

PRIVACY NOTICE – Effective 30 July 2026

This notice sets out information relating to the collection and use of personal data in the course of CSK Legal’s business operations in accordance with the provisions of the UK General Data Protection Regulation (“**UK GDPR**”) and the Data Protection Act 2018 (“**the 2018 Act**”). We take our obligations concerning personal data seriously.

1. Business Details

CSK Legal Limited (collectively referred to as “*CSK Legal*”, “*we*”, “*us*” or “*our*” in this privacy notice) is the data controller and responsible for the personal data obtained.

2. Contact Details

Full name of legal entity: CSK Legal Limited
E-mail Address: administration@csklegal.co.uk
Postal Address: 38A George Street, Birmingham, West Midlands, B3 1QA
Telephone Number: 0121 306 0170

Personal data subjects have the right to make a complaint at any time to the Information Commissioner’s Office (“**ICO**”), the UK supervisory authority for data protection issues (www.ico.org.uk).

3. Types of Personal Data Used

Personal data means “*any information relating to an identified or identifiable natural person (‘data subject’); 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*”

We may process personal data in many ways when providing legal services to clients or engaging with third parties, and when undertaking other business activities, such as collecting, using, storing, publishing and accessing personal data about individuals. The data we process can be incredibly diverse and examples would be:

“**Aggregated or Statistical Data**” includes statistical or demographic data which may be derived from personal data but which does not directly or indirectly reveal the identities of individuals. Aggregated data combined with personal data so is treated as combined data and processed in accordance with this privacy notice.

“**Behavioural Data**” includes information about behaviour, preferences or interests.

“**Contact Data**” includes address (home, business and correspondence), e-mail address and telephone numbers.

“**Criminal Offence Data**” information about criminal convictions and offences, allegations, criminal proceedings, cautions, warnings, reprimands, DBS check results and related information used to assess suitability for a role.

“**Employment Data**” information about roles, job titles, working arrangements, employment dates, contract details, reporting lines, promotion history, remuneration grade, benefits, and termination information.

“**Employment Status Check Data**” information required to confirm eligibility to work in the UK and employment statuses, right to work documentation, immigration status, identification documents and background checks.

“**Family Data**” information about family members, dependents, next of kin.

“Financial and Tax Data” includes bank account details, credit card information, payroll information, salaries, pension information, tax codes, National Insurance number and other information required for payment, deductions and financial administration.

“Identity Data” includes names, usernames or similar identifiers, marital status, date of birth and gender.

“Marketing Data” includes preferences in receiving marketing or advertising from us or our third parties, communication preferences, records of consents, opt-ins and opt-outs.

“Monitoring Data” records relating to attendance, timekeeping, training completion, supervision, performance, conduct, grievance and disciplinary matters, IT and system usage where monitored, and other records created in the course of managing a working relationship.

“Recruitment Data” information submitted as part of an application to work, such as CVs, employment history, qualifications, training, references, interview notes, application records and related correspondence.

“Special Category Data” (as defined by the UK GDPR) includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health, and data concerning a person’s sex life or sexual orientation.

“Technical and Usage Data” internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, device information and other technology on the devices you use to access this website or services.

4. How We Collect Information

We use different methods to collect data from and about an individual including:

- In the process of carrying out work for an individual (or your business) where we will in, almost all instances, act as a controller. In very limited circumstances we may act as a processor in which case we will let the individual know and ensure that an appropriate contract is put in place.
- When we communicate by email or other electronic methods, by telephone or using video conferencing, we may collect such data via our website.
- We may receive personal data from third parties, such as when taking statements from witnesses, or experts, or others of interest. We may receive personal data from open source and subscription access websites/services provided by others.
- Technical Data may be collected from analytics providers such as Google based outside of the UK.

You can set your browser to refuse all or some browser cookies from our website, or from some services we may offer. If you disable or refuse cookies, some parts of the services may become inaccessible or not function properly. CSK Legal’s [Cookie Policy](#) provides information about cookies on our website.

5. Justification for Processing Personal Data

Article 6 UK GDPR

Data controllers are required to have a legal basis for collecting and using personal data. We rely principally on the basis of legitimate interest.

