, the conditions to be satisfied are set out in Art. 49 and are as follows:

    (a) the data subject must give explicit consent, having been informed of the potential risks of the transfer (rather than unambiguous consent); or

    (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(d) the transfer is necessary for important reasons of public interest; or

(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or[14]

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a public register open to consultation by the public or any person who can demonstrate a legitimate interest therein but only to the extent that the conditions laid down by Union or UK law are fulfilled. No such conditions have yet been enacted.

188. In addition to the above permitted derogations, there is also a new derogation under the GDPR for transfers which are necessary for "the controller's compelling legitimate interests', however this criterion has a very narrow scope and any controller seeking to rely upon it will have to satisfy specific prescriptive conditions or requirements, such as ensuring that the transfer is not repetitive, concerns only a limited number of data subjects and that the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards. The transfer has to be notified to the supervisory authority and the assessment has to be documented

189. Infringement of the provisions of the GDPR dealing with international transfers of personal data may be subject to administrative fines up to €20,000,000 or, in

[14] See ¶53 above on the meaning of "legal claims". The ICO Guidance on International transfers states: "You cannot rely on this exception if there is only the mere possibility that a legal claim or other formal proceedings may be brought in the future."

the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Art. 83) (see from ¶206 below).

190. S. 18 DPA 2018 provides for some aspects of third country transfers to be dealt with in delegated legislation; In particular, in relation to whether a transfer of personal data to a third country or international organisation is to be taken to be necessary for important reasons of public interest.

191. The ICO's Guidance on International Transfers states that for there to be a restricted transfer (i.e. a transfer to which 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 received confirmation from the ICO that this view 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).

Data Protection Officers (Arts. 37-39)

192. A barrister or set of chambers must appoint a Data Protection Officer if

(a) the core activities of the barrister or the set of chambers consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(b) the core activities of the barrister or the set of chambers consist of processing on a large scale of special categories of data pursuant to Art. 9 (e.g. data concerning health or sexual orientation) and personal data relating to criminal convictions etc. referred to in Art. 10 (¶¶52 to 55 above).

193. It is not likely that a barrister or a set of chambers would carry out regular and systematic monitoring of data subjects on a large scale. This is confirmed by the Art. 29 WP guidance on Data Protection Officers.

194. Recital 91 to the GDPR, referring to similar wording in Art. 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."

195. The processing activities of an individual barrister are not likely to be sufficient to be regarded as "large scale". The Chambers which acts as a processor in relation to a number of barristers (as data controllers) will carry out substantially more processing activities. Following this rationale, it might be argued that a Chambers would not be carrying on large scale activities as it acts as a processor separately in relation to each of the barristers. However, it is uncertain whether acting in this capacity might lead to the Chambers processing enough data to be carrying out processing on a "large scale", so that the set of chambers, as opposed to the individual barrister, needs to appoint a Data Protection Officer.

196. The wording of Recital 91 and the Art. 29 WP guidelines[15] suggest that it would be unusual for a barrister or set of chambers to be required to appoint a Data Protection Officer. However, it is possible that there are some sets of chambers

[15] Extracts from the GDPR Recitals and the ART. 29 WP guidance on DPOs and DPIAs are at Annex 3.

which may be required to do so. Chambers which are in any doubt should form their own view, or obtain specialist advice.

197. In the event that a barrister or set of chambers does need to appoint a Data Protection Officer, the Data Protection Officer could not be one of the barristers in the set of chambers, for (in most cases) two reasons.

(a) Firstly, most barristers would not fall within the requirement in Art. 37(5) that the Data Protection Officer must be selected on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Art. 39, namely:

i. to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

ii. to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

iii. to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Art. 35;

iv. to cooperate with the supervisory authority;

v. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Art. 36, and to consult, where appropriate, with regard to any other matter.

