

PRIVACY NOTICE

Summary

These arrangements apply to each law firm in the Spencer West network and also to Spencer West Global Limited (each of which is referred to as “Spencer West”, “we” or “us”).

We use your personal data to provide legal services, manage our business, recruit new colleagues, comply with our legal obligations, monitor and improve the performance of our digital platforms, and provide marketing communications where you have requested them.

We may add your personal data to our global contact database administered by Spencer West Global Limited ("Spencer West Global"), and used by the Spencer West network of law firms, particularly if you are a client or prospective client

We respect your privacy and are committed to protecting your personal data. We have measures in place to safeguard your personal data when we transfer it internationally. We take steps to minimise the amount of personal data we hold about you and to keep it secure. We delete your personal data when we no longer need it, and we have policies in place to govern when that is. You have a number of rights in relation to your personal data. For further details about how we process your personal data, please see the relevant Privacy Notice below.

If you have any questions about how we use your data, please contact our Data Protection Officer at dpo@spencer-west.com.

Who are you?

A client or prospective client, someone who has signed up to receive communications from us, or is browsing our website

This Privacy Notice applies to clients and potential clients (“you” and “your”) of each of our law firms in the Spencer West network. It informs you how we look after your personal data and about your privacy rights.

You should read this Privacy Notice so that you know what personal data we collect about you, what we do with it and how you can exercise your rights in connection with it.

SPENCER WEST LLP Longbow House, 20 Chiswell Street, London EC1Y 4TW

T +44 (0)20 7925 8080 | F +44 (0)20 7681 2600 | info@spencer-west.com | www.spencer-west.com

Spencer West LLP is a limited liability partnership registered in England and Wales at the above address at which service of documents will be effective. Registered no. OC360298. Authorised and regulated by the Solicitors Regulation Authority: SRA No. 555456. A list of members of Spencer West LLP is available for inspection at the registered office. The term ‘partner’ in relation to Spencer West LLP is used to refer to a member, an employee or consultant of Spencer West LLP and the reference to such persons as partners of Spencer West LLP does not suggest that they are part of a general partnership.

1. **Controller**
2. **The data we collect about you**
3. **How we use your personal data and legal basis for doing so**
4. **Who we share your personal data with**
5. **International transfers**
6. **Data security**
7. **Retention of personal data**
8. **How to access your information and your other rights**
9. **Changes to this Privacy Notice**

1. Controller

A controller is the organisation that makes the decisions about what data is processed and is responsible for your personal data.

For the purposes of the activities set out in this notice, the main controller will be the Spencer West law firm that is providing you and/or your organisation with legal services.

Please visit our website www.spencer-west.com for details of all the Spencer West law firms and their contact details.

We have a Global Data Protection Officer, Kristy Gouldsmith, whom you may contact by email at dpo@spencer-west.com or write to at:

Spencer West
Longbow House
20 Chiswell Street
London EC1Y 4TW

The law firms and their data are supported from an administrative perspective by Spencer West Global, a limited liability company registered in England and Wales. Spencer West Global is the controller in respect of personal data processed in connection with our website www.spencer-west.com. Spencer West Global is a joint controller of your data. This privacy notice is also provided to you on behalf of Spencer West Global.

Some of our Spencer West lawyers operate as consultants at the relevant Spencer West law firm. They may be engaged directly by the relevant law firm as a self-employed consultant, or they may work through a service company.

Where we work with a consultant to provide you with legal services, this privacy notice is also provided to you on behalf of the consultant. Where the consultant is engaged through a service company, this Privacy Notice is also provided on behalf of the relevant service company.

2. The data we collect about you

In your capacity as our client or prospective client, we may collect personal data from you. Personal data means any information about an individual from which that person can be identified.

Our primary goal in collecting personal data from you is to help us:

- verify your identity
- comply with our legal obligations
- deliver our services
- improve, develop and market new services
- investigate or settle enquiries or disputes
- comply with any applicable law, court order, other judicial process, or the requirements of a regulator; and
- enforce our agreements with you.

We use different methods to collect data from and about you, including through:

<p>Direct interactions</p>	<p>You may give us your personal data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:</p> <p>apply for further information about our services using our contact form or otherwise;</p> <p>subscribe to our information emails;</p> <p>request marketing to be sent to you; or</p> <p>give us some feedback.</p>
<p>Automated technologies or interactions</p>	<p>As you interact with our website, we will collect data about your device, your browsing actions and patterns when you consent to our use of cookies.</p>
<p>Third parties or publicly available sources</p>	<p>We may receive personal data about you from various third parties and public sources including those set out below:</p> <p>Land Registry</p> <p>Companies House</p> <p>The Insolvency Service</p> <p>Electoral Roll</p> <p>Publicly available sources</p> <p>Other professionals, including surveyors, accountants, solicitors or barristers.</p>

Individual clients

If you are an individual client in receipt of our services or a prospective individual client, we will collect the following data: below:

- Name and job title
- Address, email, and phone number
- Gender and date of birth
- Contact information including the company you work for and email address, where provided
- Payment information, if necessary

- Information that you provide to us as part of us providing the services to you, which depends on the nature of your instructions to us, but that could include information about other people
- Relevant information, such as proof of address or identity, as required by anti-money laundering (AML). We need to check that you are using our services legally. To do this, we use providers that perform various checks for us in relation to AML, fraud and other 'know your client' related checks.

The following searches are made:

- Electoral roll
- Postcode address files
- Consent databases
- Telephone directories
- Mortality registers
- Politically Exposed Persons (PEP) Intelligence databases
- Sanctions databases
- Birth Index Register
- Age range
- Bank account validation and verification.

We need this data in order to provide you with our services; without it, we are unable to provide our services to you. We will continue to process personal data to satisfy our client due diligence obligations throughout the time that you are our client.

Corporate clients

When we are engaged by corporate entities, those providing instructions are not data subjects. However, as part of such instructions, personal data may be provided to us (e.g. personal data relating to officers or personnel of our corporate client).

We will ask you to provide us with personal data of the owners, directors, partners and persons with significant control of the business and we may require you to provide us with additional personal data as you use our services.