Article 9 UK GDPR

Where we process **Special Category Data**, we rely on one or more of the following conditions under **Article 9 UK GDPR**, as applicable. We would rely on the following grounds in different circumstances in respect of such processing:

- **Explicit consent:** Where consent is given to the processing of Special Category Data (often by the client or individual concerned).
- **Legal claims:** As a solicitors practice, the primary purpose for us holding and processing special category data from clients is to advise and undertake action for them as legal representatives. This processing is necessary for the establishment, exercise or defence of legal rights and claims. We may additionally process, for by way of storage, for example, personal data to establish, exercise or defend our legal rights and those of our clients.
- **Substantial public interest.** We may process data for meeting our regulatory obligations, such as, publishing diversity data of employees to our regulatory, with the view to encouraging greater diversity in legal profession.
- **Made public by the data subject.** Data subjects may have made their Special Category Data public and, where so, we may process on this basis.

6. Purposes for which we will use personal data

We have set out below a description of the ways we may use various categories of personal data. This is not exhaustive. We have identified what our legitimate interests by way of examples.

The Articles to which we refer are to those set out in the UK GDPR.

<u>Purpose/Use</u>	<u>Type of Data Processed</u>	<u>Legal Basis (as per the Articles set out in the UK GDPR)</u>
<u>Website</u>		
To improve our website and the services we provide	- Behavioural Data - Technical and Usage Data	Article 6(1)(f) – necessary for legitimate interests in improving and maintaining our website, developing our business, and informing our marketing strategy.
Staff Profiles (including staff names, photographs, roles and experience on the website)	- Employment Data - Identity Data - where relevant, Special Category Data	Article 6(1)(f) – necessary for legitimate interests in promoting our business, introducing our team to clients and prospective clients, and providing information about staff roles, experience and expertise. Where we process Special Category Data, we rely on one or more of the following conditions pursuant to Article 9: Article 9(2)(a) - the individual has given explicit consent; and/or Article 9(2)(e) – the data has been manifestly made public by the individual
<u>Administering Employment</u>		

Recruiting staff and managing/administering ongoing relationships (e.g. DBS checks, payroll, employee records).	- Contact Data - Criminal Offence Data - Employment Data - Employment Status Check Data - Family Data - Financial and Tax Data - Identity Data - Monitoring Data - Recruitment Data - where relevant, Special Category Data	Article 6(1)(b): Necessary for performance of the employment contract. Article 6(1)(c): Necessary for compliance with legal obligations as an employer. Where we process Special Category Data, we rely on one or more of the following conditions pursuant to Article 9: Article 9(2)(b) – necessary for carrying out obligations and exercising specific rights in the field of employment law; and/or Article 9(2)(f) – necessary for the establishment, exercise or defence of legal claims Where criminal offence data is processed, Article 10 UK GDPR and an applicable condition under Schedule 1 of the Data Protection Act 2018 will also apply (including where necessary for employment, safeguarding, regulatory compliance or legal claims)
Management of Security Systems	- Contact Data - Identity Data - Monitoring Data - Technical and Usage Data	Article 6(1)(f) – necessary for legitimate interests in ensuring the security of our networks, systems, devices, information and services, and in preventing unauthorised access, misuse, fraud and other security incidents.
Business management and planning including accounting and auditing	- Aggregated or Statistical Data - Contact Data - Employment Data - Financial and Tax Data - Identity Data - Monitoring Data - Recruitment Data	Article 6(1)(c) – where necessary for compliance with legal obligations. Article 6(1)(f) – necessary for legitimate interests in managing and planning our business operations, finances and resources, including accounting and auditing.
Health and medical management of employees (including, but not limited to: fitness to work assessments, sickness absence, reasonable adjustments, health-related benefits, health and safety, wellbeing, health-related departures, ill-health pension/share-plan decisions, disciplinary matters and legal disputes involving health data)	- Contact Data - Employment Data - Identity Data - Monitoring Data - Where relevant, Special Category Data	Article 6(1)(b) – necessary for the performance of the employment contract. Article 6(1)(c) – necessary for compliance with our legal obligations in relation to employment, health and safety and workforce management. Article 6(1)(f) – necessary for our legitimate interests in safeguarding and promoting the wellbeing of our workforce and others. Where we process Special Category Data, we rely on one or more of the following conditions pursuant to Article 9:

		Article 9(2)(b) – necessary for carrying out obligations and exercising specific rights in the field of employment law; Article 9(2)(c) – necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; and/or Article 9(2)(f) – necessary for the establishment, exercise or defence of legal claims.
Provision of Legal Services		
Dealing with client enquiries	- Contact Data - <i>Where relevant,</i> Criminal Offence Data - Family Data - Financial and Tax Data - Identity Data - Matter Data - <i>Where relevant,</i> Special Category Data	Article 6(1)(f) – necessary for legitimate interests in responding to enquiries, assessing whether we can assist, and managing prospective client relationships Where we process Special Category Data, we also rely on one or more of the following conditions pursuant to Article 9: Article 9(2)(f) – necessary for the establishment, exercise or defence of legal claims. Where Criminal Offence Data is processed: Article 10 and Data Protection Act 2018 Schedule 1 conditions - where necessary for legal advice, legal proceedings, or establishing, exercising or defending legal rights.
Client onboarding (including conducting conflict checks, anti-money laundering, sanctions screening and source of funds checks)	- Contact Data - Compliance Data - <i>Where relevant,</i> Criminal Offence Data - Family Data - Financial and Tax Data; - Identity Data - <i>Where relevant,</i> Special Category Data	Article 6(1)(b) — necessary for entering into or performing our contract with you. Article 6(1)(c) — necessary for compliance with our legal and regulatory obligations, including anti-money laundering, sanctions, client due diligence, conflicts, accounting, tax and professional obligations. Article 6(1)(f) — necessary for legitimate interests in managing risk, preventing fraud, conducting conflict checks, and administering our practice. Where we process Special Category Data, we rely on one or more of the following conditions pursuant to Article 9: Article 9(2)(f) – necessary for the establishment, exercise or defence of legal claims; and/or Where Criminal Offence Data is processed:

		Article 10 UK GDPR and an applicable Data Protection Act 2018 Schedule 1 condition.
Providing legal advice and representation	- Contact Data - Court, Tribunal and Regulatory Data - Criminal Offence Data (<i>where relevant</i>) - Employment Data (<i>where relevant</i>) - Family Data - Financial and Tax Data - Identity Data - Matter Data - Monitoring Data (<i>where relevant</i>) - Professional Contact Data - Where relevant, Special Category Data	Article 6(1)(b) — necessary for the performance of our contract with you. Article 6(1)(f) — necessary for legitimate interests, and those of our clients, in providing legal services, managing legal matters, communicating with third parties, and protecting legal rights. Article 6(1)(c) — necessary for compliance with legal, regulatory, court, tribunal or professional obligations. Where Special Category Data is processed: Article 9(2)(f) – necessary for the establishment, exercise or defence of legal claims. Where Criminal Offence Data is processed: Article 10 UK GDPR and Data Protection Act 2018 Schedule 1 conditions.
Communicating with clients, prospective clients, witnesses, experts, counsel, counterparties, courts, tribunals and other third parties	- Identity Data - Contact Data - Professional Contact Data - Matter Data - Communications Data - Technical and Usage Data, (where communications are through online portals or systems)	Article 6(1)(b) — where communication is necessary for performing the client retainer. Article 6(1)(c) — where communication is required by law, court rules, tribunal rules, regulatory rules or professional obligations. Article 6(1)(f) — necessary for legitimate interests in managing matters, obtaining and providing information, communicating with relevant parties, and progressing legal work.
Managing client money, billing and payments	- Contact Data - Financial and Tax Data - Identity Data	Article 6(1)(b) — necessary for performing the retainer and billing for legal services. Article 6(1)(c) — necessary for compliance with tax, accounting, client-money, AML and professional obligations. Article 6(1)(f) — necessary for legitimate interests in managing payments, recovering unpaid fees and maintaining financial records.
Complying with legal and regulatory obligations.	- Compliance Data - Contact Data - Court, Tribunal and Regulatory Data - Criminal Offence Data (<i>where relevant</i>) - Family Data - Financial and Tax Data	Article 6(1)(c) — necessary for compliance with legal and regulatory obligations. Article 6(1)(f) — necessary for legitimate interests in managing risk, maintaining records, handling complaints, responding to regulators and defending our legal position.

	- Identity Data - Matter Data - Monitoring Data - where relevant, Special Category Data	Where Special Category Data is processed: Article 9(2)(f) – necessary for the establishment, exercise or defence of legal claims Article 9(2)(g) substantial public interest with a Data Protection Act 2018 Schedule 1 condition. Where Criminal Offence Data is processed: Article 10 UK GDPR and Data Protection Act 2018 Schedule 1.
--	--	---

7. Automated Decision-Making

We do not make decisions about an individual based solely on automated processing (i.e. without human involvement) that would have legal, or similarly significant, effects for that individual.

8. Disclosures of Your Personal Data

We may need to share personal data with service providers (including, but not limited to: IT and hosting providers, payroll and pension providers, DBS/background check providers, professional advisers, insurers, regulators, local authorities) for the purposes set out in the table (6) (see above, “Purposes for which we will use personal data”).

