

PRIVACY POLICY OF:

Anthony Searle

Barrister

Serjeants' Inn Chambers, 85 Fleet Street, London EC4Y 1AE

ICO Registration Number: **ZA209538**

Policy became operational on: **30 January 2026**

Next review date: **30 January 2027**



PRIVACY POLICY

In order to provide legal advice and representation, I need to collect and hold personal data. This may include your personal data and personal data relating to other individuals involved in a matter. I take appropriate measures to protect personal data and to comply with my data protection and professional obligations. This privacy notice explains what personal data I collect, how it is used and shared, and the rights you have in relation to it.

Data controller

I, **ANTHONY SEARLE**, am a member of Serjeants' Inn Chambers. I am registered with the Information Commissioner's Office ('ICO') as a Data Controller for the personal data that I hold and process as a barrister. My registered address is **85 Fleet Street, London EC4Y 1AE** and my ICO registration number is **ZA209538**. If you need to contact me about your data or this privacy notice, you can reach me at asearle@serjeantsinn.com.

Data collection

Personal data I process is usually provided to, or gathered by, me in connection with providing legal advice and representation (including in relation to pre-action work and/or proceedings). I and/or your solicitor will usually explain why the information is needed and how it will be used.

In addition to information you (or your solicitor) provide, I may also obtain information from other sources such as:

- Publicly available sources (such as registers, searches, the internet and the media), where relevant and proportionate to the matter;
- Solicitors, barristers and other legal professionals involved in the matter, including their associates, trainees and staff;
- Chambers staff (for administrative purposes);
- Expert witnesses and other professionals instructed in the matter;
- Courts/tribunals, court staff and officials;
- Public authorities and regulatory bodies (where relevant); and
- Other parties involved in the matter.

If you are not my client

In the course of providing legal services, I may process personal data relating to individuals who are not my client. This can include, for example, opponents, witnesses, clinicians/healthcare staff, family members, and other persons connected with the matter.

I usually obtain this information from my client and/or their solicitors, from court/tribunal documents, from experts, from chambers administration, or from other parties involved in the case.

I process such information only so far as is necessary for the purposes described in this notice (in particular, providing legal advice and representation, complying with professional obligations, and establishing, exercising or defending legal claims).

Where I obtain personal data from sources other than the individual it relates to, UK GDPR generally requires that privacy information is provided to that individual, subject to applicable exceptions and exemptions (including where providing the information would involve disproportionate effort, or where it would be inconsistent with duties of confidentiality or legal professional privilege (where applicable)).

This privacy notice is intended to provide that information to individuals whose personal data I process, including individuals who are not my clients.

If you are not my client and you have questions about how your personal data is processed, you may contact me using the details set out in this notice.

What data do I process about you?

Depending on the type of work, I may collect and process **personal data** and, where relevant, **special category personal data** (which the UK GDPR treats as particularly sensitive and subject to additional protections).

Personal data may include:

- **Identity and contact details** (for example, name, email address, telephone number, address, date of birth);

- **Identifiers contained in case materials**, particularly in medical records (for example, NHS number and other reference numbers);
- **Identity documentation** where it appears in the papers or is required for administrative purposes (for example, passport or driving licence details);
- **Family details** and information about your background and current circumstances (where relevant to the issues);
- **Details relating to education, training and employment** (including work history and earnings history where relevant);
- **Financial information**, including (where relevant to the work) income, benefits, tax information, bank/payment details, and information about assets and liabilities (for example, where needed to quantify loss of earnings, care needs, or other heads of loss);
- **Online identifiers and related information**, where relevant and proportionate to the matter (for example, social media account usernames/handles and publicly available content, or material disclosed within surveillance evidence).

Where relevant (and depending on the nature of the matter), I may also need to process **special category personal data**, which can include personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious, philosophical or other beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning physical or mental health (this is commonly relevant in clinical negligence and inquests); and
- Sex life and sexual orientation.

