Privacy Policy

This Privacy Policy informs you about how we use any personal data which you provide to us, including through our websites at *www.sheppard-co.com*, our ("Site"). We are committed to protecting and respecting your privacy.

How our Privacy Policy works

Our Privacy Policy is divided into three parts:

- **Part A: General Privacy Notice** – this is our general notice about how we use personal data in our business and is directed at everyone about whom we may process personal data.
- **Part B: Client Privacy Notice** – this is our client-specific notice, which will also be applicable to everyone who is in the process of engaging, or has engaged us, to provide legal services.
- **Part C: Recruitment Privacy Notice** – this is our recruitment-specific notice, which will also be applicable to everyone submitting information to us for recruitment purposes (whether or not that's been solicited by us).

Parts B and C are supplemental to Part A and apply in addition as appropriate.

Part A: General Privacy Notice

1. Our role as data controller

When we use personal data about you or others in connection with promoting and administering our business, providing our services, or recruitment, we do so as data controller.

The data controller in England and Wales is **Aletheia Law Limited** of Central Court, 25 Southampton Buildings, London, WC2A 1 AL with registered office at 8th Floor, 167 Fleet Street, London, EC4A 2EA (together "**We/Our/Us**"). Aletheia Law Limited has overall responsibility for, and is the data controller of, personal data collected via the Site.

2. Your role in keeping your personal data up to date

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes.

3. Contact details of our Privacy Manager

We do not meet the criteria for a mandatory appointment of a Data Protection Officer under the General Data Protection Regulation. We have allocated informal responsibility to a person in our business who can deal with any data protection-related matters. You can contact our Privacy Manager by post at: Privacy Manager, Aletheia Law Limited, Central Court, 25 Southampton Buildings, London, WC2A 1 AL or by email at: enquiries@sheppard-co.com marking the subject line, 'For the attention of the Privacy Manager'.

4. Categories of personal data obtained

Personal data, or personal information, means any information about a living individual from which that person can be identified, directly or indirectly. We may collect different kinds of personal data about you when you interact with us, including via the Site, social media, email, telephone, post or in person. We may also receive this information from third parties (for example, a publicly available source or from someone who has recommended us to you and given us your contact details). We have grouped this information together as follows:

- **Identity Data**, such as your name.
- **Contact Data**, such as your email address, telephone/fax number, address and other contact details.
- **Enquiry Data**, such as your enquiries about engaging us for legal advice or job opportunities.
- **Correspondence Data**, such as any correspondence between us and you about an enquiry.
- **Technical Data**, such as your IP address, operating system, browser type and version, location and other information about how you use our Site.
- **Marketing and Communications Data**, such as your communications preferences and how you have responded to our marketing communications.
- **Tracking Data**, such as information we or others collect about you from cookies and similar tracking technologies, such as web beacons, pixels, and other digital identifiers.

We may from time to time collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your Technical Data to calculate the percentage of users accessing a specific Site feature, or we may aggregate your Marketing and Communications Data to calculate the percentage of recipients who open our email newsletter. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this Privacy Policy.

We do not usually collect any special categories of personal data about you, but you may choose to disclose this data to us. Special categories of personal data include details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data. Unless we are required to do so to comply with a legal obligation, or as an integral part of providing relevant legal services to you, we do not usually collect any personal data about you relating to criminal convictions or offences.

5. Use of personal data

Our core purposes for processing personal data are to promote and operate the business of being a law firm, to provide legal services to our clients, to maintain our client and business records, to recruit, and to comply with the law and regulations.

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where it is necessary for us in order to perform a **contract** which we are about to enter into, or

have entered into, with you (for example, a contract between you and us for us to provide legal advice to you).

- Where it is necessary for our **legitimate interests** (or those of a third party) and your interests and fundamental rights do not override those interests (for example, to monitor our IT systems and protect them).

- Where we need to **comply with a legal or regulatory obligation** (for example, the rules which require us to verify the identity of someone before they can become a client).

- Where we have your **consent** to do so (for example, if you are not a client and you ask us to sign you up for news and updates by email).

(Under the General Data Protection Regulation there are additional lawful bases, but these are the most relevant.)

6. Lawful basis, and any legitimate interests, for the processing

This table sets out in more detail the lawful basis we rely on to process personal data, depending on the category of personal data and the reason we are processing it. Note that we may process your personal data for more than one lawful basis depending on the specific purpose for which we are using your data.

