

AB Corporate LLP – Data Protection Policy

1. Introduction

1.1 We take your privacy very seriously. Please read this privacy policy carefully as it contains important information on who we are and how and why we collect, store, use and share your personal data. It also explains your rights in relation to your personal data and how to contact us or supervisory authorities in the event you have a complaint.

1.2 When we use your personal data we are regulated under the EU General Data Protection Regulation (**GDPR**) which applies across the European Union (including in the United Kingdom) and we are responsible as ‘controller’ of that personal data for the purposes of the GDPR. Our use of your personal data is subject to your instructions, the GDPR, other relevant UK and EU legislation and our professional duty of confidentiality.

2. Key terms

2.1 It would be helpful to start by explaining some key terms used in this policy:

- (a) **We, us, our:** AB Corporate LLP (registered number OC359052) of 3 Hardman Street (West Entrance) Spinningfields Manchester M3 3HF.
- (b) **Personal data:** Any information relating to an identified or identifiable individual
- (c) **Special category personal data:** Personal data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership

3. Personal data we collect about you

3.1 We set out below the personal data we will or may collect in the course of providing legal services. This may include special category personal data.

3.2 Personal data **we will** collect:

- (a) Your name, address and telephone number
- (b) Information to enable us to check and verify your identity, eg your date of birth or passport details
- (c) Electronic contact details, eg your email address and mobile phone number
- (d) Information relating to the matter in which you are seeking our advice or representation
- (e) Your financial details so far as relevant to your instructions, eg the source of your funds if you are instructing on a purchase transaction

3.3 Personal data **we may** collect depending on why you have instructed us:

- (a) Your National Insurance and tax details
- (b) Your bank and/or building society details
- (c) Details of your professional online presence, eg LinkedIn profile
- (d) Details of your spouse/partner and dependants or other family members, eg if you instruct us on a family matter or a will
- (e) Your employment status and details including salary and benefits, eg if you instruct us on matter related to your employment or in which your employment status or income is relevant.
- (f) Details of your pension arrangements, eg if you instruct us on a pension matter or in relation to financial arrangements following breakdown of a relationship
- (g) Your employment records including, where relevant, records relating to sickness and attendance, performance, disciplinary, conduct and grievances, eg if you instruct us on matter related to your employment or in which your employment records are relevant.

- (h) Your racial or ethnic origin, gender and sexual orientation, religious or similar beliefs, eg if you instruct us on discrimination claim.
 - (i) Personal identifying information, such as your eye colour or your parents' names, eg if you instruct us to incorporate a company for you.
- 3.4 This personal data is required to enable us to provide legal services. If you do not provide personal data we ask for, it may delay or prevent us from providing those services.
- 3.5 For information on why we use this personal data, see below: '**How and why we use personal data**' and '**How and why we use special category personal data**'.

4. How your personal data is collected

- 4.1 We collect most of this information from you. However, we may also collect information:
- (a) from publicly accessible sources, eg Companies House or HM Land Registry;
 - (b) directly from a third party, eg:
 - (i) sanctions screening providers;
 - (ii) credit reference agencies;
 - (iii) client due diligence providers;
 - (c) from a third party with your consent, eg:
 - (i) your bank or building society, another financial institution or advisor;
 - (ii) consultants and other professionals we may engage in relation to your matter;
 - (iii) your employer and/or trade union, professional body or pension administrators;
 - (iv) your doctors, medical and occupational health professionals;
 - (d) via any website of ours — we use cookies on our website
 - (e) via our information technology (IT) systems, eg case management, document management and time recording systems.

5. How and why we use personal data

- 5.1 Under data protection law, we can only use personal data if we have a proper reason for doing so, eg:
- (a) to comply with our legal and regulatory obligations;
 - (b) for the performance of our contract with you or to take steps at your request before entering into a contract;
 - (c) for our legitimate interests or those of a third party; or
 - (d) where you have given consent.
- 5.2 A legitimate interest is when we have a business or commercial reason to use personal data, so long as this is not overridden by your own rights and interests.
- 5.3 The tables appended to this policy explain how we use personal data and our reasons for doing so.

