

Privacy Policy

Circle Cloud Communications Ltd ("circle.cloud", "we", "us", "our")

Effective date: 9 July 2026

At a glance We are a UK business telecoms provider. This policy explains what personal data we hold, why, on what legal basis, who we share it with, how long we keep it, and your rights. If you are a prospective customer wondering how we got your details, see sections 2.2 and 5. To opt out of marketing or exercise any right, see sections 14 and 16.

1. Who we are

Circle Cloud Communications Ltd ("circle.cloud", "we", "us", "our") is registered in England and Wales under company number 09830711, with its registered office at Ariadne House, Town Quay, Southampton, SO14 2AQ. Our website address is <https://circle.cloud>.

Circle Cloud Communications Ltd is the data controller for the personal data described in this policy relating to website visitors, prospective customers, and our customers and their representatives.

Where we provide telecommunications Services, we also process personal data on your behalf and on your instructions, for example call traffic and the details of your own staff and contacts carried over the Services. In that role we act as your processor, not as controller, and that processing is governed by your Contract with us rather than this policy.

We have not appointed a statutory Data Protection Officer. Having assessed our processing, we do not consider that we are required to appoint one; if that position changes, we will appoint one and update this policy. Data protection queries should be directed to the contact details in section 16.

2. The personal data we collect

2.1 Information you give us directly

This includes information you provide when you contact us, request a quote, request a demonstration, complete a form on our website, register an account, leave a comment on our blog, or engage us to provide Services and/or Equipment.

2.2 Information we obtain from other sources when identifying prospective customers

As a business-to-business provider of telecommunications, IT services and technology, we also identify and contact prospective business customers using information we do not collect directly from you:

- Website visitor identification (LeadForensics): we use reverse IP lookup software to identify which organisations have visited our website, based on static IP address information. This tells us the name of a visiting organisation and the pages it has visited. By itself, it does not identify a named individual.
- Identifying a business contact (Clay): once we have identified an organisation that may be interested in our services, we use Clay, a business contact platform, to identify a relevant business contact and a business email address at that organisation, so we can get in touch in a relevant and targeted way.

This means we hold limited personal data about an individual business contact, typically a name, job role, employer and business email address. Our lawful basis for identifying you as a business contact

and for contacting you is our legitimate interests (see sections 3.2 and 5). Where we obtain your details from these sources, we will tell you, and no later than when we first contact you, in line with our transparency obligations.

We do not use these tools to track or profile your personal browsing habits, or to build a picture of your behaviour as an individual. Our reverse IP lookup software identifies the organisation associated with a visit, not you personally.

2.3 Information collected by CCTV

If you visit our premises, we operate CCTV for security purposes, including to protect our premises, staff and visitors, and to prevent and detect crime. Recordings may capture your image.

2.4 Information generated through your use of our Services (customers and Authorised Users)

Where you are a customer, or a representative or Authorised User of a customer, we collect and generate:

- Contract and account information, e.g. contact details and the information in your Order Form and Service Schedule, and billing address;
- Financial information, e.g. billing and payment details, and information used for credit and identity checks (see section 7);
- Call records and call metadata, and recordings of calls relating to sales, service and support (see section 6);
- Configuration and usage data relating to the Services, e.g. traffic logs, access permissions, device or extension counts, and fault reports, which we collect and use, so far as possible, in an aggregated or anonymised form;
- Support and correspondence records, e.g. helpdesk tickets, emails and other communications with our support and account teams.

2.5 Other information

We may also collect information you provide when corresponding with us by email, post, telephone or text, or via social media. Our lawful basis for handling this correspondence is our legitimate interests in responding to you and managing our relationship with you.

3. How we use your information

3.1 Operating and improving our website

We use Statistics cookies (Google Analytics via Google Tag Manager) to understand how our website is used, so we can improve it. IP addresses are anonymised for this purpose. Our lawful basis for this processing is your consent, given via our cookie banner.

3.2 Identifying and contacting prospective business customers

We use the tools described in section 2.2 to identify organisations that may be interested in our services, find a relevant business contact, and send introductory marketing communications about circle.cloud's products and services. Our lawful basis is our legitimate interests (see section 5).