Purpose/activity	**Type of data**	**Lawful basis for processing including basis of legitimate interest**
To provide the Site to you	(a) Technical Data	Legitimate interests (to promote our business and services via the web)
To register you as a recipient of our newsletters and updates	(a) Identity Data (b) Contact Data (c) Technical Data (d) Marketing and Communications Data	(a) Legitimate interests, including for any soft opt-in (to undertake direct marketing to promote our business and services) (b) In the limited circumstances where the Privacy and Electronic Communications Regulations mandate that consent is required for electronic marketing, and we are not relying on your opt-in, the lawful basis will be consent (See **Advertising, marketing and your communications preferences** below)
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Asking for feedback	(a) Identity Data (b) Contact Data (c) Enquiry Data (d) Correspondence Data (e) Marketing and Communications Data	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to ensure we

		provide our services on our most recently updated terms)
To register you as a new client and respond to your enquiry	(a) Identity Data (b) Contact Data (c) Enquiry Data (d) Correspondence Data	(a) Performance of a contract with you (b) Legitimate interests, including pursuing an opportunity to win you as a new client before ground (a) above applies
To administer and protect our business and our Site (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity Data (b) Contact Data (c) Enquiry Data (d) Correspondence Data (e) Technical Data (f) Marketing and Communications Data	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity Data (b) Contact Data (c) Enquiry Data (d) Correspondence Data (e) Technical Data (f) Tracking Data (g) Marketing and Communications Data	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our Site and the client experience	(a) Identity Data (b) Technical Data (c) Tracking Data	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform and deliver our marketing strategy)
To target potential new clients and lawyers via social media and the web	(a) Identity Data (b) Technical Data (c) Tracking Data	Necessary for our legitimate interests (to engage with the new clients and potential new lawyers via social media and the web (for example, via LinkedIn))

7. Sharing your personal data

As a law firm we comply with the SRA Code of Conduct ("**Code**"). The Code requires us to keep the affairs of our clients and prospective clients confidential, unless disclosure is required or permitted by law or consent. We may allow our officers, employees and self-employed consultants ("**colleagues**") to access your data where we believe this is necessary.

We may disclose personal data to the Solicitors Regulation Authority ("**SRA**"), HM Revenue & Customs, Information Commissioner's Office ("**ICO**") and any other regulators and other authorities who require reporting or disclosure of processing activities, or other personal data, in certain circumstances.

We may share your data with third parties to whom we have outsourced certain tasks, such as IT, business administration or marketing and analytics services.

We may share your personal data with our insurers, our professional advisors (lawyers, bankers, auditors, corporate financiers and brokers) in connection with services they provide to us.

For more information on personal data sharing connected to advertising and marketing, see

Advertising, marketing and your communications preferences below.

We may also share data with third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this Privacy Policy.

We require all third parties to respect the security of personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

We will not otherwise share personal information with any third party except where we are permitted to under data protection laws or required to by law.

8. Advertising, marketing and your communications preferences

We may use your Identity, Contact, Technical and Tracking Data to form a picture of what we think may be of relevance to you. You can also unsubscribe at any time to any email we send you by using or emailing susannah.sheppard@sheppard-co.com and requesting an opt out.

9. International transfers

Prior to 1 January 2021

We may hold copies of your personal data and other data on computers outside the European Economic Area (EEA). Sometimes we will share personal data with third parties outside the EEA. If we do this, we will comply with the rules in the General Data Protection Regulation. Whenever we transfer your personal data out the EEA, we ensure a similar degree of protection is afforded to it, either by making our own assessment of adequacy, or using one of the standard mechanisms available to us. These may include:

- Transfer to countries or organisations that have officially been deemed to provide an adequate level of protection for personal data by the European Commission (a list of which is available here).

- Using specific contracts approved by the European Commission which give personal data the same protection it has in Europe (called the "**EU Model Clauses**").

- Where we use providers based in the US, we may transfer data to them if they are part of the

Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US. If the provider is not EU-US Privacy Shield certified, we may use the EU Model Clauses.

From 1 January 2021

The General Data Protection Regulation will no longer apply to us and any transfers of personal data outside the UK that we make will be made in compliance with the UK General Data Protection Regulation.

For data transfers taking place outside of the UK from then, we ensure that a similar degree of protection is afforded to it, either by making our own assessment of adequacy, or using one of the standard mechanisms available to us. These may include:

- Transfers to the EEA because these have been confirmed by the Information Commissioner's Office as being adequate.
- Transfer to countries or organisations that have officially been deemed to provide an adequate level of protection for personal data by the Information Commissioner's Office (which for the moment is the same list as the European Commission list referred to above).
- Using specific contracts approved by the Information Commissioner's Office (which for the moment is to continue to use the Standard Contractual Clauses).

