



---

## What are my main obligations?

1. Under Principle 7 of the CLSB [Code of Conduct](#), you must keep client information confidential. This is your primary regulatory obligation in relation to your clients' data.
2. If you are obtaining a client's personal data for the purpose of providing them with legal advice or other services, you will also be a data controller under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Personal data is any information about an individual from which that individual can be identified.
3. Where the GDPR applies, you must ensure that you process your clients' personal data lawfully in accordance with the [seven data protection principles](#). This includes having appropriate security measures in place to protect the personal data you hold, which will also be necessary to meet your obligation to keep client information confidential.
4. Under the GDPR, you must not keep personal data for longer than you need it. In particular:
  - You will need to think about – and be able to justify – how long you keep different categories of personal data. This will depend on the purposes for which the data was collected.
  - You will need a policy that establishes standard retention periods for each category of personal data you hold.
  - You should periodically review the data you hold and ensure you erase or anonymise it when you no longer need it.
  - You must carefully consider any challenges to your retention of data, as individuals have a right to erasure if you no longer need to process their personal data.
5. All these obligations are the same whether you hold your clients' information electronically or in paper files.

---

## How long should I keep client data and files?

6. There is no set time period for retaining a client's file. You should follow the principles set out above in establishing appropriate internal policies. Whatever approach you take, you should ensure it is documented and communicated to your clients.
7. When setting retention periods, the following factors will be relevant:
  - You will need sufficient information to properly resolve any complaints relating to a matter.
  - You will want to retain certain information to protect yourself in the event of legal action arising from a matter.
  - Your professional indemnity insurer is likely to require you to keep information for a certain period.
  - You might be required by the CLSB to demonstrate compliance with our rules in the event of an audit or if there is a complaint.
  - It could be in the best interests of your client for you to retain certain documents for the client's future use.
8. With those considerations in mind (and subject to any specific insurance requirements), it is common to retain client files for six years after the end of the matter, as this is the usual limitation period for breach of contract and negligence claims.
9. However, you should take the following into account, particularly in relation to personal data that might be included in a client's file:
  - If you never carried out work for the client (for example, the file relates to an enquiry only), then you are unlikely to be able to justify retaining personal data for the full retention period.
  - It might not be necessary to retain all data for the full retention period.
  - You must consider any requests from individuals for their personal data to be erased and, if necessary, justify why you are retaining their personal data for the full retention period.

- 
- There might be other laws or rules applying to specific types of data, such as client identity records in organisations covered by anti-money laundering legislation.

## What happens when the retention period ends?

10. At the end of the retention period you should ensure that the client's file is disposed of securely. This is necessary to meet your obligations under the GDPR (in relation to any personal data in the file) and to ensure the client's information remains confidential.
11. For hard copy files, this might be achieved by shredding physical documents or using a service provider that safely destroys confidential waste. For electronic data, you must ensure that the data is destroyed in such a way that it can no longer be read by an operating system or application, and cannot be recovered and used for unauthorised purposes. Simply deleting the data is unlikely to be sufficient.
12. If you hold any original documents, these should be returned to the client when they are no longer needed by you and should not be destroyed without the client's consent.

## What do I need to tell clients?

13. Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.
14. You must provide individuals with information about the purposes for which you will retain their personal data, your retention periods and who the data will be shared with. In relation to sharing data, you should inform clients that you might need to share information about their matter with the CLSB for regulatory purposes, such as reporting on complaints.

- 
15. For a checklist of the information that you are required to give clients in relation to their personal data, visit the [Information Commissioner's Office](#) website.

## Other GDPR rights and obligations

16. Individual clients have [a number of other rights](#) under the GDPR of which you need to be aware, including the right to access their data and the right to have errors rectified. For more detailed guidance on complying with the GDPR, including your wider obligations beyond retention of client data, see the resources on the [Information Commissioner's Office](#) website.

**END**