We also use Click Cease, a click-fraud protection service, to identify and filter out fraudulent or automated (bot) activity on our paid online advertising, which may involve processing the IP address and device/browser information of people who click our adverts. Our lawful basis for processing this data to detect and prevent fraud is our legitimate interests. Where Click Cease places a non-essential cookie or similar technology on your device, we do so only with your consent, as described in section 4.

3.3 Sending marketing communications

Where we contact a prospective business customer directly, we send that communication using PlusVibe and/or ZOHO, our email delivery platforms. Every marketing email we send includes a way to opt out of further contact, and we will action any opt-out request promptly.

3.4 Providing Services and Equipment to customers

Where you are a customer, or a representative of a customer, we use your personal data to enter into and perform our Contract with you (or the organisation you represent), including to provision and support Services and Equipment, invoice and collect payment, provide customer support, and manage our ongoing relationship with you. Our lawful basis for this processing is performance of a contract.

3.5 Call recording, monitoring and quality assurance

See section 6.

3.6 Credit and identity checks, financing and leasing arrangements

See section 7.

3.7 Preventing fraud, and complying with our legal obligations

We use personal data as necessary to prevent and detect fraud, to comply with Applicable Laws (including telecommunications, tax and accounting requirements), and to establish, exercise or defend legal claims. Our lawful basis for this processing is compliance with a legal obligation, and, in relation to fraud prevention and legal claims, our legitimate interests.

3.8 Operating CCTV at our premises

We use CCTV to monitor our premises for security purposes, including protecting our staff, visitors and property, and preventing and detecting crime. Our lawful basis for this processing is our legitimate interests in maintaining the security of our premises, staff and visitors.

4. Cookies and similar technologies

We use cookies and similar technologies on our website. Some are essential for the site to work; others help us understand how the site is used. You can manage your cookie preferences at any time using the cookie banner or the Cookie settings link in our website footer.

Cookie category	What it does	Consent required?
Functional	Required for the website to work properly (e.g. remembering your cookie preferences). Cannot be switched off.	No, strictly necessary.
Statistics	We use Google Analytics, delivered through Google Tag Manager, to understand how visitors use our site. IP addresses are anonymised.	Yes, under PECR. Set only if you accept Statistics cookies.
Marketing / Anti-fraud	Where any of our marketing or anti-fraud tools (such as Click Cease) place a non-essential cookie or similar technology on your device, we do so to protect our advertising and understand ad performance.	Yes, under PECR. Set only if you accept these cookies.

Under PECR, we only place non-essential cookies (Statistics and Marketing / Anti-fraud) with your consent.

Separately, our LeadForensics website visitor identification (section 2.2) identifies the visiting organisation from static IP address data. This does not require a cookie on your device and is carried out under our legitimate interests (see section 5), independently of your cookie preferences.

5. Legal basis for direct marketing

Business-to-business marketing emails sent to a corporate email address are generally permitted under PECR without prior consent, provided we identify ourselves, explain how we obtained your details, and give you a simple way to opt out.

For the related processing of personal data (such as a name, job role, employer and business email address), our legal basis is legitimate interests, specifically our interest in promoting our products and services to other businesses. We have carried out a Legitimate Interests Assessment to balance this interest against your rights. You have an unconditional right to object to your data being used for direct marketing at any time, free of charge (see section 14.2).

6. Call recording and monitoring

6.1 We monitor and record calls relating to customer services and sales, as set out in our Terms & Conditions, for training purposes, to improve the quality of our customer service, to help resolve disputes, and to meet our legal and regulatory obligations. Our lawful basis for this processing is our legitimate interests in training, quality assurance and dispute resolution, and, where recording is required by law or contract, compliance with a legal obligation.

6.2 Call recordings may include the voice, and any other personal data disclosed during the call, of both our staff and the individual we are speaking with.

6.3 We retain call recordings for 12 months from the date of the call, save where a recording is needed for longer to resolve an active complaint, dispute or legal claim, or has been requested by the customer.