6. How and why we use special category personal data

- 6.1 Under data protection law, we can only use special category personal data where:
- (a) we have a proper reason for doing so (see above: **How and why we use personal data**), and

- (b) one of the 'grounds' for using special category personal data applies.
- 6.2 There are ten potential grounds for using special category personal data under data protection law. Generally, where we use special category personal data, we will do so on the ground that this is necessary for establishing, exercising or defending legal claims. This includes using special category personal data, where necessary, for:
 - (a) actual or prospective court proceedings;
 - (b) obtaining legal advice; or
 - (c) establishing, exercising or defending legal rights in any other way.
- 6.3 Where this does not apply, we will seek explicit consent to process special category personal data.

7. Promotional communications

- 7.1 We may use your personal data to send you updates (by email, text message, telephone or post) about legal developments that might be of interest to you and/or information about our services, including exclusive offers, promotions or new services or products.
- 7.2 We have a legitimate interest in processing your personal data for promotional purposes (see above '**How and why we use your personal data**'). This means we do not usually need your consent to send you promotional communications. However, where consent is needed, we will ask for this consent separately and clearly.
- 7.3 We will always treat your personal data with the utmost respect and never sell or share it with other organisations for marketing purposes. We may use third party providers for the purposes of email marketing, but only where your personal data is kept safe and confidential.
- 7.4 You have the right to opt out of receiving promotional communications at any time by:
 - (a) contacting us; or
 - (b) using any 'unsubscribe' link in emails or 'STOP' number in texts.
- 7.5 We may ask you to confirm or update your marketing preferences if you instruct us to provide further services in the future, or if there are changes in the law, regulation, or the structure of our business.

8. Who we share your personal data with

- 8.1 We routinely share personal data with:
 - (a) professional advisers who we instruct on your behalf or refer you to, eg barristers, medical professionals, accountants, tax advisors or other experts;
 - (b) other third parties where necessary to carry out your instructions, eg your funders or HM Land Registry in the case of a property transaction or Companies House;
 - (c) our insurers and brokers;
 - (d) external auditors and the audit of our accounts;
 - (e) our bank;
 - (f) external service suppliers, representatives and agents that we use to make our business more efficient, eg typing services, marketing agencies, document collation or analysis suppliers.
- 8.2 We only allow our service providers to handle your personal data if we are satisfied they take appropriate measures to protect your personal data. Where appropriate we also impose contractual obligations on service providers to ensure they can only use your personal data to provide services to us and to you.
- 8.3 We may disclose and exchange information with law enforcement agencies and regulatory bodies to comply with our legal and regulatory obligations.

8.4 We may also need to share some personal data with other parties, such as potential buyers of some or all of our business or during a re-structuring. Usually, information will be anonymised but this may not always be possible. The recipient of the information will be bound by confidentiality obligations.

9. Where your personal data is held

9.1 Information may be held at our offices and those of our third party agencies, service providers, representatives and agents as described above (see **'Who we share your personal data with'**).

9.2 Some of these third parties may be based outside the European Economic Area. For more information, including on how we safeguard your personal data when this occurs, see below: **'Transferring your personal data out of the UK and EEA'**.

10. How long your personal data will be kept

10.1 We will keep your personal data after we have finished advising or acting for you. We will do so for one of these reasons:

- (a) to respond to any questions, complaints or claims made by you or on your behalf;
- (b) to show that we treated you fairly;
- (c) to keep records required by law.

10.2 We will not retain your data for longer than necessary.

11. Transferring your personal data out of the UK and EEA

11.1 To deliver services to you, it is sometimes necessary for us to share your personal data outside the UK or European Economic Area (**EEA**), eg:

- (a) with your and our service providers located outside the UK/EEA;
- (b) if you are based outside the UK/EEA;
- (c) where there is an international dimension to the matter in which we are advising you.

11.2 These transfers are subject to special rules under European and UK data protection law.

11.3 Where these non-UK/EEA countries do not have the same data protection laws as the United Kingdom and EEA we will, however, ensure the transfer complies with data protection law and all personal data will be secure.

