VOICE OFFICE
PRIVACY POLICY

Effective Date: January 28, 2026

Last Updated: February 11, 2026

1. Introduction and Scope

This Privacy Policy ("Policy") describes how **Voice Office** ("Voice Office," "we," "us," or "our") collects, uses, retains, discloses, and protects personal information in connection with: (i) our proprietary AI-driven voice agent technology used to automate telephonic interactions, appointment scheduling, and customer communications (the "Voice Agent"); (ii) our subscriber dashboard, API integrations, and software applications (the "Platform"); and (iii) our website at voiceoffice.ca and associated domains (the "Site"). Together, these are referred to as the "Services."

Voice Office is headquartered in Milton, Ontario, Canada. We provide AI voice agent services to businesses across North America, including the healthcare, restaurant, retail, and professional services industries.

Your use of our Services is subject to this Policy and our Terms of Service. If you do not agree with the practices described herein, please discontinue use of the Services.

2. Key Definitions

The following definitions apply throughout this Policy:

- **"Subscriber"** means any business, healthcare provider, or organization that contracts with Voice Office to use the Voice Agent and Platform.
- **"Caller"** means any individual who interacts with a Voice Agent by telephone, SMS, or other communication channel (e.g., a patient booking an appointment or a customer placing an order).
- **"Personal Information"** means any information that identifies, relates to, describes, or could reasonably be linked—directly or indirectly—to an identifiable individual or household, as defined under applicable law.
- **"Protected Health Information (PHI)"** means individually identifiable health information as defined under the Health Insurance Portability and Accountability Act (HIPAA) or personal health information as defined under Ontario's Personal Health Information Protection Act, 2004 (PHIPA) and equivalent provincial legislation.
- **"Data Controller"** (or "Controller") means the entity that determines the purposes and means of processing Personal Information.

- **“Data Processor”** (or “Processor” / “Service Provider”) means the entity that processes Personal Information on behalf of the Data Controller.
- **“Sub-processor”** means a third-party vendor engaged by Voice Office to assist in the processing of Personal Information on behalf of a Subscriber.
- **“Services”** means the Voice Agent, Platform, and Site, collectively.

3. Roles and Responsibilities

3.1 Voice Office as Data Processor

When processing Caller data on behalf of Subscribers, Voice Office acts as a Data Processor (or “Service Provider” under applicable U.S. state privacy laws, or “Agent” under PHIPA). We process Caller data solely in accordance with the Subscriber’s documented instructions and our contractual obligations. We do not determine the purposes for which Caller data is processed.

3.2 Voice Office as Data Controller

Voice Office acts as a Data Controller with respect to: (a) data collected directly from Subscribers for account administration, billing, and relationship management; (b) data collected from visitors to the Site; and (c) data collected from individuals who communicate with Voice Office directly (e.g., sales inquiries, support requests).

3.3 Subscribers as Data Controllers

Subscribers are the Data Controllers of the Caller data collected through their Voice Agent. The Subscriber retains ownership of this data and bears primary responsibility for: (a) determining the purposes of processing; (b) ensuring a lawful basis exists for the collection and processing of Caller data; (c) providing appropriate notices and obtaining necessary consents from Callers (including call recording disclosures required by applicable wiretapping and privacy laws); and (d) responding to data subject rights requests from their Callers.

3.4 Callers as Data Subjects

If you are a Caller, your data is collected and processed on behalf of the Subscriber (the business you contacted). For questions about how your data is used, or to exercise your privacy rights regarding call data, please contact the Subscriber directly. Voice Office will assist the Subscriber in fulfilling verified data subject requests upon instruction.

4. Personal Information We Collect

4.1 Categories of Personal Information

We collect the following categories of Personal Information in connection with the Services:

- **Identity and Contact Data:** Names, aliases, postal addresses, email addresses, phone numbers, unique personal identifiers, and account credentials.