If you are transferring personal data to us from the EEA, in the absence of an adequacy ruling for the United Kingdom, the arrangements agreed between the UK and EU in the UK-EU Trade and Cooperation Agreement shall apply to legitimise the transfer. These arrangements are stated to last for no more than six months and are to allow time for the UK to be granted adequacy. If you are a client and wish us to put in place controller-to-controller Standard Contractual Clauses specifically for you, please let us know.

10. Safeguarding personal data

We have put in place appropriate technical and organisational measures to safeguard your personal data including using systems with end-to-end encryption.

11. Retaining personal data

We will only keep your personal data for as long as necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Unless Part B or Part C of this Privacy Policy apply, or you are still receiving our newsletter or updates, we will delete your data within two years of the date we receive it.

12. Your rights

We set out below a summary of the rights you may have under data protection laws in relation to your personal data.

- **Request access** to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you.

- **Request correction** of your personal data. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for our continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

- **Object to processing** of your personal data where we are relying on our legitimate interests (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

- **Request restriction of processing** of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

- **Request the transfer** of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which we were originally using with your consent or on account of our need to perform a contract with you. This may not be all the information we hold about you.

- **Withdraw consent at any time** where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain services to you. We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the rights set out above, please contact the Privacy Manager.

We cannot advise you in connection with our use of your data. If you need legal advice on this subject, then you will need to consult another firm.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you.

13. Supervisory authority

In the United Kingdom we are supervised by the Information Commissioner's Office (ICO). You can find out more about the ICO through its website: www.ico.org.uk. We would be happy to answer your questions and address your concerns regarding our use of your data. Please email us at enquiries@sheppard-co.com and mark your email for the attention of the Data Manager. Please also use that address for any requests to exercise your legal rights or if you have a complaint. Alternatively, you can make a complaint to the ICO at any time, but we prefer you to contact us first. We should be able to resolve the matter quickly and to your satisfaction.

14. Third-party links

Our Site may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements.

15. Updating our Privacy Policy

We regularly update this Privacy Policy. The latest version is always displayed on our Site and available on request.

Part B: Additional Client Privacy Notice

1. Categories of personal data obtained

We may collect additional categories of personal data about you when you instruct us or seek to instruct us, including via the Site, email, telephone, post or in person. We may also receive this information from third parties (for example, a publicly available source or from someone who has recommended us to you and given us your contact details). We have grouped this information together follows:

- **Identity Data**, such as copies of your passport, driving licence, birth certificate, national identity card, utility bills and/or other identifying information required to be provided to us for anti-money laundering purposes.

- **Matter Data**, which includes any personal data about you connected with your instructions to us, including correspondence between us, notes of our calls and meetings, and third party information about your matter.

- **Financial Data**, which includes bank account and/or other billing details.

- **Transaction Data**, which includes details about the costs of the matter and any payments to and from you.

2. Use of personal data

Our core purposes for processing personal data are to operate the business of being a law firm, to provide legal services to our clients, to maintain our client and business records and to comply with the law and regulations. In relation to you (or the organisation on behalf of which you instruct us) this

primarily involves: providing you with legal advice or other information that you have requested from us; invoicing you for services we have undertaken for you; keeping records of the work we have carried out for you; and fulfilling our anti-money laundering obligations.

3. Lawful basis, and any legitimate interests, for the processing

This table sets out in more detail the lawful basis we rely on to process personal data, depending on the category of personal data and the reason we are processing it. Note that we may process your personal data for more than one lawful basis depending on the specific purpose for which we are using your data.

Purpose/Activity	**Type of data**	**Lawful basis for processing including basis of legitimate interest**
To undertake anti-money laundering checks and conflict checks	(a) Identity Data (b) Matter Data (c) Financial Data	(a) Necessary to comply with a legal obligation (b) Necessary for our legitimate interests (to administer the client opening process)
To undertake the core task of providing legal advice to you and progressing your matter as instructed (using personal data)	(a) Identity Data (b) Matter Data	(a) Performance of a contract (b) Necessary for our legitimate interests (to recover debts due to us)
To undertake the core task of providing legal advice to you and progressing your matter as instructed (using special category data)	Special categories of personal data include details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data	(a) Performance of a contract (b) Explicit consent, given by way of the engagement letter or on a case-by-case basis
To undertake the core task of providing legal advice to you and progressing your matter as instructed (using criminal convictions and offences data)	Personal data about you relating to criminal convictions or offences	(a) Performance of a contract (b) Explicit consent, given by way of the engagement letter or on a case-by-case basis
To liaise with third parties as necessary to progress your matter as instructed (e.g. overseas law firms, patent agents, forensic accountants, experts or barristers)	(a) Identity Data (b) Matter Data (c) Financial Data (d) Transactional Data	(a) Performance of a contract (b) Necessary for our legitimate interests (to liaise with other professionals as necessary to progress your matter)
To manage payments, fees and charges	(a) Matter Data (b) Financial Data (c) Transactional Data	Necessary in our legitimate interests (to undertake fraud checks and take payment for our services)
To collect and recover money	(a) Matter Data	Necessary in our legitimate interests (to collect money

owed to us	(b) Financial Data (c) Transactional Data	owed to us)