12. Your rights

12.1 You have the following rights, which you can exercise free of charge:

- (a) **Access:** The right to be provided with a copy of your personal data.
- (b) **Rectification:** The right to require us to correct any mistakes in your personal data.
- (c) **To be forgotten:** The right to require us to delete your personal data—in certain situations
- (d) **Restriction of processing:** The right to require us to restrict processing of your personal data—in certain circumstances, eg if you contest the accuracy of the data
- (e) **Data portability:** The right to receive the personal data you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party—in certain situations
- (f) **To object:** The right to object:
 - (i) at any time to your personal data being processed for direct marketing (including profiling);
 - (ii) in certain other situations to our continued processing of your personal

- (g) Not to be subject to automated individual decision making data, eg processing carried out for the purpose of our legitimate interests: The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you.
- 12.2 For further information on each of those rights, including the circumstances in which they apply, please contact us or see the [Guidance from the UK Information Commissioner's Office \(ICO\) on individuals' rights under the General Data Protection Regulation](#).
- 12.3 If you would like to exercise any of those rights, please:
- (a) email, call or write to us — see below: **How to contact us**; and
 - (b) let us have enough information to identify you;
 - (c) let us have proof of your identity and address (a copy of your driving licence or passport and a recent utility or credit card bill); and
 - (d) let us know what right you want to exercise and the information to which your request relates.

13. Keeping your personal data secure

- 13.1 We have appropriate security measures to prevent personal data from being accidentally lost, or used or accessed unlawfully. We limit access to your personal data to those who have a genuine business need to access it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.
- 13.2 We also have procedures in place 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 legally required to do so.

14. How to complain

- 14.1 We hope that we can resolve any query or concern you may raise about our use of your information.
- 14.2 The [General Data Protection Regulation](#) also gives you right to lodge a complaint with a supervisory authority, in particular in the European Union (or European Economic Area) state where you work, normally live or where any alleged infringement of data protection laws occurred. The supervisory authority in the UK is the Information Commissioner who may be contacted at <https://ico.org.uk/concerns> or telephone: 0303 123 1113.

15. Changes to this privacy policy

- 15.1 This privacy policy was published on 19 August 2020.
- 15.2 We may change this privacy policy from time to time.

16. How to contact us

- 16.1 Please contact us by post, email or telephone if you have any questions about this privacy policy or the information we hold about you.
- 16.2 Our contact details are shown below:

Peter Bibby: peter.bibby@abcorporatelaw.co.uk

0844 824 8744

3 Hardman Street (West Entrance) Spinningfields Manchester M3 3HF

Appendix A – How data is processed

How data is processed	Potential lawful ground and Article of GDPR
<p>Conducting checks to identify clients and verify their identities. Screening for financial and other sanctions or embargoes.</p> <p>Other processing necessary to comply with professional, legal and regulatory obligations that apply to our business, eg under health and safety regulations or rules issued by our professional regulator</p>	<p>Art 6(1)(c)—compliance with a legal obligation, but only to the extent that this is ‘necessary’ for compliance with a legal obligation</p> <p>Otherwise, consider Art 6(1)(f)—legitimate interests</p>
<p>Gathering information as part of investigations by regulatory bodies</p>	<p>Art 6(1)(c)—but only to the extent that this is ‘necessary’ for compliance with a legal obligation</p> <p>Otherwise, consider Art 6(1)(f)—legitimate interests</p>
<p>Ensuring business policies are adhered to, eg policies covering security and internet use</p>	<p>Art 6(1)(f)—legitimate interests</p>
<p>Operational reasons, such as improving efficiency, training and quality control</p>	<p>Art 6(1)(f)—legitimate interests</p>
<p>Ensuring the confidentiality of commercially sensitive information</p>	<p>Art 6(1)(f)—legitimate interests</p>
<p>Statistical analysis to help manage your practice</p>	<p>Art 6(1)(f)—legitimate interests</p> <p>Beware that the term ‘statistical analysis’ is extremely vague and likely to fall foul of transparency requirements in Art 13 or 14 the GDPR—try to be more specific in your privacy policy</p>
<p>Preventing unauthorised access and modifications to systems</p>	<p>Art 6(1)(c)—compliance with a legal obligation, but only to the extent that this is ‘necessary’ for compliance with a legal obligation</p> <p>Art 6(1)(f)—legitimate interests</p>
<p>Updating and enhancing client records</p>	<p>Depending on your activity, a range of lawful grounds could apply:</p> <ul style="list-style-type: none"> —Art 6(1)(c)—compliance with a legal obligation, ie the obligation in the Art 5(1)(d) of GDPR itself to ensure the accuracy of personal data —Art 6(1)(b)—to the extent that the processing is necessary for the performance of your contract with the client/customer —Art 6(1)(f)—legitimate interests in relation to enhancing client records, but beware that the term ‘enhancing client records’ is extremely vague and likely to fall foul of transparency requirements in Art 13 or 14 the GDPR—try to be more specific in your privacy policy
<p>Statutory returns</p>	<p>Art 6(1)(c)—compliance with a legal obligation</p>

