

Communications & AI Agent Policy

Version 2026-10-14-draft - published 2026-10-14

This Policy sets out the rules every customer must follow when C2R.ai (Clientor) agents call, text, message or email people, and the guardrails the platform applies. It forms part of the Terms of Service. You, the customer, are the caller and sender of record for every communication your agents make, and you are responsible for complying with this Policy and the law. The platform's guardrails help you comply; they do not replace your own compliance program or legal advice.

1. Scope and principles

1.1 This Policy applies to every Agent Communication: inbound and outbound voice calls and voicemails, SMS, MMS and RCS messages, WhatsApp and other messaging-app messages, website chat, social direct messages and email.

1.2 Five principles apply to every channel:

- Consent first: contact people only with the consent the law requires for that channel and content, and keep proof.
- Say who you are and that it is AI: every communication identifies your business, and every voice call and conversation tells the person they are dealing with an AI agent.
- Respect time and frequency: contact people only within permitted hours and attempt limits.
- Stop means stop, everywhere: an opt-out on any channel stops further marketing on all channels.
- Records: keep the evidence of consent, disclosures and opt-outs for at least five years.

2. Consent for outbound calls and texts

2.1 Which consent you need. Under the Telephone Consumer Protection Act (TCPA) and the FCC's rules, a call that uses an artificial or prerecorded voice is subject to consent requirements, and the FCC has ruled that AI-generated voices are "artificial" voices. C2R.ai (Clientor) voice agents use AI-generated voices. Therefore:

- Marketing or telemarketing calls and texts (anything that advertises or encourages the purchase of goods or services, including quote follow-ups, promotions, reactivation and upsell calls) require the recipient's prior express written consent before an agent calls or texts a mobile or residential number.
- Informational calls and texts that contain no advertising (for example, confirming an appointment the person booked, a callback the person asked for, or an order update) require at least prior express consent, which a person typically gives by providing their number for that purpose. If an informational call also promotes anything, treat it as marketing.
- Calls to business lines may still be covered by state laws and by the TCPA where the number

is a mobile phone; apply the same consent standard unless you have confirmed otherwise.

2.2 What prior express written consent must look like. It must be a written agreement (an electronic signature or checkbox counts) that: clearly authorizes your business by name to deliver calls and texts using an automated system and artificial or AI-generated voices; identifies the phone number; states that consent is not a condition of purchase; and is obtained before the first call. Do not pre-check the box, bury the wording in terms of service, or make it a condition of any purchase. Each consent should name your business only, not a list of companies.

2.3 Template consent language for your web forms. Clientor provides form templates that include this wording, which you may adapt with your counsel:

> By checking this box, I agree that [Business Name] may call and text me at the number above about [products/services], including with automated technology and AI-generated or prerecorded voices. Consent is not required to buy anything. Message frequency varies. Msg & data rates may apply. Reply STOP to opt out, HELP for help. See our [Privacy Policy] and [Terms].

2.4 Speed-to-lead and form leads. Agents may call a new web-form or ad lead within seconds only if the form displayed compliant consent language and the person checked the consent box. The consent record (form URL, wording, timestamp, IP address, number and checkbox state) must be sent to Clientor with the lead, or captured by a C2R.ai (Clientor) form or widget. Leads from third-party lead generators, purchased lists or lead aggregators may not be called or texted by agents.

2.5 Reactivation and past customers. Agents may contact past customers only if you hold consent that covers the channel and the marketing purpose. An existing business relationship alone is not consent for AI-voice or automated calls or texts.

2.6 Consent records. For every Contact you upload or connect for outbound use, you must supply, or the platform must capture, the consent type, the wording shown, the date and time, the source and the number. Records must be kept for at least five years after the last communication sent in reliance on them. The platform stores consent records with each Contact and blocks outbound contact where none is recorded.

2.7 Reassigned numbers. Before calling or texting a number whose consent is more than 90 days old, you should check it against the FCC's Reassigned Numbers Database; the platform offers this check where available.

3. Do-not-call rules

3.1 National and state lists. Marketing calls and texts must not be made to numbers on the National Do Not Call Registry, or on state do-not-call lists, unless you hold prior express written consent or another exemption applies. You must hold your own subscription to the National Registry for the area codes you call (the platform will ask for your Subscription Account Number before unlocking outbound marketing) and scrub at least every 31 days. The platform scrubs outbound marketing contacts against the lists it has access to before each campaign and at least every 31 days.

3.2 Internal do-not-call list. You must keep an internal do-not-call list, honor requests not

to be called, and have a written do-not-call policy available on demand. The platform maintains an organization-wide internal do-not-call list automatically, adds every opt-out from every channel to it, and checks it before every outbound call or message.