On occasion, I may also process criminal offence data, including personal data relating to criminal convictions and offences and related security measures, and this can include information about allegations, investigations and proceedings where relevant to the matter.

My lawful basis for processing your information

In order to provide legal services and representation, I must process personal data. The UK GDPR requires that, whenever I process personal data, I have a lawful basis for doing so.

The lawful basis (or bases) I rely on when processing **personal data** will depend on the specific purpose for which it is used. In most cases, I rely on one or more of the following:

- **Performance of a contract:** processing is necessary for a contract with you, or to take steps at your request before entering into a contract.
- **Compliance with a legal obligation:** processing is necessary to comply with legal and regulatory obligations (for example, tax and accounting obligations, and professional/regulatory requirements).
- **Legitimate interests:** processing is necessary for the legitimate interests of my practice or of a third party, except where those interests are overridden by your interests or fundamental rights and freedoms.
- **Consent:** I will only rely on consent where it is appropriate and where you have a genuine free choice (for example, for a specific optional purpose). You can withdraw consent at any time. Withdrawal will not affect the lawfulness of processing carried out before consent was withdrawn.

Where I process **special category personal data** (for example, health data), I will also ensure that a UK GDPR condition for processing special category data applies. In most cases, this will be because the processing is necessary for the establishment, exercise or defence of legal claims (including prospective legal proceedings) and/or for obtaining legal advice.

Where I process **personal data relating to criminal convictions and offences** (including allegations, investigations and proceedings), I will do so only where it is authorised by UK law and an appropriate condition under Schedule 1 of the Data Protection Act 2018 applies. Where relevant, this may include processing necessary for legal proceedings, obtaining legal advice, or establishing, exercising or defending legal rights.

Examples of **legitimate interests** include but are not limited to:

- Providing legal services and advice;
- Practice management, billing, accounting and debt recovery;
- Meeting professional and regulatory requirements;
- Maintaining the security and integrity of systems and information; and
- Reporting threats to public security;
- Preventing fraud; and
- Such other purposes as set out below.

Purposes

I use your personal data for the following purposes:

- Providing legal services, including the provision of legal advice and representation in courts, tribunals, arbitrations and mediations;
- Training and supervision (for example, pupils, mini-pupils, work-shadowing students and other barristers), where appropriate and subject to confidentiality;
- Investigating and addressing concerns, complaints and queries, including dealing with my regulator where relevant;
- Investigating or addressing legal proceedings or disputes relating to my services, or as otherwise permitted by law;
- Making statutory returns as required by HMRC or other applicable law;
- Practice management and administration, including billing and debt recovery;
- Applications for panels, tenders, appointments and other professional development/career progression; and
- Conducting conflict of interest checks, and (where applicable or required) carrying out any anti-money laundering and counter-terrorist financing checks.

Sharing

In the course of processing your information to provide legal services, I may share your personal data with:

- Instructing solicitors or other lawyers involved in your case;
- A pupil, mini-pupil, work experience student, or professional colleague under my training/supervision (subject to confidentiality);
- Other parties to the matter and their legal representatives (including opposing counsel and, where relevant, opposing lay clients), for the purposes of the proceedings and/or resolving the case;
- Courts/tribunals and their staff and officials (including the judiciary), and where relevant arbitrators and mediators;
- Chambers' management and staff who provide administrative services for my practice;
- Expert witnesses and other witnesses;
- My regulator, insurers, and/or legal advisers in the event of a dispute, complaint or other legal matter;

- The Head(s) of Chambers, a senior barrister, or the complaints committee within my chambers, in the event of a complaint;
- Accountants and banking providers for accounting, billing and payments;
- IT, communications and cloud service providers used to support my practice (for example, email, document storage, secure file transfer, case management, video-conferencing and backup services), who process personal data on my behalf under appropriate contractual safeguards;
- Legal directories (such as Chambers & Partners and The Legal 500) and relevant panels/tendering committees for the purpose of maintaining my professional profile and professional development; and
- Any other party where I ask you for consent and you consent to the sharing.

