



PRIVACY NOTICE

This Notice is intended to inform you as to how and why Stone Rowe Brewer (SRB) uses personal information from clients and other members of the public. When we refer to “we” or “us” in this policy we are referring to Stone Rowe Brewer LLP.

Information we collect and hold about you

Clients

We will collect personal information about you when you contact us about providing legal services to you (for example, your name, address, email contact details, telephone number). We may require further information before we provide legal advice to you (for example, your passport or other ID) in order to comply with our regulatory requirements. We may also collect personal data about you from publicly accessible sources, e.g. Companies House or HM Land Registry as part of our service provided to you.

During the course of providing legal services to you, we may collect information about you and/or any other individuals you tell us about. Depending on the nature of the work we carry out for you, we may collect and use special categories of personal data about you or a third party you tell us about (for example, information about health, ethnic origin, religious or philosophical beliefs).

Visitors to our website

We will collect personal information that you voluntarily provide to us if you fill in a form on our website or apply for a vacancy through the website. This information may include your contact details including name, address, email, telephone number.

We may also collect information about how you use our website, and our Cookies Policy has information about how we use cookies on our website.

We use a third party data processor, Trafiki ecommerce UK, to host our website and help maintain its security and performance. To deliver this service it processes the IP addresses of visitors to the SRB website.

People who contact us via social media

If you send us a private or direct message via social media, we may share this information with SRB personnel (for example, in order to respond to a specific query or to pass on information). We will not share messages with any other organisations without your prior consent.

Queries and complaints

If you send a query or complaint to us, we will use the personal information you provide to us (for example, your name and the name(s) of any other individuals involved) in order to process your query or complaint and respond to you. Where we consider it necessary or appropriate, we will share this information with third parties such as the Solicitor's Regulation Authority.

1. How we use your information

We only ever use your personal data if we are satisfied that it is lawful and fair to do so because:

- you have given your consent to us using your information for the specific purposes described in this privacy notice
- it is necessary to enter into, or perform, a contract with you
- in order to comply with a legal obligation
- for our own (or a third party's) legitimate interests provided your rights do not override these interests. For example, we may use your personal data to comply for fraud and crime protection and for our network and information security measures, for any purpose required by law or our regulatory authority, for identifying usage trends and for data analytics as this information will help us review and improve our products, and services and under reasonable expectation to provide you with information you would expect to receive or that would benefit and enhance our relationship.

We will only use special categories of personal data relating to you or to third parties you tell us about when we have your explicit consent and/or where it is necessary to use the information for the establishment, exercise or defence of legal claims.

We will never sell your personal data or share it with third parties who might use it for their own purposes.

2. Sharing your information

We will not disclose any information you provide to any third parties other than:

- where you have given us consent to share the information
- where we instruct professional advisors on your behalf e.g. barristers, medical professionals, accountants, tax advisors or other experts
- other third parties where necessary to carry out your instructions e.g. your mortgage provider or HM Land Registry in the case of a property transaction or Companies House
- where information such as email addresses is passed to our third party service providers, who provide operational and technical support in order to make the delivery of our services more efficient. Operational and technical support is provided through information and technology systems such as case management, document management, time recording and email systems, typing services and the monitoring of our website and other technical systems

- if we are under a legal or regulatory duty to disclose or share your personal information (for example, if required to do so by a court order or for the purposes of prevention of fraud or other crime or in relation to audits, enquiries or investigations by regulatory bodies)
- in order to enforce any terms and conditions or agreements between us
- as part of a sale of some or all of our business and assets to any third party or as part of any business restructuring or reorganisation (we will always notify you in advance and we will aim to ensure that your privacy rights will continue to be protected)
- to protect our rights, property and safety, or the rights, property and safety of others (this includes exchanging information with our insurers, other companies, organisations and regulators for the purposes of fraud protection and credit risk reduction)

3. Data security

We have appropriate security measures in place to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We hold data electronically in our secure document management system and on our on-site file servers. Network infrastructure is protected using firewalls and anti-malware software. We also have off-site back-up servers in secure locations. We encrypt data leaving the firm on removable media and email, using industry standard encryption method that encrypts the data in transit. We regularly back up and encrypt all of the data we hold.

We store papers in lockable cabinets in our offices when not being actively used and we have a secure intranet storage facility for archived papers. Our offices are secure and only personnel with appropriate door codes can access areas where personal data are stored.

When necessary, we dispose of or delete your data securely.

We ensure that our employees, agents and contractors are aware of their privacy and data security obligations, and we take reasonable steps to ensure that employees of third parties working on our behalf are aware of their privacy and data security obligations.

We limit access to your personal information to those employees, agents, contractors and other third parties who have a need to know. Access to client data is restricted to the instructing team within the firm. The firm's business support teams may also have access to personal data (for example, to provide IT and document management support).

We may give third parties access to the personal information we hold about you in order to comply with our regulatory obligations (for example, the Solicitors Regulation Authority, our auditors or our professional indemnity insurers).

The transmission of information via the internet is never completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your electronic information transmitted to us and any transmission is at your own risk.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

4. Transferring your information outside the European Economic Area (EEA)

We do not transfer the information you give us to countries outside the EEA, except where the international transfer is necessary in connection with the legal services we are providing to you.

If we transfer your information outside of the EEA in this way, and the country in question has not been deemed by the EU Commission to have adequate data protection laws, we will provide appropriate safeguards and we will be responsible for ensuring your privacy rights continue to be protected as outlined in this notice.

If you are outside the EEA, your information may be transferred outside the EEA in order to provide you with our services. By submitting your personal information to us in this way you agree to the transfer and processing of your information outside the EEA.

5. Data retention

We have a Data Retention Policy which sets out our approach to the retention and deletion of the personal information we hold about you either in computer or manual files.

We will hold the information for as long as required by law, our regulatory obligations and any ongoing business relationship. Our default retention strategy for personal data is to retain personal data whilst there is an ongoing business relationship unless otherwise specified by law. Further details of what we regard as constituting “an ongoing business relationship” is set out in our Data Retention Policy which can be viewed on the SRB website at www.srb.co.uk

Please also note that personal data held on our client files may be retained for longer periods as it may be necessary to retain this data in order to allow our clients or third parties to protect their legal rights and claims. This data will not be generally accessible by our staff unless it is necessary in the context of a legal claim or request by a client or there is another overriding reason which justifies access to this data.

In relation to personal data that we receive through unsuccessful applications for job vacancies, our default retention period is for 12 months from the date of our last interaction with you. If your application is successful, the personal data that you provide during the application process will be retained by us as part of your employee file.

Retention periods may be extended or reduced if we deem it necessary (for example, to defend legal proceedings or if there is an on-going investigation relating to the information).

We review the personal data (and the categories of personal data) we are holding on a regular basis to ensure the data we are holding is still relevant to our business and is accurate. If we discover that certain data we are holding is no longer necessary or accurate, we will take reasonable steps to correct or delete this data as may be required.

6. Your rights

Under certain circumstances, by law you have the right to:

- request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it

- ask us to correct any information that we hold about you which is incorrect, incomplete or inaccurate
- ask us to erase your personal information from our files and systems where there is no good reason for us continuing to hold it
- object to us using your personal information to further our legitimate interests (or those of a third party) or where we are using your personal information for direct marketing purposes
- ask us to restrict or suspend the use of your personal information, for example, if you want us to establish its accuracy or our reasons for using it
- ask us to transfer your personal information to another person or organisation

7. Queries and complaints

Our Compliance and Data Protection Officer, Paul McNutt, oversees compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact pmc.management@srb.co.uk

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.