3.3 Training. Everyone in your organization who configures outbound agents must know these rules.

4. Calling hours, frequency and attempt limits

4.1 Hours. Outbound calls and texts must be made only within the permitted hours in the recipient's local time. Federal law permits telemarketing calls between 8:00 a.m. and 9:00 p.m.; several states set narrower windows (for example, Florida, Oklahoma and Maryland allow telephone solicitations only between 8:00 a.m. and 8:00 p.m.), and some states restrict calls on Sundays and legal holidays.

4.2 Platform default window. The platform's default outbound window for marketing calls and texts is 9:00 a.m. to 8:00 p.m., Monday to Saturday, in the recipient's local time, with no marketing calls on Sundays or US federal holidays. Informational calls and texts the person requested (for example, a callback at a time they chose, or an appointment reminder) may be sent between 8:00 a.m. and 9:00 p.m. local time. You may narrow these windows but not widen them. The recipient's time zone is determined from their known address, or else from the area code; where these differ, the platform uses the more restrictive window.

4.3 Attempt limits. The platform's defaults are: no more than 3 call attempts to the same person on the same subject in any 24-hour period, across all your numbers; no more than 2 unanswered marketing call attempts per week after the first week; and sequences stop automatically when the person replies, books, opts out or reaches the sequence's attempt limit. You may tighten these limits but not loosen them for marketing contacts.

4.4 Voicemail. Voicemails left by an AI agent are artificial-voice messages and need the same consent as the call. Voicemails must state your business name, the reason for the call, a callback number, and how to opt out.

5. Caller identification

5.1 Every outbound call must display a valid caller ID number that you are authorized to use, that the platform has assigned to you or verified, and that a person can call back during business hours to reach your business or opt out. Caller ID may not be spoofed or blocked.

5.2 The platform signs outbound calls under STIR/SHAKEN through our telephony provider and supports branded caller ID (CNAM) where available. Numbers are registered to your verified business.

5.3 Local-presence numbers are allowed only where you have a genuine business reason and the number can receive calls; number rotation to evade blocking or spam labels is prohibited.

6. AI disclosure

6.1 At the start of every call. Every Clientor voice agent states, in its first sentence, your business name, that it is an AI agent (for example, "an AI assistant for [Business Name]") and,

for outbound calls, the purpose of the call. This disclosure is on by default for inbound and outbound calls and cannot be removed.

6.2 In messaging and chat. Website chat widgets show a visible "AI assistant" label, and the first text or messaging-app message in a new conversation identifies your business and that replies come from an automated assistant.

6.3 If asked. An agent asked whether it is a human or an AI must always answer truthfully that it is an AI. Agents must never claim to be human.

6.4 Why. This approach satisfies or exceeds the disclosure rules that apply in many places, including California's bot disclosure law (Business and Professions Code § 17940 and following), the Utah Artificial Intelligence Policy Act, Maine's chatbot disclosure law, Texas's disclosure rules for healthcare uses of AI, the EU AI Act's transparency obligations, and proposed FCC rules for AI-generated calls.

6.5 Hand-off to a human. Agents must offer a way to reach a human (transfer, callback or message) when a Contact asks, and you must staff that path.

7. Recording and transcription

7.1 Several US states (including California, Delaware, Florida, Illinois, Maryland, Massachusetts, Montana, Nevada, New Hampshire, Pennsylvania and Washington) require the consent of every party before a call is recorded, and courts have applied wiretapping and eavesdropping laws to AI transcription and analysis of calls. Because the location of a caller cannot always be known, the platform plays a recording disclosure at the start of every recorded call, whatever the location.

7.2 The default opening covers both disclosures, for example: "Hi, this is Ava, an AI assistant for [Business Name]. This call is recorded and transcribed so we can help you." For outbound calls, the agent waits for the person to continue; if the person objects to recording, the agent stops recording (or offers to end the call and arrange a callback from a person) and records the objection.

7.3 You must not disable the recording disclosure while recording is on. If you turn recording off for an agent, the platform does not store audio, but transcripts may still be created for the call log and must be disclosed in the same way.

7.4 Recordings and transcripts are kept for the period you choose (default 12 months) and are used only to provide the Service to you; they are never used to train AI models.

8. Opt-out on every channel

8.1 Recognized opt-outs. The platform treats any of these as an opt-out request: replies such as STOP, STOP ALL, UNSUBSCRIBE, END, QUIT, CANCEL, REVOKE, OPT OUT or similar words (in any language the agent supports); a spoken request on a call ("don't call me again", "take me off your list"); an email unsubscribe; and any other reasonable request in any channel.

8.2 Effect. An opt-out is applied immediately: the Contact is added to the internal do-not-call list, every pending call, text and email in every sequence for that Contact is cancelled, and

no further marketing communications are sent in any channel. One confirmation text ("You're unsubscribed from [Business Name] messages. No more messages will be sent. Reply HELP for help.") may be sent within five minutes of a text opt-out, with no marketing content. Informational messages the person still needs may continue only if the person asked to keep them and the law allows it.

