

Privacy Notice to Clients

Ashfords LLP (“Ashfords”, “we”, “us” or “our”) takes privacy very seriously. Please read this Privacy Notice to Clients carefully. It contains important information on who we are and how and why we collect, store, use and share your Client 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.

When we use Client Personal Data we are regulated by Data Protection Legislation and we are responsible as a ‘controller’ of that Client Personal Data for the purposes of Data Protection Legislation. Our use of Client Personal Data is subject to your instructions, the UK GDPR, other relevant UK legislation and our professional duty of confidentiality.

Please note the definitions of the key terms referred to in this Privacy Notice to Clients are set out at the end.

1.	Personal information we collect	2
2.	How we collect personal information	3
3.	How and why we use Client Personal Data	4
4.	Promotional communications	7
5.	Who we share personal information with	8
6.	Where we store personal information	8
7.	How long we keep personal information	9
8.	Transferring Client Personal Data out of the UK	9
9.	Your rights	10
10.	Keeping Personal Data secure	11
11.	How to complain	11
12.	Changes to this Privacy Notice to Clients	11
13.	How to contact us	12
14.	Glossary	12

1. Personal information we collect

The table below sets out the categories of Client Personal Data we will or may collect in the course of advising and/or acting for you:

Categories of Personal Data we will always collect	Categories of Personal Data we may collect
<ul style="list-style-type: none"> • Name, address, and telephone number. • Information to enable us to check and verify identity, which may include date of birth, passport details, drivers licence details, and/or utility bills. • Electronic contact details, which may include email address and mobile phone number. • Information relating to the matter in which you are seeking our advice or representation. • Information to enable us to undertake financial checks on you or your business. • Financial details in relation to monies you send to us or we send to you. Information about your use of our IT, communication and other systems, and other monitoring information. • Client Personal Data which is necessary for the matter you are instructing us on. 	<ul style="list-style-type: none"> • National Insurance and tax details. • Bank and/or building society details, for example if you are instructing us on a sale transaction. • Financial details so far as relevant to the instructions, for example, the source of funds and wealth if you are instructing us on a purchase transaction. • Details of professional online presence, which may include LinkedIn profile, Companies House information, and other publicly available resources. • Details of spouse/partner and dependants or other family members/beneficiaries of estate. • Employment status and details including salary and benefits. • Nationality and/or immigration status and information from related documents, such as passport or other identification, and immigration information. • Details of pension arrangements. • Employment records including, where relevant, records relating to sickness and attendance, performance, disciplinary, conduct and grievances (including relevant Special Category Personal Data) if required for the matter on which you are instructing us. • Racial or ethnic origin, gender and sexual orientation, religious or similar beliefs if required for the matter on which you are instructing us.

	<ul style="list-style-type: none"> • Trade union membership, if required for the matter on which you are instructing us. • Details of political opinions when conducting politically exposed person checks. • Medical records if required for the matter on which you are instructing us. • Personal Data about directorships and shareholdings. • Personal Data contained in evidence and statements made in contentious matters. • Personal Data relating to disputes with employees or third party Data Subjects. • Health records of individuals injured at work. • Social welfare reports produced in family matters. • Contact details of employees/directors so that we can communicate with them in relation to your instructions. • Personal Data of employees, directors, officers, ultimate beneficial owners, customers, suppliers or service providers. • Details of visits to our offices. • Recordings of Equity Release client meetings held at the client's residential address.
--	---

Such Personal Data may include Special Category Personal Data and/or information relating to criminal convictions and criminal offences. Further information is set out in paragraph 3 below entitled '**How and why we use your Personal Data**'.

The above categories of Personal Data are required to enable us to provide our services to you. If you do not provide such Personal Data, it may delay, or prevent, us from providing services to you.

2. How we collect personal information

Most of the Client Personal Data that we use in or in connection with the matters that you instruct us on will be either provided to us by you or created by us during the course of the matter.

We may also collect Client Personal Data:

- from publicly accessible sources, such as websites and Companies House or HM Land Registry;
- directly from third parties such as:

- sanctions screening providers;
- credit reference agencies;
- client due diligence providers;
- local and public authorities;
- the Police;
- corporate service providers;
- financial institutions or advisors;
- consultants and other professionals we may engage, or work with, or be on the other side in relation to your matter e.g. barristers, other solicitors, experts, HR consultants, valuers;
- witnesses;
- where you have instructed us to do so (in your personal capacity), from:
 - your bank, building society or other financial institution;
 - your employer and/or trade union, professional body or pension administrators;
 - your doctors, medical and occupational health professionals;
- via our website, we use cookies on our website (for more information on cookies, please see our cookies policy <https://www.ashfords.co.uk/policies-terms-and-conditions/cookie-policy>);
- through newsletters, marketing or event communications we send to you, we use link click tracking within these to manage event RSVPs and automatic unsubscribes (for more information on link click tracking please see our cookies policy <https://www.ashfords.co.uk/policies-terms-and-conditions/cookie-policy>);
- via our information technology (IT) systems;
- case management, document management and time recording systems;
- door entry systems and reception logs;
- Ashfords' recording devices supplied to Ashfords staff members and/or consultants for Equity Release clients' home visits; and
- automated monitoring of our websites and other technical systems, such as our computer networks and connections, CCTV and access control systems, communications systems, email and instant messaging systems.