I may also be required to disclose personal data to law enforcement agencies, government authorities or intelligence services where required by law, or pursuant to a court order.

Use of technology, including artificial intelligence ('AI')

I may use AI-enabled tools as part of my general research and analysis workflow, often to help me understand and interrogate medical issues that arise in my work (for example, explaining medical terminology, understanding the significance of investigations such as blood results or imaging findings, and locating, summarising and analysing medical literature and clinical studies). In doing so, I generally do not input personal data and I limit prompts to non-identifying, generalised information.

I do not use AI to make decisions about you that are based solely on automated processing (including profiling) and that produce legal or similarly significant effects. All professional judgments and decisions in my practice remain my responsibility.

What I do (and do not) input into AI tools:

- I do not input client/patient identifying information, or upload case documents, into general-purpose cloud AI tools (such as ChatGPT or Claude).
- When using AI tools, I take steps to ensure that any prompts are non-identifying and do not include information from which an individual could reasonably be identified.
- In exceptional circumstances, where it is genuinely necessary to process identifying information for a specific task, I may use an offline AI tool running locally on my own device (so that data does not leave my device).

AI tools can produce inaccurate, incomplete or misleading outputs. Where I use AI-enabled tools, I use them only as an aid to research and analysis and I remain responsible for the work and any decisions taken. In particular, I apply safeguards such as:

- Data minimisation: I avoid including client/patient identifying information and I limit prompts to what is necessary for the task.
- Human review: I review outputs myself and do not rely on them without independent consideration.
- Verification: Where an output matters to the work, I cross-check it against primary sources (for example, published clinical guidance, peer-reviewed literature, or opinions from appropriately qualified experts).
- Confidentiality and security: I take steps to protect confidentiality and to use tools/settings that are appropriate for the sensitivity of the information being handled.

This is consistent with the general principle that generative AI should not be treated as authoritative and that professionals remain responsible for their work and for protecting confidential information.

If the use of any technology involves a transfer of personal data outside the UK, further information is set out in the 'Transfers to third countries and international organisations' section of this notice.

Your data protection rights are set out in the 'Your rights' section of this notice.

International transfers (outside the UK)

This privacy notice is of general application and it is not always possible to state in advance whether it will be necessary to transfer (or make accessible) your personal data outside the UK for any particular purpose.

Transfers outside the UK may be necessary, for example where you are located outside the UK, where instructions are received from outside the UK, or where the provision of legal services involves persons, organisations, courts or tribunals outside the UK. If you are based outside the UK and you would like to discuss additional precautions, please contact me as early as possible.

I may transfer (or make accessible) your personal data outside the UK if, now or in the future, I use cloud-based services (including storage, backup and other hosted software tools used to process information) that are hosted or supported from overseas. I will only do so where the transfer is permitted under UK data protection law, including by relying on one or more of the following mechanisms:

- **United States:** Where the recipient is certified under the UK Extension to the EU-US Data Privacy Framework (also known as the 'UK-US Data Bridge'), transfers may be covered by the UK's partial adequacy arrangements for the United States. See further details [here](#).
- **Adequate destinations (including Switzerland):** Where a destination is covered by the UK's adequacy regulations (which include Switzerland), it is treated as providing an adequate level of protection for UK personal data. See further details [here](#).
- **Non-adequate destinations/ safeguards:** Where a destination is not covered by UK adequacy regulations, I will put in place an appropriate safeguard (for example, the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, as applicable). You may obtain further information about the relevant safeguard (and a copy, where appropriate) by contacting me.
- **Exceptions (derogations):** In limited cases, where neither adequacy nor an appropriate safeguard is available, I may rely on an exception under Article 49 of the UK GDPR (for example, where a transfer is necessary for the establishment, exercise or defence of legal claims). These exceptions are interpreted restrictively and are not used for routine or repetitive transfers.

If a judgment or other decision that includes your personal data is published by a court or tribunal (including online), it may be accessible worldwide.

