Data Retention Policy

Purpose:	To guide all barristers and chambers on good practice in data retention policy and practice
Scope of application:	All practising barristers
Issued by:	The Information Technology Panel
Originally issued:	January 2017
Last reviewed:	November 2020
Status and effect:	**Please see the notice at end of this document. This is not "guidance" for the purposes of the BSB Handbook I6.4.**

1. Many barristers retain information from old cases. Much of it is stored on computers. This information could be disclosed or leaked in the event of a cyber-attack on a Chambers' server or a personal computer, or if data was left on the hard drive of an old PC or removable device after disposal. It may be necessary to report the fact that a data breach has occurred to persons identifiable from the information. This would be likely to be professionally embarrassing and may be costly.

2. Members of the Bar are required by their professional conduct rules and by the General Data Protection Regulation ("GDPR")[1] and the Data Protection Act 2018 ("DPA 2018") to keep information safe. Records must also be retained after a case has concluded: see rC129 of the Bar Standards Board (BSB) Handbook for public access work and rC141 of the Handbook for licensed access work (both min. 7-year retention). It may be necessary to keep data for longer in specific circumstances and for particular purposes and if required by the BMIF.

3. In the event of data loss or a data breach, it may be necessary to report the loss/breach to clients and to the regulatory bodies - the BSB and the Information Commissioner (ICO). The ICO has power to impose a fine of €20 million, or in the case of an undertaking, up to 4% of total worldwide annual turnover, whichever is higher, for breaches of some of the requirements of the GDPR. Compliance with the GDPR

[1] GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

has been mandatory from 25 May 2018 as it has direct effect, and has been incorporated into UK law in the DPA 2018. The principles set out in the GDPR will continue to apply in the event of Brexit. Arts. 33 and 34 of the GDPR contain mandatory requirements to notify the supervisory authority (ICO) and data subjects of a data breach in certain situations. Guidance on data breaches can be found here.

Regulatory obligations under the GDPR

4. GDPR Art. 5.1(c) and (e) state as follows:

> *"Personal data shall be: …*
>
> > *(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); …*
> >
> > *(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 …"*

5. If you are a data controller (which applies to barristers in private practice) it is your obligation to ensure that data subjects are notified of the purposes for which their personal data are being processed and the period for which the data will be retained **for those purposes**. The reference to the **purposes for which data is processed** (processing includes keeping the data) is a reference to the purposes which are included in your Privacy Notice to data subjects.

6. The ICO has published guidance in relation to the data minimisation and storage limitation principles.[2] This begins as follows:

> *At a glance*
>
> - *You must not keep personal data for longer than you need it.*
> - *You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.*
> - *You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.*
> - *You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.*
> - *You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.*
> - *You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.*

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation

Checklist

☐ *We know what personal data we hold and why we need it.*

☐ *We carefully consider and can justify how long we keep personal data.*

☐ *We have a policy with standard retention periods where possible, in line with documentation obligations.*

☐ *We regularly review our information and erase or anonymise personal data when we no longer need it.*

☐ *We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.*

☐ *We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.*

Creating a data retention policy

7. Under DPA 2018 you must be able to **demonstrate** compliance with the GDPR. This means that you should have a written record of your data retention policy and decisions taken about retention. If Chambers has a default data retention policy, you may wish to modify it to suit the requirements of your own practice. You will then find it easier to assess your compliance against the policy and adjust it as necessary. This should include standard retention periods for specific categories of documents. Some categories of documents will need to be retained for longer than others. How long you retain different categories of personal data should be based on the purpose and business need.

8. You also need to ensure, as part of the "privacy by design" approach to data protection, that you have automated procedures set up whereby you and your clerks are reminded when data are to be deleted or anonymised. This may also assist in identifying what needs to be erased and, how long it will take, if a data subject requests that personal data be erased.

