Privacy Notice

For clients

This Privacy Notice explains who we are, how we collect, share and use personal information about you, and how you can exercise your privacy rights. It can also be accessed on the Chilcotts Law website.

If you have any questions or concerns about our use of your personal information, then please contact us using the contact details provided below.

Key information	Details
Our name and contact details	Chilcotts Law Ltd is the controller responsible for your personal data. 10 Plymouth Road, Tavistock, Devon PL19 8AY Telephone 01822 612535 Company number 07154620 ICO registration number Z3630164
Our Data Protection Officer	David Wilde dpo@chilcottslaw.com 01822 612535
Person responsible for dealing with complaints relating to data use	David Wilde dpo@chilcottslaw.com 01822 612535
Personal data	Any information relating to an identified or identifiable individual.
Data subject	The individual to whom the personal data relates.
Special category data	Sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), data concerning health, sex life or sexual orientation.
Purposes of our processing data	In order to provide legal advice and services we obtain, record, store, organise, structure and use personal information about clients and others.

Key information	Details
Legal basis for processing data	Under data protection law, we can only process personal data if we have a lawful basis for doing so. These lawful bases are set out in Article 6 of the UK General Data Protection Regulation (UK GDPR). The bases we are most likely to rely on are: Consent – the individual has given clear consent for us to process their personal data for a specific purpose. Contract – the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract. Legitimate interest – the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. Legitimate interests can include our business or commercial interests (such as marketing, IT security, ensuring our internal policies are being complied with, obtaining and maintaining accreditations) as well as wider societal benefits (such as fraud prevention). Note that there is a new 'Recognised Legitimate Interest' under the Data (Use & Access) Act 2025 (DUAA) which may apply in limited circumstances. Legal obligation – the processing is necessary for us to comply with the law, such as our anti-money laundering and sanctions obligations, or to comply with a court order.
Information security	We have implemented appropriate technical and organisational measures to keep your personal data confidential and secure from unauthorised access, use and disclosure. Within our firm, those processing your personal data will do so only in an authorised manner and are subject to a duty of confidentiality. 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.

What personal information does Chilcotts Law collect and why?

The personal information that we may collect about you broadly falls into the following categories:

Information that you provide voluntarily

We may ask you to provide personal information voluntarily: for example, we will ask you to provide your contact details to deliver the service we have agreed, to enable you to subscribe to marketing communications from us, and/or to enable us to respond to enquiries submitted to us. We may also ask you to provide other personal information. The personal information that you are asked to provide, and the reasons why you are asked to provide it, will be made clear to you at the point we ask you to provide your personal information. Some of the personal information that we ask you to provide may include sensitive personal information, such as health-related information or information about your race or ethnicity, which we may need in order to provide the service to you.

Depending on your matter, we may ask for identity documents, information about joint clients or others involved in your matter, and financial information such as evidence of the source of funds or wealth.

Information that we collect automatically

If you visit our website, we may collect certain information automatically from your device. Specifically, the information we collect automatically may include information like your IP address, device type, unique device identification numbers, browser-type and other technical information. We may also collect information about how your device has interacted with our website, including the pages accessed and links clicked. Please see our Cookie Policy for details of cookies and how to manage your preferences.

Collecting this information enables us to better understand the visitors who come to our website, where they come from, and what content on our website is of interest to them. We use this information for our internal analytics purposes and to improve the quality and relevance of our website to our visitors.

Information that we obtain from third party sources

From time to time, we may receive personal information about you from third parties, including Thirdfort, banks and building societies, other people involved in your matter and professionals we engage, where those sources are permitted to share it with us.

The types of information we collect from third parties include identity and screening results, financial information and information about the circumstances of your matter. We use that information to verify identity, meet applicable obligations, progress your matter and maintain accurate records.

We may also collect information from publicly accessible sources, such as Companies House and HM Land Registry.

How we use your information

Our use of your information is subject to your instructions (where applicable), the Data Protection Act 2018, the UK GDPR, the Data (Use and Access) Act 2025 and our duty of confidentiality to you (where you are a client). We will collect information about you and keep this electronically, including on our computers, our case management/ document management/ time recording systems, in our email and instant messaging systems, in cloud storage, in our reception logs and on paper for a certain period of time. Under data protection law, we can only use your personal data if we have a proper reason for doing so. See the ‘Legal basis for processing personal information’ section below for further details. The main reasons for using/ processing your information/ data are to:

- deliver the legal services we have agreed in contract to provide to you. For example, we may use your information to write letters/ emails etc on your behalf or prepare legal documents to help you with your matter;
- comply with the law and our professional obligations. This includes checking for conflicts of interest and reporting suspicious activity to the National Crime Agency where required.

We use cloud storage providers to store data and ensure that our contracts with them comply with applicable law. We use Microsoft 365, including SharePoint and OneDrive, for cloud storage and document management. If you have any concerns about cloud storage, please let us know.

In some cases, we may hold more sensitive information about you, such as health information, where necessary in connection with your legal matter. If we handle special category data, we rely on an applicable condition under Article 9 UK GDPR, such as establishing, exercising or defending legal claims. Where relevant, we also meet the requirements of the Data Protection Act 2018. We handle criminal offence data only where authorised by law and with the applicable safeguards.

Except for the provision of legal services where we rely on other legal conditions to process your data, if we have obtained your consent to use your information in a particular way, you can withdraw such consent but this may limit what more we can do for you (if anything). In such cases we will explain to you any limitations that may apply to the service we provide to you.

We use Thirdfort for identity verification where appropriate and to screen all client matters for politically exposed persons (PEPs) and sanctions. Personal data we obtain to comply with our statutory anti-money laundering obligations is used for preventing money laundering and terrorist financing or for another purpose permitted by law.