- **Health and Sensitive Data:** For healthcare Subscribers, we may process PHI such as appointment details, insurance information, medical queries, and related health information disclosed by Callers during interactions with the Voice Agent.
- **Audio and Communication Data:** Call recordings, transcriptions, and SMS message content generated through the Voice Agent. Voice Office does not create or store voiceprints or other biometric identifiers from caller audio.
- **Commercial and Transactional Data:** Subscription details, billing records, service usage history, and purchasing information.
- **Technical and Telemetry Data:** IP addresses, browser type and version, device identifiers, operating system, referring URLs, interaction logs, and session data.
- **Inference Data:** Profiles generated by the AI reflecting user preferences and interaction patterns for the purpose of improving the Subscriber's specific Voice Agent performance.

4.2 Exclusions

This Policy does not apply to: (a) information that is publicly available from government records; or (b) data that has been permanently de-identified or aggregated such that it cannot reasonably be used to identify a specific individual.

5. How We Collect Personal Information

5.1 Data Provided by Subscribers

- **Account Setup:** Business name, authorized representative contact details, and billing information required to establish a Voice Office account.
- **AI Configuration Materials:** Internal documents, scripts, FAQs, and knowledge bases provided by Subscribers to configure and train their specific Voice Agent instance.
- **System Integrations:** Where a Subscriber connects Voice Office to third-party systems (such as Electronic Medical Records, CRMs, or calendaring tools), we access those systems solely to perform the actions requested by the Subscriber (e.g., checking appointment availability).
- **Marketing Preferences:** Subscribers may opt in to receive product updates and promotional communications. Marketing preferences may be managed at any time. Transactional communications (e.g., billing alerts, security notices) are not subject to opt-out.

5.2 Data Collected from Callers (on Behalf of Subscribers)

When a Caller interacts with a Voice Agent, we collect data in real time to facilitate the conversation:

- **Voice Interactions:** We capture the audio of the call and generate a real-time transcription to enable the AI to process and respond to the Caller's request. This includes any Personal Information the Caller verbally discloses during the conversation.

- **Call Metadata:** We log the incoming phone number (Caller ID), date and time of the call, call duration, and call disposition.
- **SMS and Text Communications:** Where the Subscriber has enabled SMS capabilities, the Voice Agent may send automated text messages to the Caller (e.g., appointment confirmation links) based on the context of the call and the Subscriber's configuration.

Important: Caller audio is transmitted to and processed by Voice Office and our technology partners in real time. This processing is necessary for the Voice Agent to function. The Subscriber is responsible for ensuring that appropriate call recording notices are provided to Callers in compliance with applicable laws.

5.3 Data Collected Automatically (Site and Platform)

We use cookies, pixels, and server logs to collect technical data from visitors to voiceoffice.ca and users of the Platform:

- **Strictly Necessary Cookies:** Required for the operation of the Site and Platform (e.g., session management, authentication).
- **Analytics Cookies:** Used to understand traffic patterns, usage trends, and platform performance.
- **Advertising Cookies:** We may use anonymized or hashed identifiers to measure the performance of our marketing campaigns on third-party advertising platforms. You may adjust your browser or device settings to reject non-essential cookies, though this may impact Site functionality.

Do Not Track / Global Privacy Control: Where required by applicable law, Voice Office honors opt-out preference signals, including Global Privacy Control (GPC). If your browser transmits a GPC signal, we will treat it as a valid opt-out request for the sale or sharing of Personal Information as defined under applicable state privacy laws.

6. Lawful Bases for Processing

Voice Office processes Personal Information on the following lawful bases, as applicable under PIPEDA, PHIPA, and U.S. state privacy laws:

- **Contractual Necessity:** Processing that is necessary to perform our contractual obligations to Subscribers (e.g., providing the Voice Agent service, processing payments, maintaining accounts).
- **Consent:** Where required by law, we rely on consent obtained by the Subscriber from the Caller (e.g., consent for call recording, processing of health information). For direct marketing communications, we rely on opt-in consent.
- **Legal Obligation:** Processing that is necessary to comply with applicable laws, regulations, or valid legal process (e.g., tax recordkeeping, responding to lawful subpoenas).
- **Legitimate Interest:** Processing that is necessary for our legitimate business interests, where those interests are not overridden by the data subject's rights (e.g., fraud

prevention, network security, product improvement using aggregated and de-identified data).

