

Privacy Policy

CC33, a provider of outsourced client services, respects and values the privacy of prospective and existing clients, including their customers. We are committed to responsibly protecting your privacy, ensuring that you feel secure and valued in our professional relationship.

Definitions

Data Controller: When CC33 is the data controller, we exercise complete control over how your data will be processed. As a data processor, we ensure that your data is processed responsibly and in accordance with applicable laws and regulations. This control over data processing is designed to provide reassurance and confidence in managing your personal information. The point of contact for this privacy statement is privacy@cc33.co.uk.

We may process and store information about prospective, current, or former clients, including any agents, employees, or representatives of our clients, as part of our business relationship with our clients. We also process and store information about individuals applying for employment with CC33. As a registered entity with the Information Commissioner's Office (ICO), we are dedicated to protecting this information in accordance with this privacy statement, ensuring you feel confident and secure in our data processing practices.

Data Subject: Individuals whose personal information was provided by our clients, their employees, prospective clients, and those applying for employment with CC33.

Personal Data: Any information about an identified or identifiable natural person. An identifiable natural person can be directly or indirectly identified from the information.

Sensitive Data: Any information, such as medical records, race, religion, sexuality, and political or trade union membership. We process this information with the utmost care and respect for your privacy.

Third-Party: Any individual or entity that is neither CC33 nor an employee, agent, contractor, or representative.

Data Processing: Any action performed on personal information, including collection, recording, organising, storing, sharing, and transmitting. This includes electronic and paper documents containing personal information.

Legislation: CC33 complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Where applicable, such as when processing the personal data of individuals located in the European Union, we also adhere to the requirements of the EU General Data Protection Regulation (EU GDPR) and any other relevant data protection laws or international transfer mechanisms.

Legal Basis for Processing: CC33 processes data based on the following legal bases.

Consent: Explicit consent was obtained from data subjects, particularly for the processing of Sensitive Data and for direct marketing to individuals' personal addresses, emails or telephone numbers.

Contractual Necessity: When data processing is necessary to perform a contract between CC33 and our client or their customers.

Legitimate Interests: CC33 processes personal data where it is necessary for the legitimate interests pursued by either CC33 or our clients, provided that the rights and freedoms of the data subjects do not override these interests. This includes activities such as communicating with prospective clients or employees, delivering services on behalf of our clients, and marketing to business customers. Where

legitimate interest is the basis, we continually assess the potential impact on individuals and ensure appropriate safeguards are in place.

Legal Obligation: This basis applies when CC33 is required to process personal data to comply with a legal or regulatory requirement, such as obligations under employment law, tax law, or data protection legislation.

Personal Data We Collect

CC33 collects personal data to operate effectively, fulfil our contractual obligations to clients, and communicate with existing and prospective employees. We only collect the minimum personal information necessary for each specific purpose and refrain from gathering information unnecessarily.

Personal data may be collected directly from individuals or provided to us by our clients or trusted third-party sources. The types of personal data we may collect include:

- Name
- Email address
- Home or work address
- Mobile or landline telephone number
- Information necessary for our clients to deliver services to their customers (e.g. customer reference numbers, service history, etc.)
- Employment-related information for recruitment purposes and to ensure employment regulations are complied with.

Website Visitor: We may collect technical information about the devices used to access our website. This may include IP addresses, browser types, operating systems, domain names, access times, and referring website addresses. This information is used to ensure the smooth operation of our website, diagnose issues, analyse usage trends, and enhance the overall user experience.

Business Contact Information: We collect and maintain business contact information for our clients and prospective clients to manage relationships, provide services, and support business development activities.

Retention of Personal Data: CC33 retains personal data in accordance with our Data Retention Policy, to fulfil the purposes for which it was collected, such as delivering contracted services or complying with legal and regulatory obligations. Retention durations may vary depending on client instructions, the nature of the data, and applicable statutory requirements. Where relevant, specific timeframes will be set based on contractual commitments or regulatory obligations.

Where We Obtain Data To Provide Our Services

We obtain personal data from various legitimate sources to deliver our services effectively, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. These sources may include our clients, who have a lawful basis for providing such data to us, as well as third-party providers such as credit reference agencies, public databases, and other lawful channels.

Upon request, we can disclose the origin of the data we hold, provided that doing so does not infringe upon confidentiality or contravene our contractual or legal obligations. To make such a request, please contact our Data Protection Officer at privacy@cc33.co.uk.

How We Use Personal Data

CC33 processes personal data for specific, lawful purposes in accordance with applicable data protection laws and regulations. These include:

- **Client Data Processing:** We process our clients' customer information strictly in accordance with their documented instructions, and solely to fulfil the contractual obligations between CC33 and our client.
- **Business-to-Business Marketing:** We may process business contact details to promote our services to current or prospective business clients, under the lawful basis of legitimate interest. Individuals contacted in this context will always have the option to opt out of further communications. We will maintain records of such preferences to ensure compliance with applicable laws.
- **Recruitment Activities:** When communicating with prospective employees, we rely on our legitimate interest in growing our workforce. Individuals may opt out of further contact at any time, and we will promptly process and record such requests.

We do not send marketing materials to personal email addresses or home addresses without the individual's explicit consent.

Sensitive (Special Category) Data

CC33 will only process sensitive personal data, such as information relating to health, race, ethnicity, political opinions, religious beliefs, sexual orientation, or trade union membership, where we have obtained the individual's explicit consent or where an alternative lawful basis under the UK GDPR applies (e.g. for employment law obligations or to protect vital interests). All such data is processed with the highest level of care and appropriate safeguards.