We may send you legal updates or information about our services. For electronic marketing, we ask for consent where required or use the existing customer exception where its conditions are met, including offering you an opportunity to opt out when we collect your details and in each message. You can opt out by emailing David Wilde or using the unsubscribe link. We only contact you for market research if you have opted in. We do not share your data for other organisations' own marketing.

Your information may be held on computer servers in the UK or processed by service providers. If your matter or a supplier involves a restricted international transfer, we will use applicable UK adequacy regulations, appropriate safeguards such as the UK International Data Transfer Agreement or UK Addendum, or a lawful exception. You can contact us for details of the safeguards and how to obtain a copy.

Our staff review potential screening matches. Decisions about whether we can accept or continue your matter are made with human review. Where we use AI-assisted legal tools to support our work, we apply appropriate confidentiality, security and data protection safeguards.

Will you share my information with anyone else?

We may need to share information as part of your legal matter, for example with other lawyers, witnesses, lenders, experts and other professionals we engage, or with courts, tribunals, HM Land Registry and other public bodies. We also work with trusted service providers, including Thirdfort, Microsoft 365, our practice management and document management providers, IT support and archive storage providers. We may share information with external auditors, the Solicitors Regulation Authority and CQS assessors, and with our professional indemnity insurers and their advisers, where necessary.

We sometimes need to make reports of suspicious activity to the National Crime Agency (NCA), which may contain personal data and we may have to disclose the identity of the people for whom we hold client money in our pooled client account if requested to do so by our bank.

We require contractors handling information on our behalf to keep it confidential and use it only as authorised. If you have questions about how we work with service providers, please contact us.

If you instruct us jointly with another client then it will be necessary to share certain information relevant to you with the corresponding joint client in order to fulfil your instructions to us.

Legal basis for processing personal information

Our legal basis for collecting and using the personal information described above will depend on the personal information concerned and the specific context in which we collect it. However, we will normally collect personal information from you only where we have your consent to do so, where we need the personal information to perform a contract with you, or where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms. In some cases, we may also have a legal obligation to collect personal information from you or may otherwise need the personal information to protect your vital interests or those of another person.

If we ask you to provide personal information to comply with a legal requirement or to perform a contract with you, we will make this clear at the relevant time and advise you whether the provision of your personal information is mandatory or not (as well as of the possible consequences if you do not provide your personal information, such as not being able to act in your matter without receiving the necessary information).

Similarly, if we collect and use your personal information in reliance on our legitimate interests (or those of any third party), we will make clear to you at the relevant time what those legitimate interests are.

If you have questions about or need further information concerning the legal basis on which we collect and use your personal information, please contact us using the contact details provided under the "What if I have other questions or concerns" heading below.

How long will you keep my information?

We retain personal information where we have an ongoing need to provide legal services, comply with legal or regulatory obligations or deal with complaints or claims. We may retain limited information after file closure for future conflict checks.

We normally keep records required by the Money Laundering Regulations for five years from the end of the business relationship or completion of an occasional transaction, as applicable. We delete personal data obtained for those checks at the end of the applicable period unless the Regulations allow or require us to retain it for longer.

As a general rule, we keep most paper and electronic client matter files for eight years from the conclusion of the matter. Where a matter relates to a minor, the applicable period runs from their 18th birthday. Different periods apply to some records under our Retention Policy:

- Will files are kept until six years after the testator's death or, if the date of death is unknown, until they would have reached 110.
- Probate and estate administration files are kept for 12 years from the conclusion of the matter or distribution of the estate, as applicable.
- We keep original wills and copies of grants of probate held for safekeeping indefinitely, subject to your instructions and applicable authority. We offer paid annual or five-year title deed storage under arrangements agreed with you.

You can ask us for more detail about our Retention Policy.

We also have a right in relation to client files to retain papers in order to exercise a lien (the right to withhold papers due to unpaid fees) and to demonstrate a legally admissible record at a later date of the work we have performed should it be necessary to do so.

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymise it or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

Can I see what information you hold about me?

You have the following data protection rights:

- If you wish to access, correct, update or request deletion of your personal information, you can do so at any time by contacting us using the contact details provided below.
- Depending on the circumstances, you can object to the use of your personal information, ask us to restrict its use or request that eligible information be provided in a portable format.
- You have the right to opt-out of marketing communications we send you at any time. You can exercise this right by clicking on the "unsubscribe" or "opt-out" link in the marketing e-mails we send you. To opt-out of other forms of marketing (such as postal marketing or telemarketing), then please contact us using the contact details provided below.
- Similarly, if we have collected and processed your personal information with your consent, then you can withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent.
- Where the right applies, you can ask for human review and challenge a significant decision made solely by automated means.

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws.

We may charge for document storage and for copying or retrieving a client file under our terms. Your right to request access to your personal data is separate and normally free of charge. To make a request, contact David Wilde by email, telephone or post. You may use our data rights request form if you wish. We may ask for enough information to verify your identity or a representative's authority where necessary.

What if I have other questions or concerns?

Our Data Protection Officer and contact for data protection complaints is David Wilde. You can email dpo@chilcottslaw.com, telephone 01822 612535 or write to us at the address above. If you need assistance making a request or complaint, or need this notice in an alternative format, please let us know.

Please contact David if you

- wish to complain about how your personal data is being used;
- wish to request that our records about your personal information be corrected or deleted;

We will acknowledge data protection complaints within 30 days of receiving them. We will take appropriate steps to investigate, keep you informed and tell you the outcome without undue delay. Our client complaints procedure is available on our website or on request.

You have the right to complain to the Information Commissioner. If you remain dissatisfied with our response or the way we handled your complaint, you can use the ICO data protection complaints service, call 0303 123 1113 or write to the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

First published 11 May 2018. Updated 18 November 2026.