Data retention pros and cons

9. In practice, there are a number of reasons for retaining documents/information beyond the end of a case. These include:

a. Case documents may be relevant to an appeal out of time (especially in criminal cases).

b. Anonymised case documents can be used as precedents.

c. Case documents may contain the results of research into the law, which may be relevant to a current case. These should be anonymised once any need to retain the data for other purposes has disappeared (e.g. "g" below).

d. Instructions, facts or expert opinions in a previous case may be relevant to a current case. These should be anonymised once any need to retain the data for other purposes has disappeared (e.g. "g" below).

e. Correspondence or instructions contain contact details which may be useful. These should be transposed from the correspondence and instructions to a list of contacts e.g. in Outlook, once the need to retain the documents for other reasons has disappeared (e.g. "g" below), so that the documents can then be deleted.

f. Information from case documents or records may be important when carrying out a conflict search. It will not usually be necessary to retain substantial numbers of case files for this purpose, and you may find that it is sufficient for the necessary information to be retained on the Chambers' system, for those who normally carry out these searches.

g. Case documents have to be retained in the event that a complaint is made against a barrister, or a barrister makes a claim against their insurers or solicitors. The limitation period for such claims should provide guidance as to the appropriate period of retention. You could seek assistance from your insurer as to their requirements for your document retention. In addition, an extended retention period may be required where clients are minors, lack capacity or, in criminal cases, during the defendant's custody.

The 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 bear in mind that 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."[3]

h. Correspondence, such as emails should be deleted when no longer required. If possible, it may be advisable to send emails that do not contain substantive advice in the body of the email, and provide advices as attachments which can then be saved with your case files. Emails may need to be retained in order to show that particular correspondence occurred or was received.

10. In addition to the legal requirements of the GDPR, there are practical reasons for deleting case documents after a reasonable period of time. These include:

a. It is easier to keep more limited amounts of data secure. Processing may be more efficient if the computer has more available resources (less data).

b. It is easier to search smaller quantities of data, e.g. when looking for specific data in response to a subject access request or when searching data for other purposes. It is also easier to deal with a data subject's request for erasure of personal data if the amount of personal data retained is kept to a minimum.

c. If certain types of data are retained for a long period they are more likely to be inaccurate and out of date.

d. If you retain data for old cases, and you suffer a data breach, you may be required to report the data breach to the ICO, to data subjects and to the BSB. This would be professionally embarrassing. You may not have up to date contact details for all the data subjects whose data you have retained. In such circumstances, you may be required to publicise the data breach generally, so that these data subjects can become aware of the potential risk to their data.

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

e. There may be a risk of being asked by a client or former client to provide disclosure of old documents, in litigation between the third party and the client. For example, suppose A, a pharmaceutical company, has a policy of destroying most of its data after six years. It may tell the other party to a patent dispute, B, that relevant documents have been routinely destroyed, but B may require A to contact its lawyers in previous litigation to ask them if they are still in possession of relevant documents.

f. If security is not maintained and there is a data loss, 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 level of that penalty. Serious contraventions of the Data Protection legislation are likely to be met with substantial financial penalties.

11. In the event of non-compliance with GDPR the ICO can issue an administrative fine under Art 83. Relevant factors in determining the size of the fine include:

a. the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

b. the intentional or negligent character of the infringement;

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 them;

e. any relevant previous infringements by the controller or processor;

f. the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

g. the categories of personal data affected by the infringement;

h. the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

i. compliance with previous measures ordered by the ICO or other supervisory authority against the controller or processor concerned with regard to the same subject-matter;

j. adherence to approved codes of conduct or approved certification mechanisms (note none are yet approved);

k. any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

12. The breach would be more likely to be regarded as serious if no old data has ever been deleted, if there is no data retention policy, or if no thought has been given to whether old data should be deleted. Whether or not a penalty is imposed, the ICO could insist on undertakings as to how information is retained and stored in the future.

13. You may also be at risk of civil proceedings by data subjects suffering financial or other damage.

14. BMIF have advised that such penalties are not covered by their professional indemnity insurance, but TLO (for those who have top-up insurance) provide cover up to £500,000 for legal advice and representation in relation to an investigation and data protection fines where permitted by law. Please note that there remains an ongoing discussion on whether the punitive, deterrent nature of fines, for a breach under GDPR, render them *"uninsurable"*.

15. In the event that a failure to keep information secure amounts to "serious misconduct", a barrister would be obliged to report themselves or another barrister to the Bar Standards Board under rC65.7 or rC66 of the BSB Handbook. In the event of such a failure, a barrister is obliged to take all reasonable steps to mitigate the effects, according to the guidance (gC94) under rC65.

In the event of any data breach, but particularly one involving a deliberate intrusion or access to data by a third party, consideration would have to be given to whether to inform solicitors and lay clients or the police, in particular where there was a risk of identity theft or misuse of confidential information, as mitigating steps could then be taken to avoid consequential loss and damage. Notification to data subjects is required without delay where the breach is likely to result in a high risk to the rights and freedoms of such persons. If it were decided to notify solicitors, clients and others, this could be a time-consuming, costly and embarrassing task.