6.4 If you would prefer not to be recorded on a particular call, please let our representative know at the start of the call. We will try to accommodate this, although some recording (for example, for compliance purposes) may be required by law or contract.

7. Credit checks, finance and leasing arrangements

7.1 Where a customer or prospective customer wishes to obtain Equipment under a rental, lease or finance arrangement, that arrangement is provided under a separate contract with a third-party financier or lessor.

7.2 To assess and process such applications, we and/or our finance partner(s) may carry out credit reference and identity checks, and may share relevant identity, contact and financial information with credit reference agencies and fraud prevention agencies for that purpose.

7.3 Credit reference and fraud prevention agencies will keep a record of any search, whether or not the application proceeds, and this may be seen by other organisations that make searches. If false or inaccurate information is provided and fraud is identified, details may be passed to fraud prevention agencies to prevent fraud and money laundering.

7.4 If you would like more information about how a specific finance partner or credit reference agency uses your data, please contact us using the details in section 16, or refer to that partner's own privacy notice.

7.5 Our lawful basis for this processing is performance of a contract (assessing and administering the finance or lease arrangement) and, in relation to fraud and identity checks, compliance with a legal obligation.

8. Who we share your data with

Depending on the circumstances, we may share your personal data with the recipients below, solely so that they can provide the relevant service to us or on our behalf. We do not sell your personal data to third parties.

Recipient	What they do	Why we share data
LeadForensics	Reverse IP lookup / website visitor identification	To identify prospective business customer organisations (section 2.2)
Clay	Business contact discovery	To find a relevant contact at a prospective customer (section 2.2)
Google Analytics / Google Tag Manager	Website analytics	To understand website usage (section 3.1)
Click Cease	Click-fraud protection	To protect our paid advertising from fraudulent or bot clicks (section 3.2)
ZOHO	Email delivery platform	To send marketing and prospecting emails (section 3.3)
PlusVibe	Email delivery platform	To send marketing and prospecting emails (section 3.3)
Finance providers, lessors and credit reference agencies	Assessing and providing equipment finance	To process finance and leasing applications (section 7)
IT, hosting and software providers	Providing IT infrastructure and software	To deliver the Services, our website and our business systems
Professional advisers (e.g. solicitors, accountants, IT specialists)	Advice and representation	Where we require external advice, or in connection with a complaint or legal claim
Regulators and law enforcement (e.g. the ICO, Ofcom)	Compliance and investigations	Where required or permitted by law
A prospective buyer of our business (and their advisers)	Business continuity	In the event of a merger, acquisition, restructuring or sale of all or part of our business

We only allow our service providers to use personal data to provide services to us, under contracts that require them to protect it and to act only on our instructions.

If you request a password reset on our website, your IP address will be included in the reset email for security purposes.

9. International data transfers

9.1 Some of the third-party service providers named in section 8 (including Google, and other cloud or SaaS-based tools we use to run our website, marketing and business systems) may store or process personal data outside the UK, including in the United States.

9.2 Where we, or our service providers, transfer personal data outside the UK, we ensure that an appropriate safeguard is in place for that specific transfer. Depending on the recipient and destination, this will be one of: reliance on UK adequacy regulations (which currently cover, among

others, the EU/EEA); the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses; or the UK/US Data Bridge for transfers to US organisations certified under the relevant framework.

Please contact us (section 16) if you would like details of the specific safeguard used for a particular transfer.

10. How long we keep your data

10.1 We only keep personal data for as long as necessary for the purposes it was collected, including to meet our contractual, accounting, legal and regulatory obligations.

10.2 As a guide:

- Prospective customer / marketing contact data: retained while we are pursuing a business opportunity, and deleted or anonymised after a period of inactivity of 12 months, or sooner if you object or ask us to stop.
- Customer and contract data: retained for the duration of the Contract and for 7 years afterwards, to meet contractual, accounting and tax obligations and in line with statutory limitation periods.
- Call recordings: retained for 12 months from the date of the call unless needed for longer to resolve an active complaint, dispute or legal claim, or as requested by the customer.
- Website analytics data: retained in accordance with our Google Analytics settings (currently 14 months of User Data).
- CCTV footage: held for 30 days.