3. How and why we use Client Personal Data

Under Data Protection Legislation, we can only use Personal Data if we have a proper legal basis for doing so. For example:

- to comply with our legal obligations;
- for reasons of substantial public interest;
- for the performance of our contract with you or to take steps at your request before entering into a contract;
- for our legitimate interests or those of a third party, so long as this is not overridden by your own rights

and interests; or

- where you have given consent.

Generally we do not rely on consent as a legal basis for processing your Personal Data. Where we do require consent, we will ask for that separately and clearly, and you have the right to withdraw consent at any time by contacting us.

The table below explains the purposes for which we process Client Personal Data ("Purpose") and the applicable legal basis for each Purpose:

The purpose for which we use your Client Personal Data	Legal Basis
To provide our services to you.	For the performance of our contract with you or to take steps at your request before entering into a contract with you.
<p>Conducting checks to identify our clients and verify their identity.</p> <p>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, for example, under health and safety regulations or rules issued by our professional regulator, the SRA.</p>	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 our business policies are adhered to, including policies covering security and internet use.	For our legitimate interests or those of a third party, (namely 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 and client service, the clarity, accuracy and usefulness of communications with clients, the safety of our clients, training and quality control.	<p>For our legitimate interests or those of a third party, (namely to be as efficient and effective as we can so we can deliver the best service for you).</p> <p>Your consent.</p>
Ensuring the confidentiality of confidential information.	<p>For our legitimate interests or those of a third party, (namely to protect our intellectual property and other commercially valuable information).</p> <p>To comply with our legal and regulatory obligations.</p>

Statistical analysis to help us manage our practice, including our financial performance, client base, work type or other efficiency measure.	For our legitimate interests or those of a third party, (namely to be as efficient as we can so we can deliver the best service for you).
Preventing unauthorised access and modifications to systems.	For our legitimate interests or those of a third party, (namely, to prevent and detect criminal activity that could be damaging for us and for you). To comply with our legal and regulatory obligations.
Updating 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, (namely, 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. For our legitimate interests or those of a third party, (namely, to make sure we are following our own internal procedures and working efficiently and safely so we can deliver the best service to you).
Marketing our services, knowledge and events to existing and former clients.	For our legitimate interests or those of a third party, (namely, to promote our business to existing and former clients). Your consent.
To conduct credit reference checks via external credit reference agencies. To get paid for the services we carry out for you.	For our legitimate interests or a those of a third party, (namely, to ensure your commercial viability and that we are paid in respect of the matter on which you have instructed us).
External audits and quality checks, such as SQM, CQS, or ISO accreditation and the audit of our accounts	For our legitimate interests or a those of a third party, (namely, to maintain/obtain accreditations so we can demonstrate we operate at the highest standards). To comply with our legal and regulatory obligations.

Special Category Personal Data

As and when we process Special Category Personal Data, we will process it in accordance with applicable Data Protection Legislation.

Typically, this will be where the processing is necessary for performing our contract with you or the processing is necessary for compliance with a legal obligation to which we are subject and (in addition) the processing is necessary:

(1) for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or

(2) for reasons of substantial public interest, such as where the processing is necessary for the purpose of (i) preventing or detecting unlawful acts, or (ii) protecting the public against dishonesty, or (iii) regulatory requirements relating to unlawful acts and dishonesty, or (iv) preventing fraud, or (v) making disclosures of suspicions of terrorist financing or money laundering.

On occasion we may need to obtain your explicit consent, or (in the case of another Data Subject's Special Category Personal Data) require you to obtain the Data Subject's explicit consent, before we can process that Special Category Personal Data.

If we do seek and obtain your (or another Data Subject's) explicit consent, you/they can withdraw it at any time, without affecting the lawfulness of processing based on your/their consent before its withdrawal.

Personal Data relating to criminal convictions and offences

We will only process information relating to criminal convictions and offences in accordance with applicable Data Protection Legislation.

