Octtopus AI Agency Privacy Policy

Introduction

This Privacy Policy explains how **octtopus AI Agency** ("we", "us" or "our") collects, uses, stores and safeguards personal information when providing autonomous voice and chat agents. Our agency is based in Miami, Florida, USA, and we follow the U.S. Federal Trade Commission's guidance on transparent data practices and security. We also comply with sector-specific statutes, such as the Telephone Consumer Protection Act (TCPA), the Children's Online Privacy Protection Act (COPPA), the Illinois Biometric Information Privacy Act (BIPA) and state privacy laws including the California Consumer Privacy Act (CCPA/CPRA), as applicable. This document is intended to be clear and concise, and to reassure clients that we take privacy seriously.

This policy applies to our voice AI agent, chat AI agent and full automation suite, all of which process communications (calls, text messages, social messages and web chats) to capture, qualify and nurture leads, schedule appointments and integrate with your customer relationship management (CRM) system. We do not sell or share personal data with third parties, and data is stored on secure servers accessible only to the client and us.

---

1. Information We Collect

We collect information directly from users and automatically through our services. Personal information means any information that can identify an individual, such as a name or phone number. We limit collection to what is necessary to provide our services.

1.1. Personal information provided by clients or callers

- **Contact details and lead information** – name, phone number, email address, job title, company and other information voluntarily provided when interacting with our agents.
- **Appointment or service details** – dates, times, notes or preferences required to schedule appointments and coordinate with the client's calendar.
- **Client account information** – billing and subscription data, user credentials and preferences for those who register accounts on our platform.

1.2. Communication data and logs

- **Call recordings and chat transcripts** – our voice AI agent records calls (where legally permitted) and our chat AI agent stores conversation text to deliver responses, qualify leads and schedule appointments. We disclose that we record and process these communications for service and quality purposes.
- **Metadata** – date and time of interactions, duration, phone numbers dialed, channel used (e.g., WhatsApp, SMS, web) and other technical details necessary to route and manage communications.

1.3. Automatically collected information

We do not collect or store device-level identifiers such as IP addresses, browser types, operating system details or other usage logs.
We may collect **aggregate or anonymized analytics** (for example, the total number of calls handled) solely to understand service performance. These analytics do not contain personal or device-specific information.

---

2. How We Use the Information

We use personal information only when we have a legitimate reason to do so and limit use to the purposes below:

- **Providing and improving our services** – to answer calls and messages, qualify leads, schedule appointments and route inquiries appropriately. Conversations may be used to improve our AI models and analytics, but we collect the minimum data necessary and purge it quickly.
- **Customer support and training** – call recordings and chat transcripts help us train AI models, investigate issues and improve response quality. We purge recordings within 30–60 days unless required by law or contract.
- **Compliance with laws** – including the FTC Act, TCPA, COPPA, BIPA and state privacy laws such as CCPA/CPRA.
- **Auditing and security** – to monitor for unauthorized access, maintain backups, enforce security policies and conduct periodic audits.

We do **not** sell, rent or share personal information for marketing purposes.
We may use aggregated and anonymized data for analytics and benchmarking.

---

3. Legal Basis and Consent

We operate under a patchwork of U.S. laws since there is currently no comprehensive federal AI law. We therefore rely on the following legal bases:

- **Performance of a contract** – to fulfill obligations such as processing communications, qualifying leads, scheduling appointments and integrating with client systems.
- **Legitimate interests** – improving our services, ensuring security and preventing fraud, provided these interests do not override individual privacy rights.
- **Legal obligations** – complying with statutes, regulatory requirements or lawful requests.

We do not knowingly collect information from children under 13 and will delete any such data if we discover it.

---

4. Data Sharing and Disclosure

We respect the confidentiality of personal information. We do not sell, rent or share personal data with third parties. Access to client data is restricted to authorized employees or contractors who need it for business purposes.
We may disclose information only:

- To the client who owns the data.
- To comply with legal obligations such as subpoenas or regulatory requests.
- In connection with a merger, sale or corporate reorganization.

We do not share data for targeted advertising or any unrelated commercial purpose.

---

5. Data Security

We use commercially reasonable administrative, technical and physical measures to safeguard personal information. These include:

- Encryption of communications and stored data
- Access controls and two-factor authentication
- Periodic security audits
- Monitoring for unauthorized access

While we strive to protect data, no method of transmission or storage is 100% secure.

---

6. Data Retention and Deletion

We retain personal information only for as long as necessary to provide services or as required by law.

- **Voice recordings and chat transcripts:** typically retained for **30–60 days**, then deleted automatically.
- **Client accounts and operational logs:** may be retained longer for legal or contractual reasons.

Individuals may request deletion of their personal information, subject to legal exceptions.
When information is no longer needed, we securely delete or anonymize it.

---

7. Biometric and Voice Data

Our services may capture audio and convert it to text for lead qualification and scheduling.
We do **not** create or store voiceprint templates by default.

If a client requires voiceprint-based features, we will:

- Obtain written consent before capturing or analyzing voiceprints
- Publish a retention schedule and deletion procedures
- Prohibit the sale or monetization of biometric data

---

8. State-Specific Rights (California and Others)

Residents of states with privacy laws may exercise:

- **Right to know**
- **Right to delete**
- **Right to opt-out of sale or sharing**
- **Right to correct**
- **Right to limit use of sensitive personal information**

- **Right to non-discrimination**

To exercise these rights, individuals may contact us using the details in Section 10.

---

9. Children's Privacy

Our services are not directed to children under 13.
We do not knowingly collect children's data.
If we become aware that a child has provided information, we will delete it immediately.

---

10. Contact Us

If you have questions or requests related to this Privacy Policy, please contact us:

- **Email:** [Insert contact email]
- **Address:** Miami, Florida, USA (contact us for full mailing address)
- **Phone:** [Insert contact phone number]

---

11. Changes to This Policy

We may update this Privacy Policy to reflect changes to our practices, services or legal obligations.
When we make material changes, we will post the updated policy and indicate the latest revision date.
Continued use of our services after updates constitutes acceptance of the revised policy.

---

12. Effective Date

This policy is effective as of **November 11th, 2025,** and supersedes any prior versions.