Privacy Policy

Version 2026-11-14-draft - published 2026-11-14

This Privacy Policy explains how [CLIENTOR LEGAL ENTITY], doing business as Clientor.ai and C2R ("Clientor", "we", "us"), collects, uses, shares and protects personal information when you visit clientor.ai or c2r.ai, try our demo, use our ROI calculator, contact us, or use the C2R.ai (Clientor) platform. It also explains the rights you have and how to use them. It replaces our earlier privacy policy.

1. Our two roles

1.1 When we are the controller. We decide how and why personal information is used, and this Policy applies directly, for: visitors to our websites; people who try the demo, use the ROI calculator, book a call or contact us; our customers' account holders and Users (their names, emails, logins, roles, billing contacts and activity in the dashboard); and people we contact about our own products.

1.2 When we are a processor or service provider. Our customers are businesses that use Clientor's AI agents to talk with their own customers, leads and callers ("Contacts"). When an agent answers a call to a business, texts a lead, or drafts an email for a business, we process the Contact's information on behalf of that business and under its instructions, as its processor (GDPR and UK GDPR) and service provider (California and other US state privacy laws). The business decides why that information is collected and how it is used, and its own privacy notice applies. If you are a Contact and want to access, correct or delete information a business holds about you, please contact that business; if you contact us, we will pass your request to the business and help it respond. Section 9 explains how we handle that information on the business's behalf.

2. Information we collect

2.1 Information you give us

- Demo and contact forms: your business website address, name, email address, phone number, company name, preferred call date and time, and anything you write to us.

- Demo choices: the voice and agent name you choose, and the business profile you confirm or correct.

- Your own voice in the demo (optional): if you choose "Use my voice", a short recording of your voice that you make and consent to on the page. We make a temporary copy of it with our voice engine so the demo can play in your voice (and, if you ask, call the number you entered in that voice), and we delete the recording, that copy and the demo clips within 24 hours, unless you keep your demo agent, in which case the voice moves to your workspace's Voice Studio (where you can delete it at any time). Section 6A explains how we handle voice recordings and voice prints.

- ROI calculator: the figures you enter (for example, call volume, handling time and staff cost) and, if you request the report, your name, work email and optional phone number.

- Account and billing: name, business email, phone number, organization name and role, password or single sign-on identity (handled by our authentication provider), billing address, tax identifiers, and payment details (card or bank details are entered directly with our payment processor; we receive only a token, the card brand, last four digits and expiry, or the bank name and last four digits).

- Compliance setup: business verification details, and the information needed for carrier text-message brand and campaign registration (legal business name, EIN or tax ID, business address, website, contact person and sample messages).

- Support and feedback: what you send us, and recordings of support calls where we tell you the call is recorded.

2.2 Information collected automatically

- Device and log data: IP address, browser type, operating system, language, referring page, pages viewed, time and date, and error logs.

- Cookies and similar technologies: see our Cookie Policy (clientor.ai/legal/cookies). Analytics and advertising cookies are used only with your consent where the law requires it.

- Platform usage data: features used, settings changed, credit consumption, performance and error data, and security events such as logins and failed logins.

2.3 Demo calls. When you call the temporary demo number, the call is answered by an AI agent, which tells you at the start that it is an AI and that the call is recorded. We record and transcribe the call and keep the recording, transcript, the calling number, call times and a summary, as described in the Demo Terms & Consent (clientor.ai/legal/demo-terms).

2.4 Business Brain research. When you enter a website in the demo or sign up, we research that business from public sources (its website, its Google Business Profile and reviews through official APIs, its public social pages, news and directories, and what AI assistants say about it) and look at public information about nearby businesses in the same category. This research is about businesses, not people. It may incidentally include personal information that appears publicly on business pages, such as an owner's or staff member's name and business contact details, or the first name and text of a public review. We use such information only to describe the business and set up its agents. We do not build profiles of individuals, we do not collect reviewers' or followers' contact details, and we never use this research to contact anyone other than the business that asked for it.

2.5 Information from others. We may receive information about you from: the business that invited you to its workspace; partner products in which C2R.ai (Clientor) is embedded (LuxAviate, Ezlogz and M8T) when you turn on C2R.ai (Clientor) features there; agencies that resell C2R.ai (Clientor) to you; our authentication, payment and fraud-prevention providers; and, if you sign in with Google or connect another account, the profile information that service shares with your permission.

3. How we use information (and our legal bases)

We use personal information for the purposes below. Where the GDPR or UK GDPR applies, the legal basis is shown in brackets.