198. Secondly, while the Data Protection Officer may fulfil other tasks and duties, the data controller or processor must ensure that any such tasks and duties do not result in a conflict of interests, and must not be given any instructions regarding the exercise of the assigned tasks. A barrister acting as his or her own Data Protection Officer would inevitably face a conflict of interest. They would also face problems in monitoring the processing activities of other members of Chambers while maintaining confidentiality if members of chambers routinely act on opposite sides of the same dispute.

199. Other points (set out in Art. 38):

    (a) The controller and the processor shall ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

    (b) The controller and processor shall support the Data Protection Officer in performing the assigned tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

    (c) The controller and processor shall ensure that the Data Protection Officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The Data Protection Officer shall directly report to the highest management level of the controller or the processor.

    (d) Data subjects may contact the Data Protection Officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

200. In the event that a Data Protection Officer is appointed by chambers as data processor, the Data Protection Officer would be concerned only with the processing activities of the set of chambers (e.g. provision of email and internet

facilities), as opposed to the processing activities carried out by individual barristers for their own benefit (e.g. storage of data on a personally owned home computer, storage of data in the cloud by an individual barrister using the barrister's own cloud storage account or personal email account).

Data Protection Impact Assessments (Arts. 35-36)

201. Art. 35 states as follows:

> 'Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. …
>
> A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
>
> (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
>
> (b) processing on a large scale of special categories of data referred to in Art. 9(1), or of personal data relating to criminal convictions etc. referred to in Art. 10;[16] or
>
> (c) a systematic monitoring of a publicly accessible area on a large scale.'

202. As noted in ¶194 above, GDPR Recital 91 states that a Data Protection Impact Assessment should not be necessary where the processing concerns personal data from clients by an individual lawyer. It would be possible, but exceptional, for a barrister to be required to carry out a Data Protection Impact Assessment.

203. However, as indicated in ¶195 above it is uncertain whether the processing activities of a large set of chambers (specialising say in clinical negligence) may

[16] The ICO's Guidance interprets this as meaning that "large scale" applies to both Special category data and Criminal conviction data.

be extensive enough to require the chambers to carry out a Data Protection Impact Assessment.

Representatives of controllers and processors (Arts. 3(2), 27 and 30)

204. Arts. 3(2) and 27 require data controllers not established within the EU (which will be the position after Brexit) to appoint a representative within the EU if they offer services to data subjects within the EU or monitor the behaviour in the EU of data subjects, except when the processing is occasional, does not include, on a large scale, processing of special categories of data or processing of personal data relating to criminal convictions etc., and is unlikely to result in a risk to the rights and freedoms of natural persons. This will rarely, if ever, apply to barristers or Chambers. Barristers and Chambers must form their own view on this. Where it does apply, the representative should be established in the Member State where the relevant data subjects are located. See also the separate guidance on DPOs (¶192) and DPIAs (¶201).

205. In situations where Art. 30 applies, Art. 30 requires that the representative maintains a record of processing carried out – see Record-keeping (Art. 30), from ¶154 above.

Fines (Arts. 83-84)

206. The DPA 1998 permitted the levying of administrative fines as monetary penalties for failures to comply with the Data Protection Principles in DPA 1998 up to a maximum of £500,000. Before GDPR, the ICO was generally keen to ensure compliance rather than penalise errors. However, such "fines" as were levied could amount to tens of thousands of pounds for SMEs and charities. The award and level of monetary penalties were assessed according to defined conditions by the ICO, which conditions included the seriousness of the default, whether it was deliberate and the extent to which the organisation had the ability to pay.

207. The GDPR provides in Art. 83 for the supervisory authority [ICO] to impose administrative fines in respect of infringements of the GDPR which are effective proportionate and dissuasive.

208. Part 5 of the DPA 2018 provides for a mechanism similar to the mechanism of penalty notices under DPA 1998. The ICO will consider infringements and decide whether to issue a penalty notice.

