

Whiting & Mason Solicitors

Privacy Policy

1. General

- 1.1. We are committed to protecting the privacy and security of personal information we obtain. Whether you are a client, prospective client, contact, supplier, prospective supplier, employee, consultant or anyone similar, we treat all your personal data in the same manner. Whiting & Mason Solicitors are a “data controller”. We are responsible for deciding how we hold and use the personal data we hold.
- 1.2. Whiting & Mason Solicitors is a partnership that currently operates from the following offices:
 - 1.2.1. Marple Office
17-19 Stockport Road, Marple, Stockport, SK6 6BD
Telephone: 0161 4271040 Fax: 0161 4260923
 - 1.2.2. New Mills Office
24 Union Road, New Mills, High Peak, SK22 3ES
Telephone: 01663 742432 Fax: 01663 741206
- 1.3. Website: whitingmason.co.uk
- 1.4. Email: info@whitingmason.co.uk
- 1.5. We are authorised and regulated by the Solicitors Regulation Authority (the SRA). SRA No. 61848. The SRA is the independent regulatory arm of the Law Society of England and Wales who our professional body.
- 1.6. We are registered for VAT purposes. VAT Registration No. 157839030.
- 1.7. A list of Partners can be inspected at any of our offices or can be provided on request.
- 1.8. Clients of this firm should read this policy alongside our Terms of Business, which provide further information on confidentiality. In most types of matters our Terms of Business will have been provided to you at the start of the matter. They are however also available on our website at whitingmason.co.uk/terms-of-business or can also be provided on request.
- 1.9. We collect, use and are responsible for certain personal data about you. When we do so we must comply with the UK General Data Protection Regulation (UK GDPR). The personal data we may have requested from you is collected and processed on a legitimate interest basis to fulfil the purpose we collected it for including satisfying legal, accounting or reporting purposes.

2. Types of Data

- 2.1. We may collect or use the following types of data:
 - 2.1.1. Names and contact details
 - 2.1.2. Addresses

- 2.1.3. Gender
- 2.1.4. Pronoun preferences
- 2.1.5. Occupation
- 2.1.6. Date of birth
- 2.1.7. Place of birth
- 2.1.8. National Insurance number
- 2.1.9. Marital status
- 2.1.10. Third party information (such as family members or other relevant parties)
- 2.1.11. Payment details
- 2.1.12. Financial data
- 2.1.13. Transaction data
- 2.1.14. Usage data
- 2.1.15. Employment details
- 2.1.16. Credit history and credit reference information
- 2.1.17. Criminal records data
- 2.1.18. Information relating to compliments or complaints
- 2.1.19. Records of meetings and decisions

2.2. We may also collect or use the following special category information. This information is subject to additional protection due to its sensitive nature:

- 2.2.1. Racial or ethnic origin
- 2.2.2. Political opinions
- 2.2.3. Religious or philosophical beliefs
- 2.2.4. Trade union membership
- 2.2.5. Genetic information
- 2.2.6. Health information
- 2.2.7. Sex life information
- 2.2.8. Sexual orientation information

3. Data Collection

3.1. We collect most information directly from you. However, we may also obtain this from other sources such as:

- 3.1.1. Regulatory authorities
- 3.1.2. Legal bodies or professionals
- 3.1.3. Publicly available sources
- 3.1.4. Previous employment
- 3.1.5. Credit reference agencies
- 3.1.6. Suppliers and service providers
- 3.1.7. Sanctions screening providers
- 3.1.8. Due diligence providers
- 3.1.9. Bank, building society, financial institution or advisor
- 3.1.10. Employer
- 3.1.11. Trade union
- 3.1.12. Professional body
- 3.1.13. Pension administrators
- 3.1.14. Doctors, medical or occupational health professionals