7. How We Use Personal Information

We use the Personal Information we collect for the following purposes:

- **Service Delivery:** To operate the Voice Agent, process and respond to Caller requests, schedule appointments, and perform actions directed by Subscribers.
- **Subscriber-Specific AI Improvement:** To train and improve the specific Voice Agent instance configured for each Subscriber. Caller audio and transcription data is used solely for the benefit of the Subscriber whose Voice Agent handled the interaction. Voice Office does not use Caller data to train or improve general-purpose AI models.
- **Account Administration:** To manage Subscriber accounts, process billing, and provide customer support.
- **Platform Operations:** To maintain, monitor, and improve the performance, security, and reliability of the Services.
- **Communications:** To send transactional notices (e.g., billing, security alerts) and, where opted in, marketing communications.
- **Compliance and Legal:** To comply with applicable laws, enforce our Terms of Service, and protect the rights, safety, and property of Voice Office, our Subscribers, and others.
- **Analytics:** To generate aggregated, de-identified insights about Service usage for internal business intelligence purposes.

8. AI and Automated Processing Transparency

Voice Office's core service relies on artificial intelligence to process and respond to voice communications. We believe in transparency about how our technology works:

8.1 Third-Party AI Providers

Voice Office uses a combination of proprietary technology and third-party AI service providers to power the Voice Agent, including for speech recognition, natural language processing, and text-to-speech capabilities. These third-party providers process Caller audio and text data solely to provide their services to Voice Office and are contractually prohibited from using this data for their own purposes. All third-party AI providers engaged by Voice Office maintain industry-standard security certifications (including SOC 2 and HIPAA compliance where applicable).

8.2 Automated Decision-Making

The Voice Agent makes real-time automated decisions during calls, such as determining the appropriate response to a Caller's request, routing calls, or scheduling appointments. These decisions are based on the Subscriber's configuration and training data. The Voice Agent does not make decisions that produce legal effects or similarly significant effects on Callers without

human involvement. If a Caller's request cannot be adequately handled by the Voice Agent, the call is escalated to the Subscriber's staff.

8.3 No General Model Training

Voice Office does not use Caller audio recordings, transcriptions, or interaction data to train or improve general-purpose AI models. Data is used exclusively to improve the specific Voice Agent instance configured for the Subscriber whose system handled the interaction.

9. Healthcare Data Compliance

Voice Office is designed to serve the healthcare sector and acknowledges the heightened legal and ethical obligations associated with health data.

9.1 HIPAA Compliance (United States)

For U.S. healthcare Subscribers, Voice Office operates as a "Business Associate" as defined under HIPAA. We execute Business Associate Agreements (BAAs) with applicable Subscribers and comply with the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule. We process PHI solely to perform services on behalf of the Subscriber and do not use PHI for marketing or any purpose unrelated to the Subscriber's engagement.

9.2 PHIPA Compliance (Ontario) and Provincial Health Privacy Laws (Canada)

For Canadian healthcare Subscribers, Voice Office operates as an "Agent" of the Health Information Custodian (the Subscriber) as defined under Ontario's *Personal Health Information Protection Act, 2004* (PHIPA). We also comply with applicable provincial health privacy legislation in other provinces (e.g., Alberta's *Health Information Act*). As an Agent, Voice Office:

- Processes personal health information solely for the purposes authorized by the Health Information Custodian;
- Does not use personal health information for any unauthorized purpose;
- Implements reasonable safeguards to protect personal health information against theft, loss, and unauthorized access; and
- Notifies the Subscriber of any breach or suspected breach of personal health information.

9.3 PIPEDA Compliance (Canada — Federal)

Voice Office complies with the *Personal Information Protection and Electronic Documents Act* (PIPEDA) with respect to the collection, use, and disclosure of personal information in the course of commercial activities. Where provincial privacy legislation is deemed substantially similar to PIPEDA (e.g., Alberta's PIPA, British Columbia's PIPA, Québec's Law 25), we comply with the applicable provincial legislation.

9.4 Scope of Health Data Processing

We process health data solely to fulfill the appointment scheduling, communication, and administrative needs specified by the Subscriber. We do not mine, analyze, or monetize PHI or personal health information for advertising, research, or any purpose outside the scope of the Subscriber's instructions.