We will collect, store and process the following personal data of the above-named individuals:

- Full name
- Email address
- Date of birth
- Home address
- Proof of address
- Proof of identity
- Other client due diligence information as required to on-board the company and meet our legal requirements, such as AML, fraud prevention, conflict checks and PEP checks.

We need to check that you are using our services legally. To do this, we use providers that perform various checks for us in relation to AML, fraud and other 'know your client' related checks.

The following searches are made:

- Electoral roll
- Postcode address files
- Consent databases
- Telephone directories
- Mortality registers
- PEP Intelligence databases
- Sanctions databases
- Birth Index Register
- Age range
- Bank account validation and verification

We need this data in order to provide you with our services; without it, we are unable to provide our services to you. We will continue to process personal data to satisfy our client due diligence obligations throughout the time that you are our client.

For all sole traders, limited companies or partners in unincorporated partnerships we will also collect: billing information, including bank account information and payment information.

Third parties

We may also need to process personal data in relation to third parties instructed either by our own clients or other persons or companies involved with us providing the services to our client (for instance other law firms, experts etc.).

This is a non-exhaustive list which is reflective of the varied nature of the personal data processed as part of a law firm providing legal services.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract that we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with services). In this case, we may have to cancel a service that you have with us but we will notify you if this is the case at the time.

3. How we use your personal data and legal basis for doing so

We may use your information for the following purposes:

Action	Reason	Legal basis
Responding to enquiries	<p>Our website allows you to request information about our services using an electronic enquiry form.</p> <p>Contact information is required in each case, together with details of other personal data that is relevant to your service enquiry.</p> <p>This information is used to enable us to respond to your requests.</p>	We are using your data with your consent to respond to your enquiry.
Fulfilment of services	We collect and maintain personal data that you voluntarily submit to us to enable us to provide our services. In order to do this, we need to enter your data onto our systems.	Legitimate interest.
Fulfilment of services	It is necessary for us to process your information to perform our obligations in accordance with any contract that we may have with you. This includes recording how much time we spend on your matter(s) and taking payment information.	We have a contract with you.
Fulfilment of services	We need to ensure that we provide the best client service that we can to you or others.	It is in our legitimate interest or a third party's legitimate interest to use your personal data this way.
Resolving complaints or disputes	We need to be able to resolve any complaints or disputes with you.	Legitimate interest.

Legal compliance	We use your personal data to comply with our legal obligations, including anti-money laundering, conflicts and our regulatory and statutory obligations.	It is our legal obligation to use your personal data to comply with any legal obligations imposed upon us.
Marketing communications	For clients and prospects, we use your personal data to send you information about our services which may be of interest to you. We may also conduct surveys to improve our services.	It is in our legitimate interest to use your personal data for marketing purposes and you can unsubscribe at any time.

Our business requirements – legitimate interests

Action	Reason for processing – legitimate interest
Managing our global business and marketing strategies (including recording and reporting on our business development activities).	We need to have business development and marketing strategies.
Purchasing, maintaining and claiming against our insurance policies.	We need to protect our business.
Continuously reviewing and improving our services and developing new ones.	We use your feedback to improve our services.
Obtaining legal advice, establishing, defending and enforcing our legal rights and obligations in connection with any legal proceedings or prospective proceedings.	We need to understand our obligations and establish and defend our legal rights.
Monitoring and producing statistical information regarding the use of our platforms, and analysing and improving their functionality.	We need to ensure that our website and other platforms are working properly.
Maintaining the security of our systems, platforms, premises and communications, including detecting and preventing threats.	We need to ensure that our premises and our platforms are secure.
Managing the proposed sale, restructuring, transfer or merging of any or all part(s) of our business, including responding to queries from the prospective buyer or merging organisation.	We need to be able to manage or sell parts of our business, if we choose to do so.

We have a legitimate interest in using your personal data for the above purposes. We have balanced your rights and freedoms against our business needs. Please inform us if you object to our processing.

Special category data

The UK GDPR defines special category data as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

Special category data needs more protection because it is more sensitive than regular personal data, such as name and email.

In order lawfully to process special category data, the controller must identify both a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9. These do not have to be linked

Our reason for processing your data

Action	Reason for processing – legitimate interest
Hosting you at our offices and providing hospitality services.	Explicit consent for us to use either your health or religious information to provide refreshments.
Accidents or emergencies while you are at our office.	it is necessary for us protect your vital interests or when you are incapable of giving consent.
Providing you with legal advice.	It is necessary for the establishment, exercise or defence of legal claims.
Investigating, evaluating, demonstrating, monitoring, improving and reporting on our compliance with our legal and regulatory requirements (such as AML and client verification checks).	ntial public interest.
Complying with regulatory requirements involving steps being taken to establish the existence of any unlawful act, dishonesty, malpractice or other serious improper conduct.	ntial public interest.
Responding to binding requests or search warrants or orders from courts, governmental, regulatory and/or enforcement bodies and authorities or sharing information (on a voluntary basis) with the same.	ntial public interest.
Obtaining legal advice, establishing, defending and enforcing our legal rights and obligations in connection with, any legal proceedings, including prospective proceedings.	ntial public interest.

4. Who we share your personal data with

We may share personal data with a variety of the following categories of third parties as necessary:

Entity	Legal basis for sharing
Our professional advisers such as lawyers and accountants.	Legitimate interest.
Government or regulatory authorities or law enforcement.	Legal obligation.
Professional indemnity or other relevant insurers.	Legitimate interest.
Regulators/tax authorities/corporate registries.	Legal obligation.
Third parties to whom we outsource certain services such as, without limitation, document processing and translation services, confidential waste disposal, IT systems or software providers, IT support service providers, document and information storage providers.	Legitimate interest.
Third parties engaged in the course of the services we provide to clients such as counsel, arbitrators, mediators, clerks, witnesses, cost draftsmen, court, opposing party and their lawyers, document review platforms and experts such as tax advisers or valuers.	Legitimate interest or a contractual requirement to provide our services.
Third party service providers to assist us with client insight analytics, such as Google Analytics.	Consent.

Please note this list is non-exhaustive and there may be other examples where we need to share personal data with other parties in order to provide our services as effectively as we can.