- To provide the demo, the website and the platform, including building your business profile and demo agent, reserving a demo number, running test calls, creating and securing accounts, and providing support [contract; legitimate interests in responding to your requests].

- To bill you and manage subscriptions, credits, auto top-ups, receipts, renewal reminders and collections [contract; legal obligation].

- To communicate with you about your account, security, changes to our terms and service notices [contract; legal obligation].

- To follow up on a demo or report request by email, and by phone or text only if you gave the separate consent described in section 4 [consent; legitimate interests for email to business contacts].

- To keep the platform safe and lawful, including fraud and abuse prevention, enforcing our Acceptable Use Policy and Communications & AI Agent Policy, responding to carrier traceback and complaint requests, and keeping consent and acceptance records [legitimate interests; legal obligation].

- To improve the platform using usage data and aggregated or de-identified information, as described in section 6 [legitimate interests].

- To market our products to business contacts by email, with an unsubscribe link in every message [legitimate interests; consent where required].

- To comply with law and to establish, exercise or defend legal claims [legal obligation; legitimate interests].

We do not use personal information for automated decisions that produce legal or similarly significant effects on you.

4. Phone calls and text messages from us

4.1 We call or text you about our own products only if you have given us your phone number and checked the separate, unchecked consent box that explains this, or if you asked us to call you (for example, by booking a call). Giving consent is not a condition of buying anything.

4.2 Our calls may use AI agents and artificial or AI-generated voices; we always say so at the start of the call. Message frequency varies; message and data rates may apply. Reply STOP to any text to stop texts, or HELP for help. You can also tell any agent or employee on a call that you do not want further calls, or email [SUPPORT EMAIL].

4.3 We do not sell, rent or share mobile phone numbers or text-message opt-in data with third parties or affiliates for their own marketing purposes. This applies to every category of third party listed in section 5.

5. How we share information

We share personal information only as follows:

- Service providers (subprocessors) who host, secure and run parts of the platform for us, such as cloud hosting, storage, AI model providers, authentication, email delivery, telephony and text messaging, payments, error monitoring and content delivery. They may use the information only to provide services to us. Our current list is at clientor.ai/legal/subprocessors.

- AI model providers. To generate agent replies, summaries, research and the business profile, we send the relevant text (and for voice, audio or transcripts) to our AI model providers, currently Anthropic. Our contracts prohibit them from using it to train their models.

- Carriers and messaging platforms, as needed to place calls, deliver messages and register text-message brands and campaigns (for example, telephone carriers, The Campaign Registry and Meta for WhatsApp).

- Partner products and agencies. If you use C2R.ai (Clientor) inside a partner product or through an agency, we share with that partner or agency the account and usage information needed to provide and bill the service.

- Your organization. If you are a User of a customer's workspace, the workspace's Owners and Admins can see your activity in it.

- Legal and safety. When we believe in good faith that disclosure is required by law, a subpoena or a carrier traceback request, or is needed to protect the rights, safety or property of anyone, or to investigate fraud or abuse.

- Business transfers. In connection with a merger, acquisition, financing or sale of assets, subject to this Policy's protections.

- With your consent or at your direction.

We do not sell personal information and do not share it for cross-context behavioral advertising, as those terms are defined in California law, except that, if you accept advertising cookies on our marketing websites, the advertising partners described in our Cookie Policy receive cookie and device identifiers. You can refuse or withdraw that consent at any time through "Cookie settings", and we honor Global Privacy Control signals as an opt-out.

6. AI processing, learning and model training

6.1 What AI does with your information. The platform uses AI models to understand what callers and writers say, generate replies, transcribe and summarize calls, extract facts for the business profile and suggest improvements.

6.2 No training of foundation models. We do not use customers' data, call recordings, transcripts, messages or emails, or demo data, to train or fine-tune foundation or general-

purpose AI models, and our AI model providers are contractually prohibited from doing so.

6.3 Each customer's agents learn from that customer's own activity. The platform keeps structured event logs of what each customer's agents do (questions asked, answers that resolved them, outcomes, call timing, escalations). We use these logs only inside that customer's workspace, on the customer's behalf, to improve that customer's own agents: remembering earlier conversations with a Contact, suggesting knowledge-base fixes, proposing prompt changes that are tested before the customer approves them, and picking better times to call. One customer's data is never shown to or used for another customer.

6.4 Platform learning only with opt-in, and only de-identified. If a customer opts in, we derive aggregated, de-identified signals from its event logs (for example, how often a library agent version resolves a type of request, or which AI model handles a step best) and combine them with signals from other opted-in customers to improve our library agents, test sets and model routing. These signals do not identify any customer, user or Contact and do not contain the content of calls, messages or emails. We maintain technical and organizational measures to prevent re-identification, publicly commit not to re-identify such data, and contractually require any recipient to do the same.