Typically, this will be where the processing is necessary for performing our contract with you or the processing is necessary for compliance with a legal obligation to which we are subject and (in addition) the processing is necessary for the purpose of:

(1) preventing or detecting unlawful acts, or (2) protecting the public against dishonesty, or (3) regulatory requirements relating to unlawful acts and dishonesty, or (4) preventing fraud, or (5) making disclosures of suspicions of terrorist financing or money laundering, or (6) legal proceedings or obtaining legal advice or establishing, exercising or defending legal rights.

On occasion, we may need to obtain your explicit consent, or (in the case of another Data Subject) require you to obtain the Data Subject's explicit consent before we can process information relating to criminal convictions and offences.

We have in place an appropriate policy document which we are required by law to maintain when processing Special Category Personal Data and information relating to criminal convictions and offences. This is available on request by contacting us at the address specified in paragraph 13 ('**How to contact us**').

4. Promotional communications

We will always treat Client Personal Data with the utmost respect and never sell or share it with other organisations for marketing purposes.

You have the right to opt out of receiving promotional communications at any time by:

- contacting us by emailing marketingservices@ashfords.co.uk;
- using the 'unsubscribe' link in emails or 'STOP' number in texts; or
- updating your marketing preferences on our website <https://www.ashfords.co.uk/unsubscribe>.

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.

5. Who we share personal information with

We routinely share Client Personal Data with:

- our staff and members;
- our subsidiaries (for example, Curzon House Trustees Limited);
- third party professional advisers who we instruct on your behalf or refer you to or you request we send it to, for example barristers, medical professionals, accountants, tax advisors or other experts;
- other third parties where necessary to carry out your instructions, for example your mortgage provider or HM Land Registry in the case of a property transaction or Companies House, or the other side/their legal advisers in connection with a dispute, negotiation or contractual matter on which you instruct us;
- ID check and verification providers;
- another overseas law firm or other legal service provider where your matter requires legal advice in another jurisdiction;
- credit reference agencies;
- our insurers and brokers;
- external auditors;
- our bank;
- external service suppliers, representatives and agents that we use to make our business more efficient, for example, outsourced IT service providers, marketing agencies, marketing and electronic communication service providers, document collation or analysis suppliers or debt recovery service providers all based within the UK; and
- any other third parties you ask us to send it to.

We only allow our service providers to handle your Client Personal Data if we are satisfied that we have a legal basis to share the same with them and they take appropriate measures to protect your Client Personal Data. We also impose contractual obligations on service providers to ensure they can only use your Client Personal Data to provide services to us and to you.

We may disclose and exchange information with law enforcement agencies and regulatory bodies to comply with our legal and regulatory obligations.

We may also need to share some Client Personal Data with other parties, such as potential buyers of some or all of our business or during a re-structuring or merger process. Information will often be anonymised but this may not always be possible or appropriate. The recipient of the information will be bound by confidentiality obligations.

6. Where we store personal information

Information may be held at our offices and the locations of our third party agencies, service providers, representatives and agents as described above (see **'Who we share your Personal**

Data with').

Some of these third parties may be based outside the UK. For more information, including on how we safeguard your Personal Data when this occurs, see below: '**Transferring your Personal Data out of the UK**'.

7. How long we keep personal information

We keep Client Personal Data after we have finished advising or acting for you. We do so for the following reasons and purposes:

- to respond to any questions, complaints or claims you might make or which we make on your behalf;
- to show that we treated you fairly and in accordance with the law and relevant regulation; and
- to keep and process records required by law or regulation.

We will not retain and process your Client Personal Data for longer than is necessary for the purposes set out in this Privacy Notice to Clients.

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

Generally our retention periods are 7 years after the matter we are advising or acting for you on has completed. However, longer retention periods will apply for certain types of instructions. We also reserve the right to store all emails that we have sent and/or received from you or about your matter or you for up to 15 years (either ourselves or using a third party IT service provider). Further details are available by contacting us.

When it is no longer necessary to retain your Client Personal Data, we will delete or anonymise it.

8. Transferring Client Personal Data out of the UK

To deliver services to you, it is sometimes necessary for us to share and transfer Client Personal Data outside the United Kingdom (UK), for example:

- with advisors outside the UK;
- with your and our service providers located outside the UK;
- if you are based outside the UK; or
- where there is an international dimension to the matter on which we are advising you.

These transfers may be subject to special rules under UK data protection law.

Between the UK and EU (and EEA) member states:

The UK Government has deemed the EU and EEA states to be adequate to allow for data flows from the UK. The UK Government has stated that this will be kept under review. The EU has also granted the UK an 'adequacy decision'. This means that the EU has determined the UK's data protection laws to be robust enough to ensure personal data can transfer freely from the EU (and EEA) to the UK.

No additional safeguards are therefore needed at this time.