We conduct an appropriate level of due diligence and put in place contractual documentation in relation to any sub-contractor to ensure that they process personal data appropriately and according to our legal and regulatory obligations.

Further, we may appoint external data controllers where necessary to deliver the services (for example, accountants, barristers or other third party experts). When doing so we will comply with our legal and regulatory obligations in relation to the personal data and put appropriate safeguards in place.

5. International transfers

Spencer West is a network of different law firms operating around the world. As such, we will sometimes need to transfer your personal data to recipients in jurisdictions other than your own. Some of these jurisdictions may not provide the same level of protection to your personal data as provided in your jurisdiction. If we transfer your personal data outside the United Kingdom or the European Union, we will only make that transfer if:

- that country ensures an adequate level of protection for your personal data;
- we have put in place appropriate safeguards to protect your personal data, such as a contract with the person or entity receiving your personal data which incorporates specific provisions as directed by the European Commission and the UK government;
- the transfer is permitted by applicable laws; or
- you explicitly consent to the transfer.

If you would like to see a copy of any relevant safeguards used by us to protect the transfer of your personal data, please contact our Global Data Protection Officer at: dpo@spencer-west.com.

6. Data security

We are committed to keeping the personal data provided to us secure and we have implemented appropriate information security policies, rules and technical measures to protect the personal data that we have under our control from unauthorised access, improper use or disclosure, unauthorised modification and unlawful destruction or accidental loss.

All of our partners, employees, consultants, workers and data processors (i.e. those who process your personal data on our behalf, for the purposes listed above), who have access to, and are associated with the processing of personal data, are obliged to respect the confidentiality of such personal data.

7. Retention of personal data

By law, we have to keep basic information about our clients (including contact, identity, financial and file information) for a minimum of six years, and in some cases up to twelve years, after they cease being clients.

8. How to access your information and your other rights

You have the following rights in relation to the personal data that we hold about you:

- **Your right of access:** if you ask us, we will confirm whether we are processing your personal data and, if necessary, provide you with a copy of that personal data (along with certain other details). If you require additional copies, we may need to charge a reasonable fee.
- **Your right to rectification:** if the personal data that we hold about you is inaccurate or incomplete, you are entitled to request to have it rectified. If you are entitled to rectification and if we have shared your personal data with others, we will let them know about the rectification where possible. If you ask us, where possible and lawful to do so, we will also tell you who we have shared your personal data with so that you can contact them directly.
- **Your right to erasure:** you can ask us to delete or remove your personal data in some circumstances, such as where we no longer need it or if you withdraw your consent (where applicable). If you are entitled to erasure and if we have shared your personal data with others, we will let them know about

the erasure where possible. If you ask us, where it is possible and lawful for us to do so, we will also tell you who we have shared your personal data with so that you can contact them directly.

- **Your right to restrict processing:** you can ask us to 'block' or suppress the processing of your personal data in certain circumstances, such as where you contest the accuracy of that personal data or you raise an objection with us. If you are entitled to restriction and if we have shared your personal data with others, we will let them know about the restriction where it is possible for us to do so. If you ask us, where it is possible and lawful for us to do so, we will also inform you who we have shared your personal data with so that you can contact them directly.
- **Your right to data portability:** you have the right, in certain circumstances, to obtain personal data that you have provided us with (in a structured, commonly used and machine readable format) and to reuse it elsewhere or to ask us to transfer this to a third party of your choice.
- **Your right to object:** you can ask us to stop processing your personal data, and we will do so, if we are:
 - relying on our own or someone else's legitimate interests to process your personal data, except if we can demonstrate compelling legal grounds for the processing; or
 - processing your personal data for direct marketing purposes.
- **Your right to withdraw consent:** if we rely on your consent (or explicit consent) as our legal basis for processing your personal data, you have the right to withdraw that consent at any time.
- **Your right to lodge a complaint with the Supervisory Authority:** if you have a concern about any aspect of our privacy practices, including the way we have handled your personal data, you can report it to the Supervisory Authority in your country. We would, however, appreciate the chance to deal with your concerns before you approach the Supervisory Authority, so please contact us in the first instance.

Please note that some of these rights may be limited where we have an overriding interest or legal obligation to continue to process the data, or where data may be exempt from disclosure due to reasons of legal professional privilege or professional secrecy obligations.

9. Changes to this Privacy Notice

To ensure that you are always aware of how we use your personal data, we will update this Privacy Notice from time to time to reflect any changes to our use of your personal data. We may also make changes as required to comply with changes in applicable law or regulatory requirements. Where it is practicable, we will notify you by email of any significant changes. However, we encourage you to review this Privacy Notice periodically to be informed of how we use your personal data.

Applying or enquiring to become a Partner, consultant, employee, contractor, temporary or agency worker at Spencer West

This Privacy Notice explains how and why Spencer West uses personal data about individuals who apply or enquire about applying to become our Partners, consultants, employees, contractors, trainees, work experience students, vacation scheme students, apprentices and temporary or agency workers (referred to as “applicants” or “you”). You should read this Privacy Notice, so that you know what personal data we collect about you, what we do with it and how you can exercise your rights in connection with it. Please also read any other applicable Privacy Notices that might apply to you, for example the relevant Privacy Notice if you are successful in your application to join us.

This Privacy Notice does not form part of any contract between us and you (including any contract of employment that may be offered or any other services contract).

- 1. Controller**
- 2. The data we collect about you**
- 3. How we use your personal data and legal basis for doing so**
- 4. Who we share your personal data with**
- 5. International transfers**
- 6. Data security**
- 7. Retention of personal data**
- 8. How to access your information and your other rights**
- 9. Changes to this Privacy Notice**

1. Controller

A controller is the organisation that makes the decisions about what data is processed and is responsible for your personal data.

For the purposes of the activities set out in this Privacy Notice, the main controller will be the Spencer West law firm that is recruiting.

Please visit our website www.spencer-west.com for details of all the Spencer West law firms and their contact details.