4. Why We Use Personal Data

4.1. The table below explains some examples of what we may use your personal data for and why:

What we may use your personal data for	Our reasons
Providing services to our clients	To fulfil our contract with clients or to take steps at their request before entering into a contract
Preventing and detecting fraud against you or us	For our and/or your legitimate interests, i.e. to minimise fraud that could be damaging for you and/or us
Conducting checks to identify our clients and verify their identity Screening for financial and other sanctions or embargoes Other activities necessary to comply with professional, legal and regulatory obligations that apply to our firm, e.g. under health and safety law or rules issued by our professional regulator	Depending on the circumstances: -to comply with our legal and regulatory obligations -for our legitimate interests
To check whether there is any conflict of interest between us and you and/or between you and another client	To comply with our legal and regulatory obligations
To enforce legal rights or defend or take legal proceedings	Depending on the circumstances: -to comply with our legal and regulatory obligations -for our legitimate interests or those of a third party
Gathering and providing information required by or relating to audits, enquiries or investigations by regulatory bodies	Depending on the circumstances: -to comply with our legal and regulatory obligations -for our legitimate interests
Ensuring internal business policies are complied with, e.g. policies covering security and internet use	For our legitimate interests, i.e. to make sure we are following our own internal procedures so we can deliver the best service to our clients
Operational reasons, such as improving efficiency, training and quality control	For our legitimate interests, i.e. to be as efficient as we can so we can deliver the best service to our clients at the best price
Ensuring the confidentiality of commercially sensitive information	Depending on the circumstances: -for our legitimate interests, i.e. to protect trade secrets and other commercially valuable information -to comply with our legal and regulatory obligations
Statistical analysis to help us manage our business, e.g. in relation to our financial performance, client base, services range or other efficiency measures	For our legitimate interests, i.e. to be as efficient as we can so we can deliver the best service to our clients at the best price
Protecting the security of systems and data used to provide services, preventing	Depending on the circumstances:

unauthorised access and changes to our systems	-for our legitimate interests, i.e. to prevent and detect criminal activity that could be damaging for you and/or us -to comply with our legal and regulatory obligations
Updating and enhancing client records	Depending on the circumstances: -to fulfil our contract with you or to take steps at your request before entering into a contract -to comply with our legal and regulatory obligations -for our legitimate interests, e.g. making sure we can keep in touch with our clients about existing and new services
Statutory returns	To comply with our legal and regulatory obligations
Ensuring safe working practices, staff administration and assessments	Depending on the circumstances: -to comply with our legal and regulatory obligations -for our legitimate interests, e.g. to make sure we are following our own internal procedures and working efficiently so we can deliver the best service to you
Credit reference checks via external credit reference agencies	For our legitimate interests, i.e. to ensure our clients are likely to be able to pay for our services
To deal with complaints or claims	Depending on the circumstances: -to comply with our legal and regulatory obligations -for our or your legitimate interests, e.g. to make sure any potential claim is reported to our insurer
External audits and quality checks, e.g. for Lexcel or similar accreditations and the audit of our accounts	Depending on the circumstances: -for our legitimate interests, i.e. to achieve and maintain relevant accreditations so we can demonstrate we operate at the highest standards -to comply with our legal and regulatory obligations
To share your personal data with third parties that will or may take control or ownership of some or all of our firm (and professional advisors acting on our or their behalf) in connection with a significant corporate transaction or restructuring, including a merger, acquisition, asset sale or in the event of our insolvency In such cases information will be anonymised where possible and only shared where necessary	Depending on the circumstances: -to comply with our legal and regulatory obligations -in other cases, for our legitimate interests, i.e. to protect, realise or grow the value in our business and assets

5. Sharing of Personal Data

5.1. In some circumstances we may need to share personal data with others such as:

- 5.1.1. Third parties we use to help deliver our services, e.g. providers of software we use, IT service providers including cloud services and financial institutions in connection with payments
- 5.1.2. Third party external advisors or experts
- 5.1.3. Companies providing services for money laundering checks and other crime prevention purposes
- 5.1.4. Credit reference agencies
- 5.1.5. Debt collection agencies
- 5.1.6. Fraud investigation authorities
- 5.1.7. Insurance companies, brokers or other intermediaries
- 5.1.8. Professional or legal advisors
- 5.1.9. Emergency services
- 5.1.10. Insolvency practitioners
- 5.1.11. Regulatory authorities
- 5.1.12. External auditors
- 5.1.13. Organisations we're legally obliged to share personal information with
- 5.1.14. Professional consultants
- 5.1.15. Sanctions screening providers
- 5.1.16. Due diligence providers
- 5.1.17. Bank, building society, financial institution or advisor

5.2. We only allow share personal data to those if we are satisfied they take appropriate measures to protect your personal data. We ensure all outsourcing providers operate under service agreements that are consistent with our legal and professional obligations.