6A. Voice recordings and voice prints

6A.1 What we collect. Only when a person chooses to and gives the consent in 6A.3, we collect (a) a short recording of that person reading a script (about 25 seconds), and (b) a voice model derived from it that lets our voice engine speak in a similar voice (a "voice copy"). Some laws treat a recording used this way, or the model made from it, as a voiceprint, biometric identifier or biometric information; we treat both as biometric data. We collect them in two places: the "Use my voice" step of the c2r.ai demo, and Voice Studio in the C2R.ai (Clientor) platform, where workspaces on the Business plan or above may clone the voice of the account owner or of a staff member, made by that person and with that person's own consent. Only a person's own voice may be cloned.

6A.2 Why we use it. Only to play the demo in your voice (short sample clips and, if you ask for it, one demo call to the phone number you entered), and, in the platform, to let that customer's AI agents speak in that voice. We never use voice recordings or voice models to identify or verify anyone, to infer characteristics about anyone, for marketing, or to train general-purpose AI models.

6A.3 Consent (our legal basis). We collect a voice only with the person's explicit written consent, captured before recording starts: an unchecked box stating that it is their own voice, what we make from it, why and for how long, followed by a script whose first sentence is a spoken consent ("This is my own voice, recorded for my demo." in the demo). We keep the consent evidence (the wording and its version, the time, the IP address and browser), not as part of the voice. Where the GDPR or UK GDPR applies, the basis is explicit consent (Article 9(2)(a)). A person may withdraw consent at any time by deleting the voice (6A.6); withdrawal does not affect earlier use.

6A.4 How long we keep it. Demo: the recording, the voice copy and the demo clips are deleted within 24 hours of recording, unless you sign up and keep your demo agent, in which case the voice moves to your workspace's Voice Studio and the platform rule applies. Platform: until the customer deletes the voice, the person withdraws consent or the account is closed, and in any

case no later than 3 years after the voice was last used or the person last interacted with us, whichever comes first. Encrypted backups roll off within 35 days after deletion. The full schedule is in our Biometric Data Retention and Destruction Policy (clientor.ai/legal/biometric-policy).

6A.5 Never sold; shared only with our voice engine. We never sell, lease, trade or otherwise profit from voice recordings or voice models. We disclose them only to the voice-engine subprocessor shown on our subprocessor list (clientor.ai/legal/subprocessors), under a written contract that limits its use to providing the service to us and requires deletion when we delete; where a law, subpoena or court order requires it; or with the person's consent. We protect them with at least the same care as our other confidential and sensitive information (encryption in transit and at rest, restricted access, recordings kept outside our databases).

6A.6 How to delete a voice. In the platform, an Owner or Admin can delete a voice at any time in Voice Studio; the person whose voice it is can also ask us directly. For a demo voice, or any other request, email [PRIVACY EMAIL] or use clientor.ai/legal/data-deletion. We delete the recording and the voice model, including at our voice engine, promptly and in any case within 30 days.

6A.7 Biometric privacy laws. We handle voice data in line with the Illinois Biometric Information Privacy Act (740 ILCS 14), the Texas Capture or Use of Biometric Identifier Act (Tex. Bus. & Com. Code § 503.001), Washington's biometric identifier law (RCW 19.375), and other state laws that treat voiceprints as biometric or sensitive personal information.

7. Retention

We keep personal information only as long as needed for the purposes above, then delete or de-identify it:

- Demo data (website research, profile, contact details, booking, demo call recording and transcript): 90 days after your last demo activity, unless you sign up (in which case your demo agent and profile move into your account) or ask us to delete it sooner. Demo calls that reveal abuse or fraud may be kept until the matter is resolved.

- Voice recordings and voice models: as set out in section 6A.4 (demo: within 24 hours unless kept).

- ROI calculator and contact-form leads: 24 months after our last interaction, unless you become a customer or ask us to delete it sooner.

- Account and User data: for the life of the account, then 30 days for export, then deleted within a further 60 days, except as below.

- Billing, tax and transaction records: 7 years, as tax and accounting laws require.

- Acceptance, consent and opt-out records (ours and the evidence we keep for customers): 5 years after the last communication or the end of the account, whichever is later, because telemarketing and messaging laws require or reward proof of consent.

- Security and audit logs: 12 months, or longer if needed for an investigation.

- Backups: backups roll off within 35 days of deletion from production systems.

- Customer Data we process for businesses: as the business configures and instructs (see the Data Processing Addendum), and deleted after the business's account ends as described in section 9.