We have a Global Data Protection Officer, Kristy Gouldsmith, whom you may contact by email at dpo@spencer-west.com or write to at:

Spencer West
Longbow House
20 Chiswell Street
London EC1Y 4TW

The law firms and their data are supported from an administrative perspective by Spencer West Global, a limited liability company registered in England and Wales. Spencer West Global is a joint controller of your data. This Privacy Notice is also provided to you on behalf of Spencer West Global.

2. The data we collect about you

We collect information about our applicants and we process it on an on-going basis. We will process the following data:

- Your application form containing your name, contact details, education and qualifications
- A copy of each reference obtained for you
- Documentary evidence of any qualifications
- In order to employ or engage you, we are required to establish your identify and your right to work in the UK or other relevant jurisdiction where you are being employed or engaged. We will need a copy of your birth certificate and passport (if any) (name, date of birth, nationality, photo, passport number)
- If you require reasonable adjustments in order to attend for an interview, then we will process your health data
- Your image captured by CCTV
- Information about you from your referees
- For UK applicants, we will conduct a Standard DBS check which will contain details of both spent and unspent convictions, cautions, reprimands and warnings that are held on the Police National Computer, which are not subject to filtering.

3. How we use your personal data and legal basis for doing so

We ask you for personal details to assess your suitability as a candidate and to provide the best possible recruitment experience.

We may use your information for the following purposes:

Action	Legal basis
Your submission of your CV or application.	Consent.
We will then process the data in your application or CV and the data collected on you during the recruitment process in order to assess your suitability for the position.	Legitimate interest.
Right to work checks.	Legal obligation.
<p>We hold your CV and all data collected during the recruitment process for six months in the unlikely event of any court or employment tribunal claims.</p> <p>All personal data is stored securely on servers and in the cloud.</p> <p>Images captured by CCTV for the safety and security of our clients, staff and visitors.</p>	Legitimate interest.
Information in order to make reasonable adjustments for you to attend an interview.	Legal obligation.
Legal compliance.	It is our legal obligation to use your personal data to comply with any legal obligations imposed upon us.
DBS check.	Consent.

Special category data

The (UK) GDPR defines special category data as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person’s **sex life**; and
- data concerning a person’s **sexual orientation**.

Special category data needs more protection because it is sensitive than regular personal data, such as name and email.

Action	Reason for processing – legitimate interest
Hosting you at our offices and providing hospitality services.	Explicit consent for us to use either your health or religious information to provide refreshments.
Accidents or emergencies while you are at our office.	it is necessary for us protect your vital interests or when you are incapable of giving consent.
Providing you with any reasonable adjustments	Legal obligation.

4. Who we share your personal data with

We may share personal data with a variety of the following categories of third parties as necessary:

Entity	Legal basis
Our professional advisers such as lawyers and accountants.	Legitimate interest.

Government or regulatory authorities or law enforcement.	Legal obligation.
Professional indemnity or other relevant insurers.	Legitimate interest.
Third parties to whom we outsource certain services such as, without limitation, document processing and translation services, confidential waste disposal, IT systems or software providers, IT support service providers, document and information storage providers.	Legitimate interest.

Please note this list is non-exhaustive and there may be other examples where we need to share personal data with other parties in regard to your employment or engagement.

We conduct an appropriate level of due diligence and put in place contractual documentation in relation to any sub-contractor to ensure that they process personal data appropriately and according to our legal and regulatory obligations.

5. International transfers

Spencer West is a network of different law firms operating around the world. As such, we will sometimes need to transfer your personal data to recipients in jurisdictions other than your own eg. to our head office in the UK. Some of these jurisdictions may not provide the same level of protection to your personal data as provided in your jurisdiction. If we transfer your personal data outside the European Union or the United Kingdom, we will only make that transfer if:

- that country ensures an adequate level of protection for your personal data;
- we have put in place appropriate safeguards to protect your personal data, such as a contract with the person or entity receiving your personal data which incorporates specific provisions as directed by the European Commission and the UK government;
- the transfer is permitted by applicable laws; or
- you explicitly consent to the transfer.

If you would like to see a copy of any relevant safeguards used by us to protect the transfer of your personal data, please contact our Global Data Protection Officer at: dpo@spencer-west.com.

6. Data security

We are committed to keeping the personal data provided to us secure and we have implemented appropriate information security policies, rules and technical measures to protect the personal data that we have under our control from unauthorised access, improper use or disclosure, unauthorised modification and unlawful destruction or accidental loss.

All of our partners, employees, consultants, workers and data processors (i.e. those who process your personal data on our behalf, for the purposes listed above), who have access to, and are associated with the processing of personal data, are obliged to respect the confidentiality of such personal data.

7. Retention of personal data

We keep all recruitment information for a period of six months in case of any employment tribunal or court claims. The data of the successful candidate will form the start of their HR file.

8. How to access your information and your other rights

You have the following rights in relation to the personal data that we hold about you:

- **Your right of access:** if you ask us, we will confirm whether we are processing your personal data and, if necessary, provide you with a copy of that personal data (along with certain other details). If you require additional copies, we may need to charge a reasonable fee.
- **Your right to rectification:** if the personal data that we hold about you is inaccurate or incomplete, you are entitled to request to have it rectified. If you are entitled to rectification and if we have shared your personal data with others, we will let them know about the rectification where possible. If you ask us, where possible and lawful to do so, we will also tell you who we have shared your personal data with so that you can contact them directly.
- **Your right to erasure:** you can ask us to delete or remove your personal data in some circumstances, such as where we no longer need it or if you withdraw your consent (where applicable). If you are entitled to erasure and if we have shared your personal data with others, we will let them know about the erasure where possible. If you ask us, where it is possible and lawful for us to do so, we will also tell you who we have shared your personal data with so that you can contact them directly.
- **Your right to restrict processing:** you can ask us to 'block' or suppress the processing of your personal data in certain circumstances, such as where you contest the accuracy of that personal data or you raise an objection with us. If you are entitled to restriction and if we have shared your personal data with others, we will let them know about the restriction where it is possible for us to do so. If you ask us, where it is possible and lawful for us to do so, we will also inform you who we have shared your personal data with so that you can contact them directly.
- **Your right to data portability:** you have the right, in certain circumstances, to obtain personal data that you have provided us with (in a structured, commonly used and machine readable format) and to reuse it elsewhere or to ask us to transfer this to a third party of your choice.
- **Your right to object:** you can ask us to stop processing your personal data, and we will do so, if we are:

- relying on our own or someone else's legitimate interests to process your personal data, except if we can demonstrate compelling legal grounds for the processing; or
 - processing your personal data for direct marketing purposes.
- **Your right to withdraw consent:** if we rely on your consent (or explicit consent) as our legal basis for processing your personal data, you have the right to withdraw that consent at any time.
 - **Your right to lodge a complaint with the Supervisory Authority:** if you have a concern about any aspect of our privacy practices, including the way we have handled your personal data, you can report it to the Supervisory Authority in your country. We would, however, appreciate the chance to deal with your concerns before you approach the Supervisory Authority, so please contact us in the first instance.

