DALE TIMSON
Barrister, Enterprise Chambers

PRIVACY NOTICE AND DATA RETENTION POLICY

Version 2.1. Last reviewed October 2026. Next review due by October 2027.

This document is in two parts. Part A is my privacy notice. It explains how I use personal data when I provide legal services and run my practice, and the rights of those whose data I hold. Part B is my data retention policy. It explains how long I keep records and how I dispose of them.

PART A: PRIVACY NOTICE

1. Who I am

1.1 I am Dale Timson, a self-employed barrister practising from Enterprise Chambers, 9 Old Square, Lincoln's Inn, London WC2A 3SR (telephone 020 7405 9471). I am regulated by the Bar Standards Board.

1.2 I am the controller of the personal data I process in my practice. This means that I decide how and why it is used and I am responsible for protecting it. I am registered with the Information Commissioner's Office ("the ICO") as a data controller under registration number ZA508543.

1.3 I am not required to appoint a data protection officer. Any question about this notice should be sent to me by email at daletimson@enterprisechambers.com, copied to my clerks at london@enterprisechambers.com, or by post to me at the address above.

1.4 My clerks and the staff of chambers handle personal data on my behalf, for example in managing my diary, fees and correspondence. Enterprise Chambers publishes a separate privacy notice, available at https://www.enterprisechambers.com/privacy-policy/, which covers personal data collected through the chambers website. That notice does not apply to the personal data I process in providing legal services, which is governed by this notice.

2. Scope of this notice

2.1 This notice applies to personal data which I process in providing legal services and in running my practice. It covers my clients (including public access clients and the individuals connected with company clients), instructing solicitors and other professionals, opposing parties, witnesses, experts, judges, court staff and others involved in a case, people who contact me, and people who receive information about my practice or attend my events.

3. The personal data I process

3.1 Depending on the matter, I may process the following:

(a) identity and contact details, including names, addresses, email addresses, telephone numbers, dates of birth and identity documents;

(b) professional and financial details, including occupation, employer, bank and payment details, and financial and business information;

(c) information about the matter, including the facts of a dispute or transaction, correspondence, evidence, witness statements, expert reports, court documents and my own notes and work product;

(d) special category data where it is relevant to the matter, such as information about health, racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, sex life or sexual orientation, and genetic or biometric data; and

(e) criminal offence data, being information about allegations, proceedings or convictions, which may arise in civil fraud and other matters.

4. Sources of personal data

4.1 I obtain personal data from the person concerned, and also from instructing solicitors, other parties and their representatives, witnesses and experts, courts and tribunals, my clerks and chambers, identity verification services where checks are made, and public sources such as Companies House, HM Land Registry, the Insolvency Service, court records, the press and the internet.

5. Purposes and lawful bases

5.1 I must have a lawful basis under Article 6 of the UK GDPR for each use of personal data. I use personal data for the following purposes and on the following bases:

(a) to provide legal services, including advising, drafting, negotiating and representing clients in courts, tribunals, arbitrations and mediations: performance of my contract with my client (Article 6(1)(b)) and, for others, the legitimate interests of my client and myself in the proper conduct of the matter and the administration of justice (Article 6(1)(f));

(b) to check for conflicts of interest and decide whether to accept instructions: my legitimate interest in complying with my professional obligations (Article 6(1)(f));

(c) to confirm the identity of clients and, where the Money Laundering Regulations apply, to carry out the checks they require: legitimate interests and, where the Regulations apply, legal obligation (Article 6(1)(c)) (see section 7);

(d) to issue fee notes, keep accounts and meet my tax obligations: contract and legal obligation;

(e) to deal with complaints, notify my professional indemnity insurer, the Bar Mutual Indemnity Fund ("BMIF"), and bring or defend legal claims: legal obligation and my legitimate interest in protecting my practice;

(f) to train pupils and mini-pupils: my legitimate interest in the training of barristers. Pupils and mini-pupils are bound by confidentiality, and a client may ask that they are not involved in the matter;

(g) to publish judgments, reported cases and articles: my legitimate interest in sharing legal knowledge and promoting my practice. I use only information already in the public domain or anonymised information;

(h) to respond to requests from the police, regulators and other public bodies, and for safeguarding: recognised legitimate interests under Article 6(1)(ea) and Annex 1 of the UK GDPR or, where the law requires disclosure, legal obligation; and

(i) to send information about my practice, seminars and events to professional contacts: my legitimate interest in promoting my practice and, where the law requires it, consent (Article 6(1)(a)).