We require all third parties with whom we share personal data to respect its security and to process it in accordance with applicable data protection law and any relevant contractual arrangements. Where a third-party processes personal data on our behalf, we only permit them to process it for specified purposes, in accordance with our instructions, and subject to appropriate confidentiality and security obligations. Where we share personal data with third parties who act as independent controllers (such as regulators, local authorities, safeguarding bodies, professional advisers, insurers) and they will be responsible for processing that personal data in accordance with their own data protection obligations.

9. International Transfers

We may transfer personal data to a third country. Where we do so, we seek to ensure that the transfer complies with UK data protection law. This may include transferring data to a country covered by UK adequacy regulations, using the UK International Data Transfer Agreement or the UK International Data Transfer Addendum to the European Commission’s standard contractual clauses, or relying on another lawful transfer mechanism.

10. How We Keep Your Information Safe

We and our processors have put in place appropriate security measures to prevent an individual’s personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Access to personal data is restricted to those employees, agents, contractors and other third parties who require such access for legitimate business purposes.

11. How Long We Keep Information

We retain personal data for as long as reasonably necessary to fulfil the purposes it was collected it for.

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

Typically, we would retain the information during the course of the relationship with the party concerned are being provided, or employment is being maintained, or there is some ongoing relationship with the third party/website user concerned. Where any such relationship ends, we usually retain data for a period of at least seven years.

12. Your Legal Rights

Under certain circumstances, an individual has rights under data protection laws in relation to their personal data. However, these rights to **do not exist where by complying with any request, we might breach a duty of confidentiality or breach legal privilege**. As a solicitors practice, this will likely apply in the vast majority of business operational matters with which we deal where any request is made by a non-client or non-employee.

The various rights, however, to the extent that they apply, would be:

Request access to your personal data (commonly known as a “*data subject access request*”). This enables an individual to receive a copy of the personal data we hold about them.

Request correction of your personal data that we hold about them. This enables the individual to have any incomplete or inaccurate data we hold about them corrected, though we may need to verify the accuracy of the new data they provide to us.

Request erasure of your personal data in certain circumstances. This enables an individual to ask us to delete or remove personal data where there is no good reason for us continuing to process it. They have the right to ask us to delete or remove their personal data where they have successfully exercised their right to object to processing (see below), where we may have processed their information unlawfully or where we are required by law to erase their personal data.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about the individual’s situation which causes them to object to processing on this ground if they feel it impacts on their fundamental rights and freedoms. They have the right to object where we process their personal data for direct marketing purposes. However, we may demonstrate that we have legitimate grounds to process their personal data which overrides their rights and freedoms.

Request restriction of processing an individual’s personal data. This enables an individual to ask us to restrict the processing of their personal data in the following scenarios:

- if they want to establish the personal data’s accuracy;
- where our use of the personal data is unlawful but they do not want us to erase it;
- where we no longer need the personal data for processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing under Article 21(1) pending verification whether the legitimate grounds of the controller override those of the data subject.

Request transfer of an individual’s personal data to the individual or to a third party. We will provide to an individual, or a third party they have chosen, the individual’s personal data in a structured, commonly used format.

Right to withdraw consent where we rely on consent as the basis for processing personal data, withdrawal will not affect the lawfulness of processing carried out before withdrawal. We rarely rely on consent, however.

An individual does not usually have to pay a fee to access their personal data (or to exercise any of the other rights). However, a reasonable fee may be charged if the request is manifestly unfounded, repetitive or excessive. Alternatively, we may decline to comply in such circumstances.

We may request information and identification documentation from an individual to help us confirm the individual’s identity when exercising their rights. This is to assist in preventing personal data from being disclosed to any person that has no right to receive it.

We seek to respond to all legitimate requests within one month, although it could take longer if the individual's request is complex or they have made a number of requests. In this case, we will notify them and keep them updated.

13. Changes to the Privacy Notice and Your Duty to Inform Us of Changes

We keep our privacy notice under regular review. This version was last updated in July 2026. It is important that the personal data we hold about an individual is accurate and current. Individuals with a relationship with CSK Legal are asked to keep us informed of all personal data changes which occur during CSK Legal's relationship with them, for example a new address or email address.

14. Third-Party Links and Social Media

This website may include links to third-party websites, plug-ins, applications or social media platforms. In the event an individual accesses those links or enables those connections, a third party may be able to collect or share personal data about that individual. CSK Legal does not control these third-party websites and are not responsible for their content or privacy statements. We encourage individuals to read the privacy policy of every website/platform you visit.

Where an individual interacts with us through social media, the use of that platform is also subject to the platform's own terms and privacy policy. Please do not send sensitive personal information through social media.