Please note that some of these rights may be limited where we have an overriding interest or legal obligation to continue to process the data, or where data may be exempt from disclosure due to reasons of legal professional privilege or professional secrecy obligations.

9. Changes to this Privacy Notice

To ensure that you are always aware of how we use your personal data, we will update this Privacy Notice from time to time to reflect any changes to our use of your personal data. We may also make changes as required to comply with changes in applicable law or regulatory requirements. Where it is practicable, we will notify you by email of any significant changes. However, we encourage you to review this Privacy Notice periodically to be informed of how we use your personal data.

Employees at Spencer West

This Privacy Notice explains how and why Spencer West uses personal data about individuals who are employed by us.

You should read this Privacy Notice, so that you know what personal data we collect about you, what we do with it and how you can exercise your rights in connection with it.

This Privacy Notice does not form part of any contract between us and you (including any contract of employment that may be offered or any other services contract).

1. **Controller**
2. **The data we collect about you**
3. **How we use your personal data and legal basis for doing so**
4. **Who we share your personal data with**
5. **International transfers**
6. **Data security**
7. **Retention of personal data**
8. **How to access your information and your other rights**
9. **Changes to this Privacy Notice**

1. Controller

A controller is the organisation that makes the decisions about what data is processed and is responsible for your personal data.

For the purposes of the activities set out in this Privacy Notice, the main controller will be the Spencer West law firm that employs you. If you are employed by Spencer West Global, Spencer West Global will be the main controller.

Please visit our website www.spencer-west.com for details of all the Spencer West law firms and their contact details.

We have a Global Data Protection Officer, Kristy Gouldsmith, whom you may contact by email at dpo@spencer-west.com or write to at:

Spencer West
Longbow House
20 Chiswell Street
London EC1Y 4TW

The law firms and their data are supported from an administrative perspective by Spencer West Global, a limited liability company registered in England and Wales. Spencer West Global is a joint controller of your data. This Privacy Notice is also provided to you on behalf of Spencer West Global.

2. The data we collect about you

When you are employed by us, we will collect and process a wide variety of your personal data. We start by collecting the personal data on your CV or application form and the information that we gathered from you during the recruitment process. This personal data forms the start of your HR file. We will collect additional information from third parties including former employers. Once you have been employed, we continue to process additional personal information in the course of job-related activities throughout the period of you working for us.

In order for you to be employed by us, we will collect your name, home address, gender, identification number, date of birth, employment start date and your signature. We will also need to see your passport as proof of your right to work.

In order to pay you, we will need your identification number and your bank account details. We may also receive court orders that require us to make deductions from your pay (eg. non-payment of tax or child maintenance.)

We will have information on your next of kin and emergency contact.

During your time with us, we will collect information about your health, such as when you are ill, have had an accident, require spectacles or have a medical or dentist appointment. We need to process this personal

data in order to fulfil our legal obligations to you as your employer, with your consent (eg. spectacles or a dentist appointment) or as a requirement of your employment contract.

If you become pregnant, we will process your health data in order to assure ourselves, and you, that the workplace is safe for you. You also have rights in the workplace when you are pregnant and we will process your health data and proof of your baby's birth in order to fulfil your rights for maternity leave.

If you wish to take paternity leave (if applicable, depending on jurisdiction), we will process your personal data (your name and your request) in order to fulfil your legal right to do so.

You may have the right to request flexible working (depending on jurisdiction) and we will process your personal data (your name and your request) during this process.

There may come a time that we will be required to process your personal data during a disciplinary or grievance process. This information will likely be your name and statements from other people about you. We will also hold performance information about you.

If you leave us, we will collect personal data from your resignation letter and your leaving date.

We provide pensions for our staff (depending on jurisdiction) and need to process your name, date of birth, identification number and your salary information in order to do this.

We will have data on your salary, annual leave, any benefits, and your job titles, work history, working hours, holidays, training records and professional memberships.

Your image in a photo or video is your personal data. We may wish to use your image on our website or other marketing information in order to promote the business but will always seek your consent for this. You do not have to agree that we can use your image – it is completely your choice.

We may have CCTV on site and if so will have footage containing your image.

We will have information about your use of our information and communications systems to ensure compliance with our IT policies and to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

For UK employees, we may conduct a Standard DBS check which will contain details of both spent and unspent convictions, cautions, reprimands and warnings that are held on the Police National Computer, which are not subject to filtering.

During the course of your employment, you will be required to put your name on or sign a wide variety of documents. Your name or signature is your personal data but the contents of the document, unless it is about you, is not your personal data.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

3. How we use your personal data and legal basis for doing so

Most of our processing is because we either have a legal obligation to process the data, or because we have a contract of employment with you. On occasion, we will seek your consent to process your personal data but you are free to refuse.