10. Audio Recording and Transcription

- **Purpose:** Calls are recorded and transcribed to enable real-time AI processing, provide the Subscriber with an accurate record of the interaction, and facilitate quality assurance and Subscriber-specific AI model improvement.
- **Consent and Legal Notices:** The Subscriber is solely responsible for configuring their Voice Agent to provide legally required disclosures to Callers (e.g., "This call may be recorded") in compliance with all applicable federal, state, and provincial wiretapping, eavesdropping, and electronic surveillance laws. Voice Office provides Subscribers with configurable disclosure settings but does not independently verify Subscriber compliance.
- **Ownership:** Call recordings and transcripts are the property of the Subscriber. Voice Office retains this data as a Processor on behalf of the Subscriber, subject to the retention periods described in Section 13.
- **No Biometric Identifiers:** Voice Office does not derive, create, or store voiceprints, voice signatures, or other biometric identifiers from Caller audio. Audio is used solely for transcription, real-time AI response generation, and quality assurance.

11. Disclosure of Personal Information

Voice Office does not sell, rent, or trade Personal Information for monetary or other valuable consideration. We do not share Personal Information for cross-context behavioral advertising. We disclose Personal Information only in the following circumstances:

- **To the Subscriber:** Caller data collected during an interaction is made available to the Subscriber on whose behalf the data was collected. The Subscriber is the owner and Controller of this data.
- **To Sub-processors:** We engage vetted third-party service providers to assist in delivering the Services, including cloud hosting, database management, telephony (VoIP), AI processing, email delivery, and payment processing. Sub-processors are contractually bound by data processing agreements that require them to: (i) process data solely on Voice Office's instructions; (ii) maintain appropriate technical and organizational security measures; and (iii) not use the data for any unauthorized purpose. A current list of categories of Sub-processors is available upon request to privacy@voiceoffice.ca.
- **To Legal Authorities:** We may disclose Personal Information if compelled by a valid subpoena, court order, or government regulation, or where we believe in good faith that disclosure is necessary to: (i) comply with applicable law; (ii) protect the rights, property,

or safety of Voice Office, our Subscribers, or others; or (iii) prevent fraud or other illegal activity.

- **Corporate Transactions:** In the event of a merger, acquisition, reorganization, bankruptcy, or sale of all or a portion of our assets, Personal Information may be transferred as part of the transaction. We will provide notice of any such transfer and any choices you may have regarding your data.
- **With Consent:** We may disclose Personal Information where the individual has provided explicit consent to such disclosure.

12. Financial Transactions

Voice Office does not directly store credit card numbers, banking credentials, or other sensitive payment data on its infrastructure. All payments are facilitated through PCI-DSS compliant third-party payment processors. Where the Voice Agent assists a Caller in navigating a payment flow, the actual processing and storage of financial data occur on the secure servers of the payment gateway. Voice Office may retain transaction records (e.g., amount, date, and transaction reference number) for billing and accounting purposes.

13. Data Retention

Voice Office retains Personal Information only as long as necessary to fulfill the purposes described in this Policy, to comply with our legal obligations, or to enforce our agreements.

- **Subscriber Account Data:** Retained for the duration of the active subscription. Upon cancellation, data is retained for a 30-day grace period to allow for reinstatement, after which it is permanently deleted unless a longer retention period is required by law.
- **Caller Interaction Data (Recordings and Transcripts):** Retained on a rolling 30-day basis by default. Subscribers may configure shorter or longer retention periods based on their compliance requirements. Data held by Sub-processors is deleted in accordance with the same retention schedule.
- **Technical and Telemetry Data:** Retained for up to 12 months for analytics and security purposes, after which it is deleted or aggregated and de-identified.
- **Marketing Data:** Retained until the individual opts out of marketing communications. We periodically remove inactive contacts from our marketing lists.
- **Financial and Billing Records:** Retained for a minimum of 7 years as required by applicable tax and accounting regulations.
- **Deletion Protocol:** When data reaches the end of its applicable retention period, it is securely deleted or anonymized using industry-standard methods. Deletion requests directed to Sub-processors are confirmed in writing.