5.3. Personal data will not be sold or rented to third parties and we will not share the information with third parties for marketing purposes.

6. Retention

- 6.1. Personal data will be stored for as long as is necessary to enable your instructions to be carried out, to allow for the ongoing administration of your instruction, and to comply with our legal and regulatory obligations.
- 6.2. We will not keep your personal data for longer than we need it for the purpose for which it was collected or as required by law.
- 6.3. As a general rule, we will keep your personal data for at least six years from the conclusion of your matter, in case you, or we, need to bring or defend any complaints or claims. However, different retention periods apply for different types of personal data and for different services. If you have any specific queries, please do not hesitate to contact us and we will be pleased to discuss these with you.

7. Access to Personal Data

7.1. You have the right of access to your personal information. If you wish to receive a copy of the personal information we hold on you, you may make a data subject access request. If your

personal information is inaccurate or incomplete, you can request that it is corrected. You can ask for your information to be deleted or removed if there is not a compelling reason for us to continue to have it.

8. Keeping Personal Data Secure

- 8.1. We have implemented appropriate technical and organisational measures to keep your personal data confidential and secure from unauthorised access, use and disclosure. We limit access to your personal data to those who have a genuine business need to access it. Those processing your personal data will do so only in an authorised manner and are subject to a duty of confidentiality.
- 8.2. We require our business partners, suppliers and other third parties to implement appropriate security measures to protect personal data from unauthorised access, use and disclosure.
- 8.3. We have procedures to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are required to do so.

9. Information Specifically for Employees, Consultants, Job Applicants and Similar

- 9.1. In addition to the general information outlined in this policy, we also need to collect and process personal data relating to our employees, consultants, job applicants and similar personnel for employment and HR purposes.
- 9.2. There may be additional types of personal data we may need to collect in this regard, such as:
 - 9.2.1. Salary and benefits information
 - 9.2.2. Employment history and qualifications
 - 9.2.3. Right to work documentation
 - 9.2.4. Performance and disciplinary records
 - 9.2.5. Absence and sickness records
 - 9.2.6. Health and medical information
 - 9.2.7. Emergency contact details
 - 9.2.8. Pension and insurance information
 - 9.2.9. Equality and diversity data
 - 9.2.10. IT usage and access logs
- 9.3. We may need to share employee data with:
 - 9.3.1. HMRC and other government bodies
 - 9.3.2. Pension providers and payroll processors
 - 9.3.3. Occupational health professionals
 - 9.3.4. Legal advisors and insurers
 - 9.3.5. Regulatory authorities
 - 9.3.6. IT service providers
- 9.4. Employee records are retained for a minimum of six years after employment ends; however, they may be retained for a longer period for legal or regulatory reasons at our discretion.

10. Complaints

- 10.1. Please contact us if you have any queries or concerns about our use of personal data. We hope we will be able to resolve any issues you may have. You may however also have the right to lodge a complaint with the Information Commissioner's Office (the UK data protection regulator also known as the ICO).
- 10.2. The ICO's contact details are as follows: Website: www.ico.org.uk/make-a-complaint, Telephone: 03031231113, Address: Wycliffe House, Water Lane, Wilmslow, SK9 5AF.
- 10.3. We are registered with the ICO. ICO Reference No. Z7723437.

11. Updating of Privacy Policy

- 11.1. We review this policy from time to time and may amend it. The most up to date version will be available on our website at whitingmason.co.uk/privacy-policy or can also be provided on request.

12. Monitoring & Review

- 12.1. The firm's General Data Protection Regulation Manager (GDPR Manager), Joanne C Potts, is responsible for this policy.
- 12.2. The GDPR Manager will monitor compliance with this policy and will review this policy regularly and at least annually.

13. Queries

- 13.1. If you have any queries in relation to this policy, then please do not hesitate to contact us as we shall be happy to discuss them with you.