Between the UK and Non-EU (and Non-EEA) countries:

The following countries to which we may transfer Client Personal Data have been assessed by the European Commission and, from 01 January 2021, are also recognised by the UK Government as providing an adequate level of protection for Personal Data:

Andorra; Argentina; Faroe Islands; Guernsey; Isle of Man; Israel; Japan; Jersey; New Zealand; Switzerland; and Uruguay.

The European Commission has also made partial findings of adequacy in relation to Canada (for commercial organisations).

Except for the countries listed above, where we transfer Client Personal Data to non-EU (and non-EEA) countries we will ensure the transfer complies with Data Protection Legislation. Our standard practice is to use standard data protection contract clauses which have been approved by the European Commission and recognised by the UK Government/ICO. To obtain a copy of those clauses or if you would like further information please contact us (see '**How to contact us**' below).

9. Your rights

You have the following rights in respect of your Personal Data, which you can exercise free of charge:

Access	The right to be provided with a copy of your Personal Data.
Rectification	The right to require us to correct any mistakes in your Personal Data.
To be forgotten	The right to require us to delete your Personal Data - in certain situations.
Restriction of processing	The right to require us to restrict processing of your Personal Data - in certain circumstances (e.g. if you contest the accuracy of the Personal Data).
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.
To object	The right to object: at any time to your Personal Data being processed for direct marketing (including profiling); to decisions being taken by automated means which produce legal effects concerning you or similarly significantly affect you; and in certain other situations to our continued processing of your Personal Data (e.g. processing carried out for the purpose of our legitimate interests).

Not to be subject to automated individual decision-making	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.
---	---

For further information on each of those rights, including the circumstances in which they apply, please contact us or consult the guidance issued by the UK Information Commissioner’s Office (ICO) on individuals’ rights under the UK General Data Protection Regulation.

If you would like to exercise any of those rights, please:

- email, or write to us (see below: ‘**How to contact us**’); and
- let us have enough information to identify you (e.g. your full name, address and client or matter reference number); and
- 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
- let us know what right you want to exercise and the information to which your request relates.

To the extent that a Data Subject makes a request in relation to any of the above rights in relation to the Client Personal Data for which we are both a Data Controller, both you and us will provide reasonable assistance to each other in respect of any such request.

10. Keeping Personal Data secure

We have appropriate technical and organisational measures in place to look to prevent Personal Data from being accidentally lost, or used or accessed unlawfully. Those processing your Client Personal Data are subject to a duty of confidentiality.

We 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.

11. How to complain

We hope that we can resolve any query or concern you may raise about our use of your Client Personal Data.

You have the right to lodge a complaint with a supervisory authority 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/make-a-complaint/> or telephone: **0303 123 1113**.

12. Changes to this Privacy Notice to Clients

This Privacy Notice to Clients was updated on 21st July 2021. We may change this Privacy Notice to Clients from time to time.

13. How to contact us

Please contact us by post, email or telephone if you have any questions about this Privacy Notice to Clients or the personal data we hold about you.

Our contact details are shown below:

Risk & Compliance, Ashford House, Grenadier Rd, Exeter EX1 3LH

risk&compliance@ashfords.co.uk

01392 337000, asking for the Risk & Compliance team

From 1st January 2021, if you are based in the EEA you may contact our authorised representative:

Contact: Data Protection Officer

Address:

CORNET VINCENT SEGUREL

251 bd Pereire – 75852 Paris

France

Email: rgpd@cvs-avocats.com

Please ensure that, in any correspondence you send, Ashfords LLP is referenced in the subject heading.

14. Glossary

Agreement

means the agreement between you and us for the provision of legal services by us to you.

Client Personal Data

Personal Data processed by either us or both you and us under the Agreement, in respect of which (as between us and you) you are the original Data Controller. This shall include, as applicable, your Personal Data, your employees', contractors' and any other staff's Personal Data, your customers' Personal Data (either consumer customers or the representatives of any business customers, including their staff) and any other Personal Data disclosed to us by you or your representatives, or obtained by us or anyone engaged by us, in relation to the services to be provided under the Agreement.

Data Controller

Means a person or entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

Data Protection Legislation	all applicable privacy and data protection laws, including the UK General Data Protection Regulation, the Data Protection Act 2018, and any applicable regulations and secondary legislation in England and Wales relating to the processing of Personal Data and/or the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).
Data Subject	an individual who is the subject of Personal Data.
Personal Data	Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal Data Breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
Processing, processes, process	either any activity that involves the use of Personal Data or as Data Protection Legislation may otherwise define processing, processes or process. It includes any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring Personal Data to third parties.
Special Category Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership; genetic and biometric data; data concerning health, or a person's sex life or sexual orientation.
We, us, our	Ashfords LLP.