14. Breach Notification

Voice Office maintains an incident response program designed to detect, investigate, and respond to security incidents involving Personal Information.

14.1 Notification to Subscribers

In the event of a confirmed or suspected breach involving Caller data processed on behalf of a Subscriber, Voice Office will notify the affected Subscriber without unreasonable delay and in any event within the timeframe required by the applicable Data Processing Agreement or BAA, and no later than 72 hours after becoming aware of the breach. Notification will include a description of the nature of the breach, the categories and approximate number of records affected, and the measures taken or proposed to address the breach.

14.2 Regulatory Notification

- **PIPEDA (Canada):** Where a breach of security safeguards creates a real risk of significant harm to an individual, Voice Office will report the breach to the Office of the Privacy Commissioner of Canada and notify affected individuals as required under PIPEDA's breach notification provisions.
- **PHIPA (Ontario):** Where there is a breach involving personal health information, Voice Office will notify the affected Health Information Custodian (Subscriber) and, where required, the Information and Privacy Commissioner of Ontario.
- **HIPAA (United States):** In accordance with the HIPAA Breach Notification Rule, Voice Office will notify the affected Covered Entity (Subscriber) of any breach of unsecured PHI. The Subscriber, as the Covered Entity, bears responsibility for notifying affected individuals and the U.S. Department of Health and Human Services.
- **U.S. State Laws:** Voice Office will comply with applicable state breach notification laws, including providing timely notice to affected individuals and state attorneys general as required.

14.3 Record Keeping

Voice Office maintains records of all privacy and security incidents, including those that do not meet the threshold for external notification, for a minimum of three years.

15. User Rights

15.1 Rights of Subscribers

Subscribers may access, correct, export, or delete their business data through the Voice Office dashboard or by contacting support. Upon termination of a subscription, Subscribers may request a full data export prior to the expiration of the 30-day grace period described in Section 13.

15.2 Rights of Callers

Because Voice Office processes Caller data as a Data Processor on behalf of the Subscriber, data subject rights requests from Callers must be directed to the Subscriber (the business the Caller contacted). Voice Office will assist the Subscriber in fulfilling verified requests upon instruction. This includes requests to access, correct, delete, or obtain a copy of Personal Information.

15.3 Communication Preferences

- You may opt out of marketing communications at any time by clicking “Unsubscribe” in our emails or by contacting us at privacy@voiceoffice.ca.
- You may opt out of automated SMS messages by replying “STOP.”

16. Regional Privacy Rights

16.1 United States — State Consumer Privacy Laws

Residents of states with comprehensive consumer privacy laws—including California (CCPA/CPRA), Colorado, Connecticut, Virginia, Utah, Texas, Oregon, and others—may have the following rights with respect to their Personal Information:

- **Right to Know / Access:** You may request information about the categories and specific pieces of Personal Information we have collected about you.
- **Right to Delete:** You may request the deletion of your Personal Information, subject to our role as a Processor and applicable legal exceptions.
- **Right to Correct:** You may request that we correct inaccurate Personal Information.
- **Right to Opt Out:** You may opt out of the sale or sharing of your Personal Information. As stated in Section 11, Voice Office does not sell or share Personal Information for cross-context behavioral advertising.
- **Right to Non-Discrimination:** We will not discriminate against you for exercising any of these rights.
- **Right to Limit Use of Sensitive Personal Information:** Where applicable, you may direct us to limit the use of sensitive Personal Information to purposes authorized by law.

HIPAA Exemption: Personal Information that qualifies as PHI under HIPAA is generally exempt from state consumer privacy laws. If your data is processed as PHI, your rights are governed by HIPAA and must be exercised through your healthcare provider.

To submit a rights request, please contact us using the information in Section 19. We will verify your identity before processing any request and will respond within the timeframe required by applicable law.

16.2 Canada — PIPEDA and Provincial Privacy Laws

Canadian residents are protected under PIPEDA and applicable provincial privacy legislation. You have the following rights:

- **Access and Accuracy:** You have the right to request access to your Personal Information and to request corrections to any inaccuracies.
- **Withdrawal of Consent:** You may withdraw consent for the processing of your Personal Information at any time, subject to legal or contractual restrictions and reasonable notice. Withdrawal of consent may affect our ability to provide certain Services.