Appendix A – How data is processed

How data is processed	Potential lawful ground and Article of GDPR
Staff administration and assessments, monitoring staff conduct, disciplinary matters	<p>Depending on your activity, a range of lawful grounds could apply:</p> <ul style="list-style-type: none"> —Art 6(1)(c)—compliance with a legal obligation, to the extent that your purposing activity is necessary to comply with a legal obligation, eg in relation to gender pay reporting —Art 6(1)(f)—legitimate interests, eg operational efficiency, security
Marketing	<p>Art 6(1)(f)—legitimate interests, but this is a complex area and you may require consent in any event under PECR 2003. See drafting note to Promotional communications section</p>
External audits and quality checks	<p>Art 6(1)(f)—legitimate interests. It is certainly the case that an organisation will have a legitimate interest in obtaining and maintaining a quality mark like ISO. However, as above, the question here will be:</p> <ul style="list-style-type: none"> —does that legitimate interest outweigh the interests or fundamental rights of the data subject, and if yes: —is the processing necessary for the purpose of the legitimate interest <p>The second point could depend on whether the accreditation body insists on having access to all client/customer files or data. If it does, then you are in a stronger position to argue that the processing is necessary. If, however, the accreditation body allows you to withhold the files/data of clients who do not consent, it is far more difficult to say that the processing is necessary to obtain or maintain your accreditation and this would point you in the direction of consent as your lawful ground</p> <p>Art 6(1)(a)—consent, where you cannot rely on legitimate interests</p>

Appendix B – What we use personal data for

What we use personal data for	Our reasons
To provide legal services to our clients	For the performance of our contract with our client or to take steps at our client's request before entering into a contract
Conducting checks to identify our clients and verify their identity Screening for financial and other sanctions or embargoes Other processing necessary to comply with professional, legal and regulatory obligations that apply to our business, eg under health and safety regulation or rules issued by our professional regulator	To comply with our legal and regulatory obligations
Gathering and providing information required by or relating to audits, enquiries or investigations by regulatory bodies	To comply with our legal and regulatory obligations
Ensuring business policies are adhered to, eg policies covering security and internet use	For our legitimate interests or those of a third party, ie to make sure we are following our own internal procedures so we can deliver the best service to you
Operational reasons, such as improving efficiency, training and quality control	For our legitimate interests or those of a third party, ie to be as efficient as we can so we can deliver the best service for you at the best price
Ensuring the confidentiality of commercially sensitive information	For our legitimate interests or those of a third party, ie to protect our intellectual property and other commercially valuable information To comply with our legal and regulatory obligations
Statistical analysis to help us manage our practice	For our legitimate interests or those of a third party, ie to be as efficient as we can so we can deliver the best service for you at the best price
Preventing unauthorised access and modifications to systems	For our legitimate interests or those of a third party, ie to prevent and detect criminal activity that could be damaging for us and for you To comply with our legal and regulatory obligations
Updating and enhancing client records	For the performance of 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 or those of a third party, eg making sure that 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	To comply with our legal and regulatory obligations

Appendix B – What we use personal data for

What we use personal data for	Our reasons
	For our legitimate interests or those of a third party, eg to make sure we are following our own internal procedures and working efficiently so we can deliver the best service to you
Marketing our services and those of selected third parties to: —existing and former clients; —third parties who have previously expressed an interest in our services; —third parties with whom we have had no previous dealings.	For our legitimate interests or those of a third party, ie to promote our business to existing and former clients
External audits and quality checks and the audit of our accounts	For our legitimate interests or those of a third party, ie to maintain our accreditations so we can demonstrate we operate at the highest standards To comply with our legal and regulatory obligations