4. Sharing personal data

In order to provide you (or your organisation) with our services, we may provide personal data to the courts, to lawyers advising other parties in your matter, or to other professionals (such as overseas law firms, patent agents, forensic accountants, experts or barristers).

5. Retaining personal data

We store some files digitally and others in hard copy. In each case we may use third parties to store your files. We keep matter files for six to eight years, or longer if required by law. This is explained in more detail in our Information Retention Policy. Clients can request a copy of this any time.

6. Destruction and retrieval

We will destroy your files at the end of their storage period, or earlier with client consent. Please write and tell us if you object to this. We will charge you if you want us to retrieve your files after we have completed our work.

7. Source of the personal data

Most of the personal data we process will be obtained directly from you, but we may also acquire personal data about you (and others) from other parties connected with you or your matter. We also get data from publicly available sources.

8. Failure to provide personal data

Other than where compelled to do so by a court or relevant law or regulation, you are not under any obligation to provide personal data to us. However, if we need personal data to carry out our duties (for example, anti-money laundering and conflict checks), and you do not provide this information, we may not be able to continue to act for you. If this happens, we will inform you.

Part C: Recruitment Privacy Notice

1. Categories of personal data obtained

We may collect additional categories of personal data about you when you apply to join us, including via the Site, email, telephone, post or in person. We may also receive this information from third parties (for example, a publicly available source or from someone who has recommended you to us and given us your CV). We have grouped this information together as follows:

- **Identity Data**, such as a copy of your passport and your date of birth.
- **Career Data**, such as details about your education and qualifications, your skills and your experience/career.
- **Financial Data**, such as your salary history and bank account and tax details.

2. Why and how we use personal data

Our core purposes for processing personal data are to operate the business of being a law firm, to recruit and maintain staff and lawyers and to comply with the law and regulations. In relation to you this primarily involves considering your personal data in the context of our hiring and business development needs and complying with our legal and regulatory obligations.

3. Lawful basis, and any legitimate interests, for the processing

The table below sets out in more detail the lawful basis we rely on to process personal data, depending on the category of personal data and the reason we are processing it. Note that we may process your personal data for more than one lawful basis depending on the specific purpose for which we are using your data.

Purpose/Activity	**Type of data**	**Lawful basis for processing including basis of legitimate interest**
Reviewing your career, checking your identity, assessing your suitability to join us and corresponding with you about this	(a) Identity Data (b) Career Data (c) Financial Data	Necessary for our legitimate interests (to recruit persons suitable to work in a regulated law firm)
Preliminary steps in your joining the firm (e.g. making you an offer or setting up payment mechanics)	(a) Identity Data (b) Career Data (c) Financial Data	Necessary for our legitimate interests (to recruit persons suitable to work in a regulated law firm and to effect payments to successful candidates)

4. Sharing personal data

If we share your personal data, we will require the recipient to keep it confidential and secure. We may share your personal data with our insurers, our regulators, our professional advisors, our colleagues and our overseas branches. In order to provide you (or your organisation) with our services, we may provide personal data to the courts, to lawyers advising the other parties to a matter, or to other professionals (such as overseas law firms, patent agents, forensic accountants, or barristers). We will not otherwise share personal information with any third party except where we are permitted to under data protection laws.

We will use your data to conduct a disclosure barring service check (also sometimes referred to by its old name, a CRB check) and to verify your identity.

5. Retaining personal data

If your application is successful, then we will enter into more detailed binding documentation which will include a further privacy notice. That privacy notice will explain how we process your data once you have joined us.

If your application is unsuccessful, then we will delete your data within two years of the date when we reject your application or you withdraw your candidacy, as appropriate.

6. Source of the personal data

Most of the personal data we obtain will be directly from you, but we may also obtain personal data about you (and others) in the course of undertaking our recruitment activities. We may also obtain further personal data about your from publicly available sources.

7. Failure to provide personal data

We cannot properly consider your application to join us unless you go through our normal application process which includes a consideration of your CV and attending one or more interviews.

8. Automated decision making, including profiling

We do not currently use any automated decision making, or profiling, as part of our recruitment practices. If we do so, this will be subject to separate arrangements and a different privacy notice.