Legal basis	Action
<p><i>We will process this personal data because we have a legal obligation to do so.</i></p>	<p>your passport to ensure that you have the right to work</p> <p>your name, home address, gender, identification number, date of birth and signature are processed because we are required to do so by the tax authorities</p> <p>we may receive a court order that require us to make deductions from your pay (eg. non-payment of tax or child maintenance)</p> <p>we will process your health data if you are ill or have an accident because we have a legal obligation to do so</p> <p>if you become pregnant, we will process your health data because we have a legal obligation to fulfil your rights for maternity leave (if applicable)</p> <p>if you wish to take paternity leave (if applicable), we will process your personal data because we have a legal obligation to fulfil your rights for paternity leave</p> <p>if you wish to request flexible working (if applicable) we will process your personal data because we have a legal obligation to fulfil your right to request flexible working</p> <p>if you are involved in a disciplinary or grievance process, we will process your personal data because we have a legal obligation to provide a disciplinary or a grievance process</p> <p>we have a legal obligation to provide pensions for our staff (where applicable) and we need to process your name, date of birth, identification number and your salary information in order to do this.</p>
<p><i>We will process this personal data because we have a contract of employment with you.</i></p>	<p>your application form and the information that we gathered from your during the recruitment process</p> <p>we will need your identification number and your bank account details in order to pay you</p> <p>your qualifications</p>

<p><i>We will process this personal data because you have consented for us to do so.</i></p>	<p>we can only use your image in a photo or video for marketing purposes with your consent. You may withdraw your consent at any time but this will not affect our use of your image while we had your consent</p> <p>we process your health data with your consent if you would like to get VDU spectacles or have a medical or dentist appointment</p> <p>we will collect personal data from your resignation letter.</p> <p>Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know.</p>
<p><i>We will process this personal data because we have a legitimate interest in doing so.</i></p>	<p>During the course of your employment, you will be required to put your name on or sign a wide variety of documents. This use of your personal data is necessary for the running of our business.</p> <p>We will process your personal data during our appraisal process as we have a legitimate interest in appraising our staff and helping you to achieve your best.</p> <p>Sharing your personal data with our software and service providers, where necessary to do so.</p> <p>You have the right to object to our processing your data using legitimate interest. Please speak to us if you have any concerns.</p>

Special category data

The (UK) GDPR defines special category data as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);

- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Special category data needs more protection because it is sensitive than regular personal data, such as name and email.

In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment. On rare occasions, there may be other reasons for processing, such as it is in the public interest to do so. The situations in which we will process your particularly sensitive personal information are listed below. We have indicated the purpose or purposes for which we are processing or will process your more sensitive personal information.

- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including any of the following, to the extent that they are applicable in the relevant jurisdiction: statutory maternity pay, statutory sick pay, and pensions. We need to process this information to exercise rights and perform obligations in connection with your employment.
- If we reasonably believe that you or another person are at risk of harm and the processing is necessary to protect you or them from physical, mental or emotional harm or to protect physical, mental or emotional well-being.

Do we need your consent?

- We do not need your consent if we use special categories of your personal information in accordance with our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.
- We do not need your consent where the purpose of the processing is to protect you or another person from harm or to protect your well-being and if we reasonably believe that you need care and support, are at risk of harm and are unable to protect yourself.

4. Who we share your personal data with

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Entity	Legal basis
Our professional advisers such as lawyers and accountants.	Legitimate interest.
Government or regulatory authorities or law enforcement.	Legal obligation.
Professional indemnity or other relevant insurers.	Legitimate interest.
Third parties to whom we outsource certain services such as, without limitation, document processing and translation services, confidential waste disposal, IT systems or software providers, IT support service providers, document and information storage providers.	Legitimate interest.
Third parties engaged in the course of the services we provide to clients such as counsel, arbitrators, mediators, clerks, witnesses, cost draftsmen, court, opposing party and their lawyers, document review platforms and experts such as tax advisors or valuers.	Legitimate interest or a contractual requirement to provide our services.
Pension administrators.	Legal obligation.

Please note this list is non-exhaustive and there may be other examples where we need to share personal data with other parties in regard to your employment.

We conduct an appropriate level of due diligence and put in place contractual documentation in relation to any sub-contractor to ensure that they process personal data appropriately and according to our legal and regulatory obligations.

5. International transfers

Spencer West is a network of different law firms operating around the world. As such, we will sometimes need to transfer your personal data to recipients in jurisdictions other than your own eg. to our head office in the UK. Some of these jurisdictions may not provide the same level of protection to your personal data as provided in your jurisdiction. If we transfer your personal data outside the European Union or the United Kingdom, we will only make that transfer if:

- that country ensures an adequate level of protection for your personal data;

- we have put in place appropriate safeguards to protect your personal data, such as a contract with the person or entity receiving your personal data which incorporates specific provisions as directed by the European Commission and the UK government;
- the transfer is permitted by applicable laws; or
- you explicitly consent to the transfer.

If you would like to see a copy of any relevant safeguards used by us to protect the transfer of your personal data, please contact our Global Data Protection Officer at: dpo@spencer-west.com.

6. Data security

We are committed to keeping the personal data provided to us secure and we have implemented appropriate information security policies, rules and technical measures to protect the personal data that we have under our control from unauthorised access, improper use or disclosure, unauthorised modification and unlawful destruction or accidental loss.

All of our partners, employees, consultants, workers and data processors (i.e. those who process your personal data on our behalf, for the purposes listed above), who have access to, and are associated with the processing of personal data, are obliged to respect the confidentiality of such personal data.

7. Retention of personal data

We keep all HR data in accordance with our HR Retention Schedule.

8. How to access your information and your other rights

You have the following rights in relation to the personal data that we hold about you:

- **Your right of access:** if you ask us, we will confirm whether we are processing your personal data and, if necessary, provide you with a copy of that personal data (along with certain other details). If you require additional copies, we may need to charge a reasonable fee.
- **Your right to rectification:** if the personal data that we hold about you is inaccurate or incomplete, you are entitled to request to have it rectified. If you are entitled to rectification and if we have shared your personal data with others, we will let them know about the rectification where possible. If you ask us, where possible and lawful to do so, we will also tell you who we have shared your personal data with so that you can contact them directly.
- **Your right to erasure:** you can ask us to delete or remove your personal data in some circumstances, such as where we no longer need it or if you withdraw your consent (where applicable). If you are entitled to erasure and if we have shared your personal data with others, we will let them know about the erasure where possible. If you ask us, where it is possible and lawful for us to do so, we will also tell you who we have shared your personal data with so that you can contact them directly.