10.3 Suppression records (exception to the above): where you opt out of marketing or object to our use of your data, we keep a minimal record of your details on a suppression list for as long as necessary to ensure we continue to honour your request. Keeping this limited record is itself necessary to respect your objection, and it overrides the deletion periods above.

10.4 Registered users can view, edit, or delete their account information at any time.

11. Keeping your data secure

11.1 We maintain appropriate technical and organisational measures designed to protect personal data against unauthorised or unlawful processing, and against accidental loss, destruction or damage. These include access controls and authentication, encryption of data in transit, staff confidentiality obligations and training, and due diligence on our third-party service providers.

11.2 We limit access to personal data to those who have a genuine business need, and anyone processing your data on our behalf does so under a contract that requires them to protect it.

11.3 No transmission of information over the internet can be guaranteed to be completely secure; any transmission is at your own risk.

11.4 We have procedures in place to deal with any suspected personal data breach. Where legally required, we will notify affected individuals and the ICO without undue delay.

12. Children

Our website and Services are intended for business use and are not directed at, or intended for, children. We do not knowingly collect personal data relating to children.

13. Automated decision-making and profiling

We do not make decisions that produce legal effects concerning you, or that similarly significantly affect you, based solely on automated processing.

The tools described in section 2.2 involve limited automated matching, to identify organisations that may be interested in our services and a relevant business contact at those organisations. This may involve associating a business contact with their employer and job role. We do not use this to evaluate your personal characteristics, interests or behaviour, and no decision with a legal or similarly significant effect is made about you as a result of that matching.

14. Your rights

You have the right to: access; rectification; erasure; restriction/objection; portability (where applicable); to object to direct marketing at any time; and to withdraw your consent at any time (for example, in relation to Statistics cookies).

To exercise any of these rights, please contact us using the details in section 16. So that we can handle your request efficiently, please tell us which right you wish to exercise and include enough detail for us to identify your data. We may ask you for proportionate information to confirm your identity before we act.

If you are unhappy with how we have handled your data, you also have the right to complain to the Information Commissioner's Office (ICO). See section 15.

14.1 Making a subject access request

Subject access requests are free. We will normally respond within one calendar month. Where we reasonably need to confirm your identity before we can act, that period runs from the point we receive the information we need to verify you. We may also pause the time limit while we seek clarification of a broad request, as permitted under the Data (Use and Access) Act 2025. In the rare case that a request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or decline to act, and we will explain why. Any identity check will be proportionate.

14.2 Objecting to direct marketing

You can ask us to stop using your data for direct marketing at any time, free of charge, by using the unsubscribe link in any marketing email, by replying to ask us to stop, or by contacting us using the details in section 16.

15. Data protection complaints

Email: info@circle.cloud

Telephone: 0333 043 6600

Postal address: Circle Cloud Communications Ltd, Ariadne House, Town Quay, Southampton, SO14 2AQ

Please include enough information for us to investigate properly. We will acknowledge within 30 days and respond without undue delay. You do not have to complain to us first, but we would welcome the opportunity to put things right.

You also have the right to complain to the Information Commissioner's Office (ICO), which is in the process of being reconstituted as the Information Commission:

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

16. Contact us

Same details as in section 15.

17. Other website features

17.1 Comments

When visitors leave comments on the site, we collect the data shown in the comments form, plus the visitor's IP address and browser user agent string, to help with spam detection. Our lawful basis for this is our legitimate interests in running our blog and preventing spam. An anonymised string created from your email address (a hash) may be shared with the Gravatar service to check whether you use it; Gravatar's own privacy policy applies to that check. Once a comment is approved, your profile picture is publicly visible alongside it.

17.2 Embedded content

Pages on this site may include embedded content (for example, videos or articles) from other websites. Embedded content behaves as if you had visited the other website directly, and that website may collect data about you, use cookies, and monitor your interaction with the embedded content.

18. Changes to this policy

We may update this policy from time to time to reflect changes in our practices or the law. The date at the top of this page shows when it was last revised.