5.2 Where I rely on legitimate interests, including recognised legitimate interests, any person may object to that use of their personal data on grounds relating to their particular situation. I will then stop unless I have compelling legitimate grounds which override their interests, rights and freedoms, or I need the data for the establishment, exercise or defence of legal claims. Any person may object to direct marketing at any time, and I will then stop.

5.3 Where I rely on consent, it may be withdrawn at any time by contacting me. Withdrawal does not affect anything done before it. In most cases I do not need consent because another lawful basis applies.

6. Special category and criminal offence data

6.1 To process special category data I rely on Article 9(2)(f) of the UK GDPR, which permits processing necessary for the establishment, exercise or defence of legal claims. To process criminal offence data I rely on paragraph 33 of Schedule 1 to the Data Protection Act 2018 ("the DPA 2018"), which permits processing necessary for legal proceedings, for obtaining legal advice, or for establishing, exercising or defending legal rights. Occasionally I may rely on the data having been manifestly made public by the person concerned, or on that person's explicit consent.

6.2 The DPA 2018 requires a controller to keep an appropriate policy document when relying on certain conditions in Schedule 1, principally the substantial public interest conditions. None of the conditions on which I rely requires one, and I do not rely on any condition which does. If my practice changes so that I need to rely on such a condition, I will put an appropriate policy document in place before doing so.

7. Identity checks and money laundering

7.1 Where I accept instructions directly from a client under the public access scheme, or where no solicitor or other professional has already verified the client's identity, I ask for evidence of identity. For an individual this will usually be photographic identification and proof of address. For a company it will usually be details of the company and of the individuals who own or control it. I do this to confirm who I am acting for, to check for conflicts of interest and to guard against fraud.

7.2 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("the Money Laundering Regulations") apply to a barrister only for certain types of work, principally where I assist in the planning or execution of a financial or real property transaction, or give tax advice. Most of my work, which consists of advising on and conducting disputes and litigation, is outside their scope.

7.3 Where the Money Laundering Regulations apply to particular work, I will carry out the customer due diligence they require. This may include verifying identity from a reliable and independent source, identifying any beneficial owner and understanding the purpose of the instructions. I will use the information obtained for those checks only for the prevention of money laundering and terrorist financing, unless the law permits otherwise, and I will keep it for five years from the end of the matter, after which I will delete it unless the law requires me to keep it.

8. Whether you must provide personal data

8.1 There is no statutory obligation to provide personal data to me. However, I need certain information from a client in order to accept instructions, carry out identity and conflict checks and act. If it is not provided, I may be unable to act or to continue acting.

9. Recipients of personal data

9.1 I share personal data only where it is necessary and lawful. Depending on the matter, recipients may include:

(a) my clerks and the staff of chambers, who act for me under obligations of confidentiality;

(b) instructing solicitors and other professional advisers involved in the matter;

(c) courts, tribunals, arbitrators and mediators, and other parties and their representatives, as the matter requires;

(d) witnesses and experts;

(e) pupils and mini-pupils;

(f) BMIF and my own professional advisers;

(g) the Bar Standards Board, the Legal Ombudsman and the Bar Council;

(h) HM Revenue and Customs, law enforcement agencies and other public bodies, where the law requires or permits disclosure;

(i) my accountants and bank; and

(j) service providers who support my practice, including providers of IT, email, secure cloud storage, document management, transcription, translation and dictation services, who act on my instructions under written terms and must keep the data confidential and secure.

9.2 I do not sell personal data.

10. Technology

10.1 I use technology in my practice, including secure cloud storage, email, document management and, from time to time, software tools which assist with summarising or organising material, checking drafts and research. The providers of those services act as my processors under written terms, and I check their security and confidentiality arrangements before use. I use identifiable client or case information only with services which keep it confidential and do not use it to train their systems. I review all work produced with the assistance of such tools and I remain responsible for my advice and work. No decision about any person is made by such a tool.

11. Transfers outside the United Kingdom

11.1 Some of my service providers, and sometimes parties or advisers in a matter, are based outside the United Kingdom. Where personal data is transferred outside the United Kingdom, I ensure that it is protected by one of the safeguards permitted by UK law, namely: that the destination is covered by UK adequacy regulations (including the EU and EEA, and US organisations certified under the UK Extension to the EU-US Data Privacy Framework); that the transfer is made under the ICO's International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, after I have satisfied myself that the standard of protection will not be materially lower than in the United Kingdom; or that an exception applies, for

example where the transfer is necessary for legal claims. Further information about these safeguards is available from me on request.