- **Complaints:** If you believe your privacy rights have been violated, you may contact our Privacy Officer. If we are unable to resolve your concern, you have the right to file a complaint with the Office of the Privacy Commissioner of Canada or the applicable provincial privacy commissioner.

17. Children's Privacy

Our Services are designed for use by businesses and are not directed at individuals under the age of 13. Voice Office does not knowingly collect Personal Information from children under 13 (or under 16 where required by applicable state law). In the healthcare context, a parent or legal guardian may provide information about a minor patient to the Voice Agent in their capacity as the authorized representative. If we become aware that we have collected Personal Information from a child without appropriate parental consent, we will take prompt steps to delete such information. To report a concern, please contact us at privacy@voiceoffice.ca.

18. Third-Party Links and Integrations

The Services may contain links to external websites or integrate with third-party software (e.g., EMR systems, CRMs, calendaring tools) at the Subscriber's direction. Voice Office does not control these third-party platforms and is not responsible for their privacy practices. This Policy applies solely to data processed by Voice Office. We encourage Subscribers and Callers to review the privacy policies of any third-party service with which Voice Office integrates.

19. Geographic Location of Data Processing

Voice Office is headquartered in Milton, Ontario, Canada. Our technical infrastructure is distributed across data centers located in Canada and the United States to ensure high availability and low latency.

Cross-Border Transfer Notice: By using the Services, you acknowledge that your Personal Information may be transferred to, stored, and processed on servers located in the United States. While your data is in the United States, it is subject to U.S. laws and may be accessible to U.S. government authorities, courts, or law enforcement agencies under lawful authority. Voice Office implements the following safeguards for cross-border transfers:

- Contractual data processing agreements with all Sub-processors that require equivalent privacy protections;
- Encryption of data in transit and at rest (see Section 20);
- Access controls limiting data access to authorized personnel with a legitimate business need; and
- Regular security assessments of infrastructure and Sub-processors.

20. Information Security

Voice Office implements administrative, technical, and physical safeguards designed to protect Personal Information against accidental loss, unauthorized access, disclosure, alteration, and destruction.

- **Encryption:** All data is encrypted in transit using TLS 1.2 or higher and at rest using AES-256 encryption.
- **Access Control:** We employ Role-Based Access Control (RBAC). Access to Personal Information and PHI is restricted to authorized personnel with a documented business need.
- **Vulnerability Management:** We conduct regular security assessments and vulnerability scans of our infrastructure.
- **Sub-processor Standards:** Our third-party AI and infrastructure providers maintain industry-recognized certifications including SOC 2 Type II and HIPAA compliance. Voice Office conducts due diligence on all Sub-processors prior to engagement and on an ongoing basis.
- **Employee Training:** All Voice Office personnel with access to Personal Information receive privacy and security awareness training.

Disclaimer: No method of transmission over the internet or electronic storage is completely secure. While we implement rigorous safeguards, we cannot guarantee absolute security. Subscribers are responsible for maintaining the confidentiality of their account credentials and for configuring appropriate access controls within their Voice Office dashboard.

21. Updates to This Policy

Voice Office reserves the right to update this Policy to reflect changes in our practices, technology, legal requirements, or business operations. When we make material changes, we will: (a) update the “Last Updated” date at the top of this Policy; (b) notify Subscribers via email or a prominent notice within the Platform; and (c) where required by law, obtain consent before applying material changes to previously collected data. We encourage you to review this Policy periodically.

22. Contact Information

For questions about this Privacy Policy, to exercise your privacy rights, or to raise a compliance concern, please contact:

Voice Office

Attn: Privacy Officer

Milton, Ontario, Canada

General Inquiries: contact@voiceoffice.ca

Privacy Inquiries: privacy@voiceoffice.ca

Website: voiceoffice.ca

We will acknowledge receipt of your inquiry within five (5) business days and will endeavor to respond substantively within thirty (30) days, or as otherwise required by applicable law.