209. The consideration will include the following matters:

(a) the nature, gravity and duration of the failure;

(b) the intentional or negligent character of the failure;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by the controller or processor;

(e) any relevant previous failures by the controller or processor;

(f) the degree of co-operation with the ICO, in order to remedy the failure and mitigate the possible adverse effects of the failure;

(g) the categories of personal data affected by the failure;

(h) the manner in which the infringement became known to the Commissioner, including whether, and if so to what extent, the controller or processor notified the Commissioner of the failure;

(i) the extent to which the controller or processor has complied with previous enforcement notices or penalty notices;

(j) adherence to approved codes of conduct or certification mechanisms;

(k) any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly);

(l) whether the penalty would be effective, proportionate and dissuasive.

210. The level of the maximum fine set out by the GDPR is up to €10M or 2% of annual worldwide turnover from the previous year of an undertaking, if there is a breach by the controller or processor of Arts. 8, 11, 25 – 39, 42 and 43. Under the DPA 2018 s.155, the sums are to be paid to the ICO in sterling.

211. The ICO has exercised its powers to make such penalties in several instances, including penalties of around £20M. The ICO follows its Regulatory Action Policy when setting the quantum of any penalty. The following factors are likely to increase any penalty:

- vulnerable individuals or critical national infrastructure are affected;
- there has been deliberate action for financial or personal gain;
- advice, guidance, recommendations or warnings (including those from a data protection officer or the ICO) have been ignored or not acted upon;
- there has been a high degree of intrusion into the privacy of a data subject;
- there has been a failure to cooperate with an ICO investigation or enforcement notice; and
- there is a pattern of poor regulatory history by the target of the investigation.

212. If there is a breach of the following obligations the fine is €20M or for undertakings 4% of annual worldwide turnover from the previous year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Arts. 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Arts. 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Arts. 44 to 49;

(d) any obligations pursuant to UK law adopted under GDPR Chapter IX: these relate to specific processing situations such as employment, journalism, archiving in the public interest and (which could be more relevant for barristers) as set out in the DPA 2018 and rules adopted by the ICO to monitor processing in relation to an obligation of professional secrecy (there are as yet no such rules);

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the ICO pursuant to Art. 58(2) or failure to provide access in violation of Art. 58(1).

213. GDPR requires that the exercise of these powers is subject to judicial control. In the DPA 2018 (ss.162 and 205) this is effected by the provision of an appeal process to the First-tier or Upper Tribunal.

Compensation (Art. 82)

214. An individual may seek compensation for material or non-material damage as a result of an infringement of the GDPR from a controller (e.g. barrister) or a processor (e.g. chambers). This is a new development as it provides direct liability for processors where the processor has not complied with its obligations under the GDPR specific to processors or where it has acted outside or contrary to the instructions of the controller. The controller is liable for all infringements of the GDPR, whether or not personally at fault.

215. The DPA 2018 s.168 states that non-material damage includes distress.

216. Where a controller or processor pays full compensation for the damage caused he may claim back from the other controllers or processors that part of the compensation for which they are responsible.

217. There is a defence to liability in the GDPR (Art. 82(3)) – but the burden of proof lies on the controller or processor seeking to rely on it. The controller/processor is exempt from liability where it proves that it is not in any way responsible for the event giving rise to the damage.

218. Under the GDPR where there is more than one controller or processor, all are responsible for the entire damage caused. This has not been expressly reproduced in the DPA 2018. The only reference is to specific processing, i.e. law enforcement processing and processing by the intelligence services, which limits recovery where there are joint controllers in certain circumstances to the joint controller who is responsible for compliance with the provision of the data protection legislation that is contravened.

219. An individual may choose to seek relief through a representative body (Art. 80) which can issue proceedings on the individual's behalf. The body has to be a non-profit body which acts in the public interest and which is active in the field of protection of data subjects' rights and freedoms with regard to the protection of their personal data. Ss. 187, 188 and 168(2) DPA 2018 provide for this route. Presently, no representative bodies have been identified.