Security of Personal Data

CC33 stores all personal data in controlled, secure environments designed to prevent unauthorised access, use, alteration, or disclosure. We maintain an Information Security Management System (ISMS) that governs the secure processing and storage of electronic data in line with recognised best practices.

Our security measures include, but are not limited to:

- Role-based access controls
- Encryption of data in transit and at rest
- Pseudonymisation where appropriate
- Regular vulnerability assessments and security audits
- Ongoing staff training in data protection and information security

These safeguards are reviewed regularly to ensure their effectiveness and alignment with evolving regulatory and security requirements.

Use of Cookies

When you visit our website, we may collect specific technical data using cookies to support system administration, traffic filtering, domain identification, and usage analytics. In most cases, this data does not directly identify individuals. However, some cookies, particularly targeting cookies, may collect limited personal information such as IP addresses or device identifiers.

We may use the following categories of cookies:

- **Analytical or performance cookies**

These allow us to recognise and count the number of visitors to our website and observe how they navigate the site. This helps us improve website performance and usability by ensuring users can easily find what they need.

- **Functionality cookies**

These cookies are used to remember your visit when you return to the site, allowing us to tailor content or settings based on your previous visits.

- **Targeting cookies**

These track the pages you visit and the links you follow to help us tailor advertising and website content to your interests. This data may be shared with third parties for advertising purposes.

Cookie Control

You can manage your cookie preferences through your browser settings or our website's cookie consent tool, where applicable. Most browsers accept cookies by default, but you can usually modify your settings to decline or delete cookies if you prefer. Please note that disabling certain cookies may affect your experience and limit some website features.

Links to Other Websites

Our website may contain links to external websites for your convenience and information. Please note that once you leave our site by following such a link, we do not have control over the content, functionality, or privacy practices of the destination website. As such, we cannot be responsible for the protection and privacy of any information you provide while visiting these sites, and this privacy notice does not apply to them. We recommend reviewing the privacy policies of any third-party websites you visit.

Sharing Data With Third Parties

C33 does not sell, rent, or lease personal data to third parties.

However, we may share personal data with trusted third-party service providers (contractors) who support us in delivering our services. These parties may include IT service providers, communication platforms, or other operational partners.

All such contractors are required to implement security measures equivalent to those used by CC33 and, where applicable, are bound by legally enforceable agreements. These agreements ensure that your personal information remains confidential, secure, and is processed solely by our documented instructions and for no other purpose.

How to Access and Control Your Data

Clients and individuals have the right to access the personal data we hold about them, ensuring it is accurate, up-to-date, and relevant to the purposes for which it was collected.

To request access, please submit a Subject Access Request (SAR) to privacy@cc33.co.uk. We will respond within one calendar month of receiving your request, in accordance with the UK General Data Protection Regulation (UK GDPR).

You may also contact us with personal data enquiries by calling 0114 399 0087 or writing to us at our registered office address, which can be found on our website or company correspondence.

Your Rights

Under the UK General Data Protection Regulation (UK GDPR), individuals have the following rights regarding their personal data:

- **Right to Rectification:** You have the right to request the correction of any inaccurate or incomplete personal data we hold about you.
- **Right to Erasure:** Also known as the "right to be forgotten," this allows you to request the deletion of your personal data under certain circumstances, such as when the data is no longer necessary for the purpose for which it was collected.
- **Right to Restrict Processing:** You may request that we limit the processing of your data if you contest its accuracy, the processing is unlawful, or you object to the processing and we are considering your objection.
- **Right to Data Portability:** You have the right to receive your data in a structured, commonly used, and machine-readable format and to request that it be transferred to another data controller where technically feasible.
- **Right to Object:** You may object to the processing of your data for direct marketing or where processing is based on legitimate interests.
- **Right to Withdraw Consent:** Where we rely on your consent to process personal data, you may withdraw that consent at any time. This will not affect the lawfulness of any processing carried out before withdrawal.
- **Right to Lodge a Complaint:** If you believe your data protection rights have been violated, you have the right to complain to the Information Commissioner's Office (ICO): <https://ico.org.uk/for-the-public/>

Where We Store and Process Personal Data

CC33 processes and stores personal data primarily within the United Kingdom, in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Where it is necessary to transfer personal data outside the UK, we ensure that appropriate safeguards are in place to protect such data. These may include the use of:

- UK adequacy decisions (where the destination country has been recognised as providing adequate protection); or
- Standard Contractual Clauses (SCCs) or other lawful transfer mechanisms approved by the Information Commissioner's Office (ICO).

All international transfers are conducted in accordance with applicable legal requirements to ensure your data remains protected and secure.

Incident Handling

CC33 takes the security of personal data seriously. In the event of a personal data breach, we assess the nature, scope, and potential impact of the incident in line with our internal incident response procedures.

Where a reportable breach is likely to result in a risk to the rights and freedoms of individuals, such as financial loss, identity theft, reputational damage, or discrimination, we will report the incident to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it, in accordance with UK GDPR requirements.

Examples of reportable incidents include, but are not limited to:

- Unauthorised disclosure of sensitive or personal data
- Data loss affecting service users or customers
- Breaches leading to identity theft, financial hardship, or exclusion from insurance

Privacy Commitment

At CC33, we are committed to protecting the privacy and security of all personal data we process. We regularly review and update our privacy practices to ensure ongoing compliance with applicable data protection laws, including the UK GDPR and the Data Protection Act 2018.

We value the trust placed in us and are committed to transparency, accountability, and responsiveness in all matters relating to data privacy. If you have any questions, concerns, or requests regarding this privacy notice or how we handle your data, please contact us at privacy@cc33.co.uk.