- **Your right to restrict processing:** you can ask us to 'block' or suppress the processing of your personal data in certain circumstances, such as where you contest the accuracy of that personal data or you raise an objection with us. If you are entitled to restriction and if we have shared your personal data with others, we will let them know about the restriction where it is possible for us to do so. If you ask us, where it is possible and lawful for us to do so, we will also inform you who we have shared your personal data with so that you can contact them directly.
- **Your right to data portability:** you have the right, in certain circumstances, to obtain personal data that you have provided us with (in a structured, commonly used and machine readable format) and to reuse it elsewhere or to ask us to transfer this to a third party of your choice.
- **Your right to object:** you can ask us to stop processing your personal data, and we will do so, if we are:
 - relying on our own or someone else's legitimate interests to process your personal data, except if we can demonstrate compelling legal grounds for the processing; or
 - processing your personal data for direct marketing purposes.
- **Your right to withdraw consent:** if we rely on your consent (or explicit consent) as our legal basis for processing your personal data, you have the right to withdraw that consent at any time.
- **Your right to lodge a complaint with the Supervisory Authority:** if you have a concern about any aspect of our privacy practices, including the way we have handled your personal data, you can report it to the Supervisory Authority in your country. We would, however, appreciate the chance to deal with your concerns before you approach the Supervisory Authority, so please contact us in the first instance.

Please note that some of these rights may be limited where we have an overriding interest or legal obligation to continue to process the data, or where data may be exempt from disclosure due to reasons of legal professional privilege or professional secrecy obligations.

9. Changes to this Privacy Notice

To ensure that you are always aware of how we use your personal data, we will update this Privacy Notice from time to time to reflect any changes to our use of your personal data. We may also make changes as required to comply with changes in applicable law or regulatory requirements. Where it is practicable, we will notify you by email of any significant changes. However, we encourage you to review this Privacy Notice periodically to be informed of how we use your personal data.

Partners, consultants, contractors, temporary or agency workers at Spencer West

This Privacy Notice explains how and why Spencer West uses personal data about individuals and companies that consult or contract with us.

You should read this Privacy Notice, so that you know what personal data we collect about you, what we do with it and how you can exercise your rights in connection with it.

This Privacy Notice does not form part of any contract between us and you.

1. **Controller**
2. **The data we collect about you**
3. **How we use your personal data and legal basis for doing so**
4. **Who we share your personal data with**
5. **International transfers**
6. **Data security**
7. **Retention of personal data**
8. **How to access your information and your other rights**
9. **Changes to this Privacy Notice**

1. Controller

A controller is the organisation that makes the decisions about what data is processed and is responsible for your personal data.

For the purposes of the activities set out in this Privacy Notice, the main controller will be the Spencer West firm that has engaged your services.

Please visit our website www.spencer-west.com for details of all the Spencer West law firms and their contact details.

We have a Global Data Protection Officer, Kristy Gouldsmith, whom you may contact by email at dpo@spencer-west.com or write to at:

Spencer West
Longbow House
20 Chiswell Street
London EC1Y 4TW

The law firms and their data are supported from an administrative perspective by Spencer West Global, a limited liability company registered in England and Wales. Spencer West Global is a joint controller of your data. This Privacy Notice is also provided to you on behalf of Spencer West Global.

2. The data we collect about you

When you are a consultant engaged by us, we will collect and process a wide variety of your personal data. We start by collecting the personal data on your CV or application form and the information that we gathered from you during the recruitment process. This personal data forms the start of your consultant file. We will collect additional information from third parties including former employers or contracting parties or other background check agencies. Once you have been retained, we continue to process additional personal information in the course of consultant-related activities throughout the period of you consulting for us.

Our primary goal in collecting personal data from you is to help us:

- retain your services
- verify your identity
- comply with the requirements of the regulator and anti-money laundering (AML) legislation
- investigate or settle enquiries or disputes
- enforce our agreement with you; and
- protect the rights, property or safety of us or third parties, including our clients.

We use different methods to collect data from and about you including through:

Information	Legal basis
<p><i>Direct interactions</i></p>	<p>In order for you to be retained by us as a consultant, we collect process and store:</p> <p>Your full name</p> <p>Address, email, and phone number</p> <p>Gender and date of birth</p> <p>Contract start date and end date</p> <p>Information on any compliments, complaints or issues arising during your time with us</p> <p>Contact information including the company you work for and email address, where provided (if not a sole trader)</p> <p>Relevant information, such as proof of address or identity, as required by anti-money laundering regulations and criminal record checks, and as part of our contractor onboarding procedure. The sources for such verification may comprise documentation which we request from you or through the use of online sources or both</p> <p>Your Practising Certificate (or equivalent in relevant jurisdiction) and your record of continuing competence</p> <p>Information you provide to us for the purposes of attending meetings and events, including dietary</p>

	requirements which may reveal information about your health or religious beliefs
<i>Anti-money laundering checks</i>	<p>We are required to perform AML checks on all consultants. To do this, we have various providers that perform AML and fraud checks. The following searches are made:</p> <ul style="list-style-type: none"> Electoral roll Postcode address files Consent databases Telephone directory Mortality registers PEP intelligence database Multiple sanction databases Birth Index Register Age range Bank account validation and verification
<i>Criminal record checks</i>	<p>As required by our regulator, we will process your personal data for the purposes of a criminal records check. We do not take your documents directly but use a third party service provider for our checks. The service provider will require either your passport or driving licence and proof of address, such as a utility bill. Once the check is complete, we will be notified of the existence of any unspent criminal convictions.</p>
<i>Third parties or publicly available sources</i>	<p>We may receive personal data about you from various third parties and public sources including those set out below:</p> <ul style="list-style-type: none"> Companies House or equivalent; the legal regulator; Insolvency services; LinkedIn; Other professionals, including solicitors or barristers; and Client or colleague feedback.

If you fail to provide personal information

Where we need to collect personal data by law, or under the terms of a contract that we have with you, and you fail to provide that data when requested, we may not be able to enter into a contract with you. In this

case, we may have to cancel the contract that we have with you but we will notify you if this is the case at the time.