I will not transfer personal data outside the UK except where necessary for the purposes set out in this notice and in accordance with UK data protection law.

If you require any further information, you can reach me at asearle@serjeantsinn.com.

Keeping your personal data secure

I take appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. These measures are risk-based and may include, where appropriate:

- Limiting access to personal data to those who need it for the purposes of providing legal services (including chambers staff providing administrative support), and ensuring appropriate confidentiality obligations apply;
- Secure storage and handling of information (including access controls and secure backup arrangements);
- Secure communications practices where sensitive information is shared; and
- Maintaining reasonable steps to keep devices and accounts protected (for example, strong authentication and keeping software up to date).

Where I use third-party service providers to support my practice (for example, email, storage or other IT services), I take reasonable steps to ensure appropriate security measures and confidentiality obligations are in place.

If a personal data breach occurs, I will assess it and take appropriate steps. Where required by law, I will notify the ICO and/or affected individuals without undue delay.

Retention of data

I retain personal data for as long as is necessary for the purposes set out in this privacy notice, and in accordance with my Retention and Disposal Policy (a copy is available on request). Personal data will be reviewed periodically and deleted or anonymised when it is no longer required.

I will typically retain case files for at least 15 years following the conclusion of a case/matter or receipt of final payment, whichever is later. This reflects Bar Mutual Indemnity Fund's published position that barristers have good reason to retain key case records for at least 15 years, linked to the 15-year long-stop limitation period in section 14B of the Limitation Act 1980. In some matters (including those involving infants or protected parties), a longer retention period may be appropriate. For more information, please read the Bar Council's Data Retention Policy Guidance [here](#).

You may ask me to delete or anonymise your personal data. I will consider any such request and will delete or anonymise personal data where I no longer need it. However, the right to erasure is not absolute and I may need to retain personal data where, for example:

- There is an unresolved issue, claim, complaint or dispute;

- I am required to retain it to comply with legal or professional obligations; or
- It is necessary for the establishment, exercise or defence of legal claims.

Where pleadings, advices or other documents have been drafted, I may retain anonymised and/or redacted versions for learning purposes and legal research. Where I do so, I will remove personal identifiers and keep the continued retention under review.

Your rights

The UK GDPR gives you a number of **rights in relation to your personal data**. These include:

- The right to be informed about how your personal data is used;
- The right of access (often called a 'subject access request') – you can ask for a copy of the personal data I hold about you, and for information about how I use it;
- The right to rectification – you can ask me to correct inaccurate personal data, and in some circumstances to complete incomplete data;
- The right to erasure ('right to be forgotten') in certain circumstances;
- The right to restrict processing in certain circumstances;
- The right to data portability in certain circumstances;
- The right to object in certain circumstances (particularly where processing is based on legitimate interests);
- The right to withdraw consent (where processing is based on consent)
- Rights relating to automated decision-making and profiling (where applicable).

If you have questions about any processing described in this notice, or you wish to exercise your rights, please contact me using the details below.

Complaints and remedies

If you are unhappy with how I have handled your personal data or a request you have made, you have the **right to complain** to the Information Commissioner's Office ('ICO').

You may also have the right to seek a remedy through the courts and, in some cases, to claim compensation for damage (including distress) caused by an infringement of data protection law.

Further information, including how to make a complaint, is available from the [ICO's website](#).

Accessing and correcting your information

You may request access to, correction of, and/or a copy of your personal data by contacting me at asearle@serjeantsinn.com.

To help me deal with your request as efficiently as possible, please provide:

- Your full name and contact details;
- A description of the information you are requesting (and, if relevant, the approximate dates or context); and
- Any reference number or matter details you have been given.

If I am not satisfied about your identity, I may ask for additional information to verify it. I will only request information that is necessary for this purpose.

I will respond to requests without undue delay and within one month, subject to any permitted extension where a request is complex or numerous.

I may update this privacy notice from time to time. When I make significant changes, I will publish the updated notice on my chambers website profile and will provide it to you on request.