Practical suggestions for individual barristers

Dealing with old documents

16. Before the GDPR came into effect, many barristers may not have given much thought to the deletion of archives, and they may have retained all emails and case documents. It could be difficult to find convincing reasons for having retained so much information that has ceased to be of any current use.

17. Carry out an assessment of the risks involved in retaining archives without routinely destroying data after a period of time, including the risk of a data breach and the risk that archives contain particularly sensitive data.

18. Take note of the following points:

a. Failure to destroy old documents may involve a breach of the data protection legislation.

b. The risk of a penalty being imposed following a breach is likely to be reduced if the barrister has a data retention policy and follows that policy. The policy might consist of a reasoned and documented decision of the basis on which old documents and data are being retained.

c. The information held in archives may become less sensitive than current information as time goes by, but bear in mind that some information such as criminal convictions affected by the Rehabilitation of Offenders Act, are intended to be forgotten after a period so the later, inadvertent disclosure of such information may cause substantial distress.

d. Routine and regular destruction of data in archives can involve considerable practical difficulty which can be eased by clear organisation of files. Automated reminders as to when deletion should take place should be considered.

19. Consider whether in the light of the above points it is reasonable and justifiable to retain archives indefinitely.

20. Include indemnities in your data processing agreements, to limit your exposure to breaches by those processors.

21. Individual barristers should also consider the following:

a. Whether your documents and emails are stored sensibly so that they can be found when needed. You should consider keeping work files and emails in separate folders for each year and subfolders for each matter, in order to simplify the task of deleting them.

b. Create a written data retention policy document. A version which you can adapt was contained in the Riliance GDPR Toolkit, which was previously made available. If you did not download it yourself, check whether your clerks or colleagues downloaded this useful suite of documents.

c. Whether, and to what extent, old case documents should be routinely deleted, and at what intervals (having regard to the purposes for which the

documents are needed, the needs of your practice and your data protection obligations).

d. To the extent necessary, how to retain old case documents (e.g. in a separate secure archive which is not accessible via the internet) so that they remain available when required but are retained securely. Guidance on cloud based solutions can be found here.

Additional points for sets of Chambers to consider

22. Sets of Chambers should also consider the following:

a. Does Chambers have an identified staff member/officer responsible for data protection and retention?

b. Is data (including archived data) being stored sufficiently securely?

c. Has Chambers identified where data resides (including archives, backups and deleted data), how long it is kept for, and how and when it is deleted?

d. Have all practicable steps been taken to ensure that deleted data is actually deleted, and is deleted in a secure fashion?

e. In the case of archived emails held outside Chambers, does the service provider actually delete data from the archive, or does it merely delete the index references to the data?

f. Have all practicable steps been taken to ensure that backups would not be corrupted in the event of a hacking attack?

g. Is it possible to impose a block on downloading of data (by an unauthorised third party) if more than a certain quantity of data is downloaded in a short space of time?

Related guidance

23. The Bar Council has previously provided related guidance, which you may find of assistance: Guidelines on Information Security and Email Guidelines for the Bar. The guidelines do not form part of the Code of Conduct, and following them does not necessarily provide a defence to complaints of misconduct or of inadequate professional service. It is the individual responsibility of the barrister to preserve the confidentiality of the client's affairs.

24. For those barristers that are qualified to provide legal advice and representation direct to the public, see also the BSB's Public Access Guidance for Barristers.

Important Notice

This document has been prepared by the Bar Council to assist barristers on matters of IT. **It is not "guidance" for the purposes of the BSB Handbook I6.4, and neither the BSB nor bodies regulating information security nor the Legal Ombudsman is bound by any views or advice expressed in it**. It does not comprise - and cannot be relied on as giving - legal advice. It has been prepared in good faith, but neither the Bar Council nor any of the individuals responsible for or involved in its preparation accept any responsibility or liability for anything done in reliance on it. For fuller information as to the status and effect of this document, please see here.

This is a generic policy on the use of information technology. It should not be used before being reviewed and amended to cover the specific circumstances of any particular individual or chambers.

The policy refers to other policies which chambers should have in place.

The policy does not cover disciplinary procedures which might arise as a result of breach of the policy, which should be added to this policy or dealt with separately.

This policy was drafted in **January 2017 and updated in November 2020**. Chambers should regularly review their policies email policy to take account of legislative change, developments in best practice and the relevant sections of the BSB Handbook.