3. How we use your personal data and legal basis for doing so

We may use your information for the following purposes:

Action	Reason	Legal Basis
Fulfilment of a contract	We collect and maintain personal data that you voluntarily submit to us to enable us to have a contract with you.	It is necessary for us to process your information to perform our obligations in accordance with any contract that we may have with you. It is in our legitimate interest or a third party's legitimate interest to use your personal data in such a way to ensure that we provide the very best client service we can to you or others (eg. client feedback).
Legal compliance	We use your personal data to comply with our legal obligations (regulatory and anti-money laundering legislation, conflicts or similar obligations).	It is our legal obligation to use your personal data to comply with any legal obligations imposed upon us.

4. Who we share your personal data with

We may share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Entity	Legal basis
Our professional advisers such as lawyers and accountants.	Legitimate interest.
Government or regulatory authorities or law enforcement.	Legal obligation.
Professional indemnity or other relevant insurers.	Legitimate interest.
Regulators/tax authorities/corporate registries.	Legal obligation.
Third parties to whom we outsource certain services such as, without limitation, document processing and translation services, confidential waste disposal, IT systems or software providers, IT support service providers, document and information storage providers.	Legitimate interest.
Third parties engaged in the course of the services we provide to clients such as counsel, arbitrators, mediators, clerks, witnesses, cost draftsmen, court, opposing party and their lawyers, document review platforms and experts such as tax advisors or valuers.	Legitimate interest or a contractual requirement to provide our services.
Third party service providers to assist us with client insight analytics, such as Google Analytics	Consent.

Please note this list is non-exhaustive and there may be other examples where we need to share personal data with other parties.

We conduct an appropriate level of due diligence and put in place contractual documentation in relation to any sub-contractor to ensure that they process personal data appropriately and according to our legal and regulatory obligations.

Further, we may appoint external data controllers where necessary to deliver the services (for example, accountants, barristers or other third party experts). When doing so we will comply with our legal and regulatory obligations in relation to the personal data and put appropriate safeguards in place.

5. International transfers

Spencer West is a network of different law firms operating around the world. As such, we will sometimes need to transfer your personal data to recipients in jurisdictions other than your own eg. to our head office

in the UK. Some of these jurisdictions may not provide the same level of protection to your personal data as provided in your jurisdiction. If we transfer your personal data outside the European Union or the United Kingdom, we will only make that transfer if:

- that country ensures an adequate level of protection for your personal data;
- we have put in place appropriate safeguards to protect your personal data, such as a contract with the person or entity receiving your personal data which incorporates specific provisions as directed by the European Commission and the UK government;
- the transfer is permitted by applicable laws; or
- you explicitly consent to the transfer.

If you would like to see a copy of any relevant safeguards used by us to protect the transfer of your personal data, please contact our Global Data Protection Officer at: dpo@spencer-west.com.

6. Data security

We are committed to keeping the personal data provided to us secure and we have implemented appropriate information security policies, rules and technical measures to protect the personal data that we have under our control from unauthorised access, improper use or disclosure, unauthorised modification and unlawful destruction or accidental loss.

All of our partners, employees, consultants, workers and data processors (i.e. those who process your personal data on our behalf, for the purposes listed above), who have access to, and are associated with the processing of personal data, are obliged to respect the confidentiality of such personal data.

7. Retention of personal data

By law, we may have to keep information about our consultants (including contact, identity, financial and file information) for a minimum of six years, and in some cases up to twelve years, after they cease being consultants. The length of period will vary according to jurisdiction.

8. How to access your information and your other rights

You have the following rights in relation to the personal data that we hold about you:

- **Your right of access:** if you ask us, we will confirm whether we are processing your personal data and, if necessary, provide you with a copy of that personal data (along with certain other details). If you require additional copies, we may need to charge a reasonable fee.
- **Your right to rectification:** if the personal data that we hold about you is inaccurate or incomplete, you are entitled to request to have it rectified. If you are entitled to rectification and if we have shared your personal data with others, we will let them know about the rectification where possible. If you ask us,

where possible and lawful to do so, we will also tell you who we have shared your personal data with so that you can contact them directly.

- **Your right to erasure:** you can ask us to delete or remove your personal data in some circumstances, such as where we no longer need it or if you withdraw your consent (where applicable). If you are entitled to erasure and if we have shared your personal data with others, we will let them know about the erasure where possible. If you ask us, where it is possible and lawful for us to do so, we will also tell you who we have shared your personal data with so that you can contact them directly.
- **Your right to restrict processing:** you can ask us to 'block' or suppress the processing of your personal data in certain circumstances, such as where you contest the accuracy of that personal data or you raise an objection with us. If you are entitled to restriction and if we have shared your personal data with others, we will let them know about the restriction where it is possible for us to do so. If you ask us, where it is possible and lawful for us to do so, we will also inform you who we have shared your personal data with so that you can contact them directly.
- **Your right to data portability:** you have the right, in certain circumstances, to obtain personal data that you have provided us with (in a structured, commonly used and machine readable format) and to reuse it elsewhere or to ask us to transfer this to a third party of your choice.
- **Your right to object:** you can ask us to stop processing your personal data, and we will do so, if we are:
 - relying on our own or someone else's legitimate interests to process your personal data, except if we can demonstrate compelling legal grounds for the processing; or
 - processing your personal data for direct marketing purposes.
- **Your right to withdraw consent:** if we rely on your consent (or explicit consent) as our legal basis for processing your personal data, you have the right to withdraw that consent at any time.
- **Your right to lodge a complaint with the Supervisory Authority:** if you have a concern about any aspect of our privacy practices, including the way we have handled your personal data, you can report it to the Supervisory Authority in your country. We would, however, appreciate the chance to deal with your concerns before you approach the Supervisory Authority, so please contact us in the first instance.

Please note that some of these rights may be limited where we have an overriding interest or legal obligation to continue to process the data, or where data may be exempt from disclosure due to reasons of legal professional privilege or professional secrecy obligations.

9. Changes to this Privacy Notice

To ensure that you are always aware of how we use your personal data, we will update this Privacy Notice from time to time to reflect any changes to our use of your personal data. We may also make changes as required to comply with changes in applicable law or regulatory requirements. Where it is practicable, we will notify you by email of any significant changes. However, we encourage you to review this Privacy Notice periodically to be informed of how we use your personal data.