Messaging Compliance Policy

Purpose

This policy outlines the requirements for sending SMS messages via VoIPcloud to recipients in North America. It applies to all Application-to-Person (A2P) messaging, regardless of the phone number type used (e.g., long code, toll-free), and must be followed by all VoIPcloud customers using our messaging services.

Messaging guidelines

All messages sent to and within North America via VoIPcloud must comply with the rules and requirements set out below, including:

- Consent (opt-in)
- Revocation of consent (opt-out)
- Sender identification
- Permitted use and prohibited content
- Filtering evasion
- Enforcement measures

1.0 Consent (opt-In)

What constitutes valid consent?

Consent must be obtained directly from the individual and cannot be bought, sold, or transferred (e.g., purchasing a contact list does not qualify).

Before sending your first message:

- You must clearly explain the type of messages the individual is agreeing to receive.
- Consent must be documented (e.g., a signed form, timestamped opt-in online).
- If you delay your first message, you must reconfirm consent when you eventually send it.
- Consent is specific to the campaign, brand, or purpose for which it was collected—it doesn't extend to other campaigns or businesses.
- Proof of consent should be retained in accordance with local regulations, even after the individual opts out.

Alternative consent scenarios

Consent may also be valid in the following situations:

1. **Contact initiated by the recipient**
   If an individual contacts you first (e.g., asking for business hours), you may respond to their message. However, unless further consent is obtained, you may not send additional messages unrelated to that inquiry.
2. **Informational messages based on a prior relationship**
   You may send one-time, informational messages (e.g., appointment reminders, receipts, OTPs, delivery updates) if:
   - The recipient provided their phone number to you,
   - Took an action that triggered the communication (e.g., booking, placing an order), and
   - Has not opted out or expressed preference not receive messages from you.

These messages must not promote products, encourage purchases, or support advocacy causes.

2.0 Ongoing messaging and opt-out

If you're sending messages regularly:

- Include a reminder on how to unsubscribe using standard opt-out language.
- Respect recipient preferences regarding message frequency.

- Periodically reconfirm consent based on local guidelines.

Opt-out requirements

Your first message must include standard opt-out instructions, such as:

"**Reply STOP to unsubscribe**"

Other accepted keywords include: STOPALL, UNSUBSCRIBE, CANCEL, END, QUIT.

If a recipient opts out:

- You may send one final confirmation message.
- No further messages may be sent unless they opt in again.

3.0 Sender identification

You must clearly identify yourself (the party that collected the opt-in) in each message, except in direct replies during an ongoing conversation.

4.0 Usage limitations

Certain types of content are strictly prohibited on VoIPcloud's messaging platform, regardless of consent:

- Illegal content under local, state, or federal laws.
- Cannabis or CBD-related messaging (prohibited in the U.S. due to federal laws).
- Prescription medication offers that can't be legally sold over-the-counter.
- Hate speech, harassment, or exploitation.
- Fraudulent or malicious messages, including malware and phishing attempts.
- Content designed to evade spam detection filters.

Country-specific rules

You are responsible for reviewing and complying with all local regulations for each recipient's country.

Age and geographic gating

For content related to alcohol, tobacco, gambling, firearms, or adult material:

- You must verify the recipient is above the legal age in their location.
- You must comply with all jurisdiction-specific laws and industry standards.
- You must have processes in place to demonstrate compliance.

5.0 Filtering evasion

Customers must not use tactics that intentionally bypass spam or fraud detection systems. This includes:

- **Misspelling or obfuscating words** to avoid detection.
- **Non-standard opt-out phrases** that prevent recipients from unsubscribing.
- "**Snowshoeing**" – spreading messages across multiple numbers to mask volume.
- **Simulated social engineering** – using phishing-like messages for testing.

VoIPcloud actively monitors messaging patterns and may review message content (in accordance with our Privacy Policy) to detect violations.

6.0 Enforcement and violations

VoIPcloud is committed to maintaining a trusted messaging environment. If we detect a violation:

- We will attempt to work with you to bring your messaging into compliance.
- In serious cases or continued violations, we may suspend or terminate access to some or all VoIPcloud services—potentially without prior notice.

Violations include non-compliance with:

- This Messaging Policy
- Local, state, or federal laws
- Industry guidelines or best practices
- VoIPcloud's Fair Use Policy