8.3 Speed. The platform honors opt-outs immediately, which is faster than the legal maximums (for example, 10 business days under the FCC's rules and the CAN-SPAM Act, and 15 days under Florida's statute after a STOP reply).

8.4 HELP. Replies of HELP or INFO receive your business name, a support contact and opt-out instructions.

8.5 Re-subscription. A Contact who opted out may be contacted again only if they opt back in, for example by texting START or re-submitting a consent form.

9. Text messaging (SMS, MMS, RCS)

9.1 Registration. US carriers require every business sending application-to-person text messages from standard local numbers to register its brand and each messaging campaign with The Campaign Registry (A2P 10DLC). Unregistered traffic is blocked. Toll-free numbers require toll-free verification. The platform collects the registration details during onboarding and submits them through our messaging provider; texting stays locked until registration is approved.

9.2 Content rules. Messages must identify your business, match the use case you registered, and comply with the CTIA Messaging Principles and Best Practices and carrier codes of conduct. Prohibited content includes the categories listed in the Acceptable Use Policy. Public URL shorteners are not allowed; the platform uses a branded link domain.

9.3 Opt-in for texts. The opt-in must disclose your business name, the type of messages, that message frequency varies (or the frequency), that message and data rates may apply, and how to get help and opt out, and must link to your terms and privacy policy. Your privacy policy must state that you do not share mobile numbers or text opt-in data with third parties for marketing.

9.4 First message. The first message after opt-in must confirm the program, frequency, rates, HELP and STOP instructions.

9.5 Quiet hours for texts. Marketing texts follow the hours in section 4. Even with consent, the platform does not send marketing texts outside 8:00 a.m. to 9:00 p.m. recipient local time.

10. WhatsApp and other messaging apps

10.1 WhatsApp messages are sent through the WhatsApp Business Platform and must comply with Meta's WhatsApp Business Messaging Policy and Commerce Policy.

10.2 You must obtain opt-in before sending a WhatsApp message to a person, stating that they will receive messages from your business on WhatsApp. Messages sent outside the 24-hour window after the person's last message must use an approved message template. Honor every request to stop messages, and do not send content in categories Meta prohibits.

10.3 Other messaging and social channels (for example, Instagram or Facebook direct messages) must follow the platform owner's messaging rules, including limits on when businesses may message people first.

11. Email

11.1 Commercial emails sent by agents must comply with the CAN-SPAM Act and other applicable laws. Every commercial email must: use accurate "From", "To", "Reply-To" and routing information that identifies your business; use a subject line that is not misleading; identify itself as an advertisement where required; include your valid physical postal address; and include a clear, working unsubscribe mechanism that works for at least 30 days after sending. Unsubscribe requests are honored immediately by the platform.

11.2 For bulk sending, the platform sets up SPF, DKIM and DMARC for your sending domain, supports one-click unsubscribe headers, keeps suppression lists and monitors complaint rates, as major mailbox providers require. Bulk email stays locked until your domain is authenticated.

11.3 Recipients in Canada, the EU and the UK may require opt-in consent for marketing email; do not send marketing email to them without it.

12. Inbound calls and messages

12.1 Inbound answering does not need outbound consent, but the AI and recording disclosures in sections 6 and 7 still apply.

12.2 If an inbound caller asks to be called back or texted, that request is consent only for that callback or text and the related informational follow-up, not for marketing.

12.3 Missed-call text-back sends one informational text replying to the missed call; it must not contain marketing unless the caller has given prior express written consent.

13. Platform guardrails

The platform provides these controls. They are on by default and you may make them stricter:

- Outbound lock: outbound calls, outbound texts and bulk email are disabled for a new organization. An Owner unlocks them only after completing the outbound compliance checklist: business verification; confirming the consent sources for the contacts to be called; National Do Not Call Registry subscription details; caller ID registration; A2P 10DLC registration (for texts); domain authentication (for email); and accepting this Policy again for outbound use. Each unlock is recorded.
- Consent gate: an agent cannot place an outbound call or send an outbound text to a Contact without a consent record matching the channel and purpose.
- Do-not-call scrubbing against national, state where available, and internal lists.
- Calling windows and attempt limits as in section 4.

- Automatic disclosures at the start of every call and conversation.
- Answering-machine detection with compliant voicemail messages.
- Opt-out handling across all channels as in section 8.
- Content checks that flag prohibited content and unregistered use cases before sending.
- Logs: every attempt, consent, disclosure, opt-out and outcome is logged on the Contact timeline.

14. Your responsibility; our enforcement

14.1 You remain responsible for your communications even when the platform's guardrails are on. Guardrails depend on the accuracy of the consent data and settings you supply.

14.2 We may pause outbound channels, require changes or suspend accounts as described in the Acceptable Use Policy, including on a carrier complaint, a traceback request, a high opt-out or complaint rate, or evidence of missing consent.

14.3 Before turning on outbound calling for consumer contacts, we recommend that you have your own counsel review your consent language and practices.