12. Retention

12.1 I keep personal data only for as long as necessary. My own work on a matter, including advices, drafts, notes and emails, is kept for 15 years from the end of the matter, which reflects the 15 year long-stop limitation period for negligence claims and the advice of BMIF. Other documents relating to a matter are kept for 7 years from the end of the matter. Paper copies are securely shredded at the end of the matter unless their return is requested. I keep a minimal record of clients, parties and matters for conflict checking while I remain in practice. Full details are in Part B.

13. Security

13.1 I take appropriate technical and organisational measures to protect personal data. These include encrypted devices, accounts protected by strong passwords and multi-factor authentication, secure storage and disposal of paper documents, limiting access to those who need it, and confidentiality obligations on those who work with me. I may access your information securely while working temporarily outside the UK; it remains under my control and protected by the same security measures. If a personal data breach occurs, I will deal with it promptly and, where the law requires, report it to the ICO and inform those affected.

14. Automated decision-making

14.1 I do not make decisions about any person based solely on automated processing which produce legal or similarly significant effects.

15. Your rights

15.1 Subject to certain conditions and exemptions, you have the right to ask for a copy of your personal data and information about how I use it; to ask me to correct inaccurate or incomplete data; to ask me to erase your data; to ask me to restrict my use of your data; to receive data you have provided to me in a structured, machine-readable format, or to have it sent to another controller; to object to my use of your data as described in paragraph 5.2; and to withdraw consent where I rely on it.

15.2 These rights may be limited by law, in particular where information is subject to legal professional privilege or to my duty of confidentiality to a client, or where providing it would disclose personal data about another person.

16. How to exercise your rights

16.1 Requests should be made to me using the contact details in section 1. I may ask for proportionate evidence of identity before acting on a request, and the time for my response runs from receipt of that evidence.

16.2 I will respond within one month. If a request is complex, or there are several requests, I may extend that period by up to two further months, and I will explain why. If I need a request to be clarified, the time for my response is paused until the clarification is received. I will carry out reasonable and proportionate searches.

16.3 No fee is normally payable. I may charge a reasonable fee, or decline to act, if a request is manifestly unfounded or excessive.

17. Complaints

17.1 If you are unhappy with the way I have handled your personal data, please tell me first using the contact details in section 1 so that I can try to put matters right. I will acknowledge your complaint within 30 days, consider it without undue delay and tell you the outcome.

17.2 You also have the right to complain to the ICO, which regulates data protection in the United Kingdom, at https://ico.org.uk/make-a-complaint or on 0303 123 1113. The ICO will usually expect a complaint to have been raised with me first.

17.3 Complaints about the legal services I have provided are dealt with separately under the complaints procedure of chambers and, where applicable, by the Legal Ombudsman.

18. Marketing

18.1 I may send professional contacts information about my practice, seminars and events. Anyone may unsubscribe at any time by using the link in any such message or by emailing me or my clerks at london@enterprisechambers.com. I will act on such a request promptly and in any event within 7 days. I keep a record of those who have unsubscribed, limited to their name and email address, so that they are not contacted again.

19. Changes to this notice

19.1 I review this notice at least once a year and whenever the law or my practice changes. If I intend to use personal data for a new purpose, I will provide information about that purpose before doing so. The current version is available on my profile on the Enterprise Chambers website and on request.

PART B: DATA RETENTION POLICY

1. Purpose and scope

1.1 This policy sets out how long I keep the records and personal data held in my practice, and how I dispose of them securely. It applies to all records, paper and electronic, held by me or on my behalf by my clerks and service providers.

1.2 This policy should be read with my privacy notice in Part A. Records held on chambers' systems are also subject to the arrangements of Enterprise Chambers for the security of those systems.

2. Definitions

2.1 In this policy, "UK GDPR" means Regulation (EU) 2016/679 as it forms part of the law of the United Kingdom, as amended, including by the Data (Use and Access) Act 2025; "DPA 2018" means the Data Protection Act 2018; "matter" means a case or piece of work; and "the end of a matter" means the later of the date of my last work on it and the final conclusion of the proceedings or transaction, including any appeal and the payment of my fees.