8. Your choices and rights

8.1 Everyone. You can unsubscribe from our marketing emails using the link in each email, stop texts by replying STOP, refuse non-essential cookies through "Cookie settings", and ask us for a copy of, correction of, or deletion of your personal information by writing to [PRIVACY EMAIL] or using the form at clientor.ai/legal/data-deletion.

8.2 US state privacy rights. Depending on where you live (including California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah and Virginia), you may have the right to: know and access the personal information we hold about you and how we use and disclose it; correct it; delete it; receive it in a portable format; opt out of its sale, of sharing for cross-context behavioral advertising, and of targeted advertising and profiling for significant decisions; limit the use of sensitive personal information; and not be discriminated against for using these rights. We do not sell personal information or use sensitive personal information to infer characteristics. You can use your rights by emailing [PRIVACY EMAIL] or using the form at clientor.ai/legal/data-deletion. We will verify your request by matching information you provide to what we hold (for example, by confirming your email address). You may use an authorized agent, who must provide your signed permission; we may still ask you to verify your identity. If we deny your request, you may appeal by replying to our decision with "Appeal" in the subject line; we will answer within the time the law allows, and if you are unhappy with the result you may contact your state attorney general.

8.3 California notice at collection. In the past 12 months we have collected these categories of personal information: identifiers (name, email, phone, IP address); customer records (billing details); commercial information (plans and purchases); internet activity (website and platform usage); geolocation approximated from IP address; audio information (demo and support call recordings); biometric information (voice recordings and voice models, only with the consent described in section 6A); professional information (company and role); and inferences limited to your business's needs (for example, which agents to recommend). Sources, purposes, recipients and retention are described in sections 2, 3, 5 and 7. We have not sold or shared personal information except advertising-cookie identifiers where you consented, and we do not knowingly sell or share the information of consumers under 16.

8.4 EU, UK and Swiss rights. If the GDPR or UK GDPR applies, you have the rights of access, rectification, erasure, restriction, data portability and objection (including to direct marketing at any time), and the right to withdraw consent at any time without affecting earlier processing. You may complain to your local data protection authority. Our EU representative and UK representative under Article 27, where required, are: [EU REPRESENTATIVE] and [UK REPRESENTATIVE].

8.5 Timing. We respond within 45 days (US state laws) or one month (GDPR), extendable where the law allows, and tell you if we need more time.

9. Information we process for businesses (Contacts)

9.1 When a business uses C2R.ai (Clientor) to answer calls, send texts, chat or email, we process Contact information (name, number, email, what was said or written, call recordings and transcripts, appointment and CRM details) only on that business's behalf, under our Data Processing Addendum with it. We do not use it for our own marketing, do not sell it, do not use it to train foundation AI models, and do not share it with other customers.

9.2 Agents are required to tell callers at the start of a call that they are speaking with an AI agent and, if the call is recorded, that it is recorded. To stop calls or texts from a business, tell the agent, reply STOP, or contact the business. Opt-outs are applied across all channels that business uses on our platform.

9.3 If you contact us about a business's use of your information, we will forward your request to the business and help it respond. If the business has closed its account, we will act on your request directly where we still hold the information.

10. International transfers

We are based in the United States and process information in the United States and in the other countries where our service providers operate, as shown for each provider on our subprocessor list. When we transfer personal information from the EEA, the UK or Switzerland to countries without an adequacy decision, we use the European Commission's Standard Contractual Clauses, the UK International Data Transfer Addendum, or another lawful transfer mechanism, together with supplementary safeguards.

11. Security

We protect personal information with encryption in transit, encryption of sensitive fields at rest, tenant isolation, access controls, multi-factor authentication for staff, logging and monitoring, and regular backups. More detail is in our Security Overview (clientor.ai/security). No system is perfectly secure; if a breach affects your personal information, we will notify you and the authorities as the law requires.

12. Children

Our websites and platform are for businesses and are not directed to children under 16. We do not knowingly collect personal information from children under 16. Customers may not use C2R.ai (Clientor) agents to communicate with children under 13 or to collect their personal information. If you believe a child has given us personal information, contact [PRIVACY EMAIL] and we will delete it.

13. Changes to this Policy

We may update this Policy. We will post the new version with a new "Last updated" date and, for material changes, notify account holders by email or in the dashboard at least 30 days before the change takes effect, unless the law requires a change sooner.

14. Contact us

[CLIENTOR LEGAL ENTITY], Attn: Privacy, [ADDRESS]. Email: [PRIVACY EMAIL]. Data protection contact: [DPO/CONTACT].