3. Basis for the retention periods

3.1 The UK GDPR requires that personal data is kept for no longer than is necessary for the purposes for which it is processed. The retention periods in section 5 have been set having regard to the following:

(a) the Limitation Act 1980, under which most claims in contract and tort must be brought within 6 years, claims on a deed or for the recovery of land within 12 years, and negligence claims for latent damage within 3 years of the date of knowledge, subject to a long-stop of 15 years from the act or omission complained of (sections 2, 5, 8, 14A, 14B and 15);

(b) the advice of BMIF, endorsed in the Bar Council's Data Retention Policy Guidance (May 2025), that barristers should retain notebooks, emails and their attachments, attendance notes and documents they have drafted for at least 15 years, being the long-stop period under section 14B of the Limitation Act 1980;

(c) the BSB Handbook, which requires a barrister acting on public access instructions to keep, or ensure that the client keeps, copies of instructions, advices, documents drafted and notes of conferences for at least 7 years after the last item of work (rule C129), and requires complaints records to be kept for 6 years from resolution (rule C108);

(d) the requirement of HM Revenue and Customs that a self-employed person keeps business records for at least 5 years after the 31 January online filing deadline for the tax year to which they relate; and

(e) regulation 40 of the Money Laundering Regulations, which requires customer due diligence records to be kept for 5 years from the end of the business relationship and then deleted unless an exception applies.

4. General principles

4.1 Retention periods run from the end of the matter unless otherwise stated in section 5. Where I am instructed again in the same matter, the period runs afresh from the end of the further work.

4.2 At the end of each period I will review the record within the following 12 months and securely destroy or anonymise it, unless there is a specific reason to keep it longer, such as an actual or threatened claim, complaint or regulatory investigation, or a request from BMIF. I will record any decision to keep a record longer, with the reason and a further review date.

4.3 Original documents belonging to a client or solicitor are returned at the end of the matter and are not retained by me.

4.4 A request for erasure will be considered in accordance with Part A and this policy.

5. Retention schedule

5.1 I retain records for the following periods:

Type of record	Retention period	Reason
My work product and record of the matter: advices, opinions, statements of case and other documents drafted or approved by me, notes of conferences and telephone advice, notebooks, attendance notes, and emails with their attachments	15 years from the end of the matter	Long-stop limitation period under section 14B of the Limitation Act 1980; BMIF advice
Instructions and the documents supplied with them, bundles, disclosure, witness statements, expert reports and court documents (electronic copies)	7 years from the end of the matter	Ordinary 6 year limitation period plus one year; rule C129 for public access matters
Paper copies of instructions and papers	Securely shredded at the end of the matter, unless their return is requested	Electronic copies are retained as above; chambers' practice on completion of work
Original documents belonging to a client or solicitor	Returned at the end of the matter	They belong to the client or solicitor
Public access case record (dates of instructions, work done and fees)	7 years from the end of the matter	Rules C128 and C129 of the BSB Handbook
Evidence of identity and customer due diligence records	5 years from the end of the matter, then deleted. A note that the check was made is kept with the matter record	Regulation 40 of the Money Laundering Regulations, where they apply; the same period is used for other identity checks
Enquiries which do not lead to instructions	12 months from the enquiry, save for the name and subject matter kept on the conflict record	Long enough to deal with any follow-up enquiry
Fee notes, invoices, bank records and accounts	7 years from the end of the tax year to which they relate	Meets the HMRC requirement of 5 years after the 31 January filing deadline
Complaints about my services	6 years from resolution of the complaint	Rule C108 of the BSB Handbook
Conflict record: names of clients and other parties, and a short description of each matter	While I remain in practice	Needed to identify conflicts of interest; kept to the minimum
Data protection requests, data protection complaints and personal data breach records	6 years from the close of the request, complaint or breach	To demonstrate compliance and to deal with any claim
Anonymised precedents, research notes and published judgments	Indefinitely	No personal data is retained once anonymised; judgments are public

Type of record	Retention period	Reason
Marketing and event contact lists	Until the person unsubscribes, or 2 years after the last contact, whichever is earlier	Keeps the list accurate and limited to active contacts
Record of those who have unsubscribed	For as long as I send marketing	Needed to ensure they are not contacted again

6. Secure disposal

6.1 Paper records are disposed of by cross-cut shredding or through a confidential waste service. Electronic records are deleted from my devices, cloud storage and email, and from backups in their normal cycle. Devices are securely wiped or destroyed when they are replaced.

7. Suspension of disposal

7.1 If I become aware of a claim, complaint, regulatory investigation or litigation relating to a matter, I will suspend the disposal of the relevant records until it has been resolved, and record the reason.

8. Review

8.1 I review this policy, together with Part A, at least once a year and whenever the law or my practice changes. This policy was last reviewed in October 2026. The next review is due by October 2027.