

VoiceRun Privacy Policy

Effective Date: November 20, 2025

VoiceRun (“**VoiceRun**,” “**we**,” “**us**,” or “**our**”) provides a cloud-hosted platform for building, deploying, and operating AI-powered voice agents and related services, including telephony, speech-to-text (STT), text-to-speech (TTS), large language model (LLM) orchestration, and developer tools.

This Privacy Policy explains how we collect, use, disclose, and safeguard personal information when you:

- Visit **voicerun.com** or any related websites that link to this Policy;
- Create and use a VoiceRun account (including via our management console and APIs);
- Use VoiceRun to run calls, agents, or other workloads; or
- Interact with us via email, support tickets, or other channels.

By using VoiceRun, you agree to the practices described in this Privacy Policy.

1. Who We Are & Scope

VoiceRun, Inc is a Delaware Corporation with offices in Cambridge, MA, USA.

This Privacy Policy is primarily aimed at **platform users who sign up for a VoiceRun account** (including individual developers, employees of business customers, and other administrators). It also explains, at a high level, how we handle personal information belonging to people who interact with VoiceRun-powered voice agents (for example, callers to a phone number that uses VoiceRun).

If you are interacting with a VoiceRun-powered agent created by one of our customers, that customer is the “controller” or “business” for your personal information, and their privacy notice will apply in addition to this one.

2. Key Concepts

We use a few important terms:

- **Account Data** – Information about you as a platform user, such as your name, email, login credentials, organization, and billing details.
- **Customer Content** – Any content and data you or your organization send through VoiceRun (for example: call audio, transcripts, prompts, agent configuration, business logic, and payloads sent via our APIs).

- **Telemetry / Aggregated Data** – De-identified telemetry, performance metrics, and usage statistics that we generate from operating the platform (for example: call duration, error rates, model latency).

We treat **Customer Content** as your or your organization's data. We use **Telemetry / Aggregated Data** to operate and improve VoiceRun, but we design it so it does not identify individual users or callers.

3. Information We Collect

3.1 Information You Provide to Us

When you interact with VoiceRun, you may provide:

1. **Account and Profile Information**
 - Name, email address, password or SSO identifier;
 - Organization name, role, and team membership;
 - Billing details such as billing contact, company address, and limited payment details (payment card information is typically processed by our payment processor rather than stored directly by VoiceRun).
2. **Customer Content (Voice, Text, and Other Inputs)**
 - **Voice & Audio Data:** Audio from phone calls or other voice channels that you route through VoiceRun. Depending on your configuration, this may include both real-time streaming audio and (if you enable recordings) stored call recordings.
 - **Transcripts & Text:** Real-time transcripts of calls, prompts and system messages you define for agents, and text inputs/outputs exchanged with LLMs.
 - **Agent Logic & Configuration:** Call-flow scripts, prompts, business rules, routing logic, and other voice-UX assets that you configure in the platform.
3. **User Content & Communications**
 - Support requests, emails, and other messages;
 - Feedback, bug reports, and survey responses;
 - Content you submit via forms (for example: "Contact sales" forms).
4. **Payment and Commercial Information**
 - Subscription plan, minutes used, invoices, and records of transactions.

3.2 Information We Collect Automatically

When you use VoiceRun, we automatically log certain information, such as:

- **Device & Log Data**
 - IP address, browser type, operating system, device identifiers;

- Dates/times of access, pages viewed, referring URLs;
- API usage (request time, endpoint, status codes, latency).
- **Usage & Performance Telemetry**
 - Call duration, call outcomes, model response times;
 - Error codes and diagnostics generated by our systems;
 - Aggregate statistics about features used and performance.
- **Cookies & Similar Technologies**
 - We use cookies and similar tools (such as local storage and pixels) for authentication, preferences, analytics, and (where applicable) marketing. See **Section 8 (Cookies & Tracking)**.

3.3 Information We Receive from Third Parties

We may receive information from:

- **Authentication / Identity Providers**
 - If you sign in with a third-party authentication provider (for example, an enterprise SSO or OAuth provider), we receive basic profile information (such as name, email, unique ID) from that provider.
- **Telephony, STT, TTS, and LLM Providers**
 - VoiceRun operates as an orchestration layer that relies on cloud telephony carriers, speech-to-text, text-to-speech, and large language model providers (for example, Twilio-like telephony providers and STT/LLM vendors).
 - As part of processing your calls and prompts, these providers return transcripts, synthesized speech, and model outputs to us.
- **Integration Partners & Customers**
 - If your organization connects VoiceRun to an external system, we may receive identifiers (for example, customer IDs, lead IDs) and other metadata your organization chooses to sync.
- **Public or Enterprise Data Sources**
 - Limited business contact or firmographic information may come from enterprise data providers (e.g., to pre-populate company fields or validate accounts), where permitted by law.

4. How We Use Your Information

We use personal information for the following purposes

1. To Provide and Operate the Services

- Setting up and maintaining your account and workspace;
- Routing and processing voice calls and text interactions;
- Executing your configured call flows, prompts, and integrations;
- Providing dashboards, logs, and analytics.

2. To Secure, Monitor, and Maintain the Platform

- Monitoring availability and performance;
- Detecting and preventing fraud, abuse, or security incidents;
- Debugging and supporting business continuity and disaster recovery plans.

3. To Improve VoiceRun

- Analyzing aggregated and de-identified telemetry to improve reliability, latency, and user experience;
- Developing new features and functionality.

4. To Communicate with You

- Responding to your support requests and questions;
- Sending service-related communications (for example, security alerts, billing notices, feature updates);
- Sending optional product updates or marketing communications (where permitted and subject to your preferences).

5. To Comply with Law and Enforce Our Rights

- Responding to lawful requests from public authorities;
- Enforcing our terms, policies, and agreements;
- Protecting our rights, property, and safety, or the rights, property, and safety of others.

We do **not** use your Account Data or Customer Content to make decisions that produce legal or similarly significant effects about you solely by automated means.

5. How We Use AI, Voice, and Customer Content

5.1 Real-Time Processing

During a call or interaction, VoiceRun:

- Receives audio via telephony or over the web;
- Uses voice activity detection and STT services to create transcripts;
- Sends transcripts and context to LLMs and other models to generate responses;
- Uses TTS to generate a spoken reply;

This processing is necessary to provide the services you have configured.

5.2 Storage of Audio, Transcripts, and Metadata

- **Transcripts & Metadata:** We store transcripts and call metadata (timestamps, call duration, disposition codes, etc.) so that you can review calls, debug flows, and monitor performance.
- **Audio Recordings:** We store audio recordings only if recording is enabled in your configuration or required for a specific feature or legal obligation (for example, for quality assurance or compliance). Where supported, you may be able to configure retention periods or disable recordings at the account or campaign level.

5.3 Training and Tuning of AI Models

- **We do not use your Customer Content (such as call audio, transcripts, prompts, and business logic) to train or fine-tune our foundation models or third-party foundation models for the benefit of other customers, unless:**
 - you have explicitly opted in; or
 - we offer a clearly labeled feature where such training is necessary and you choose to enable it.
- We may use **aggregated and de-identified telemetry** (for example, error rates, latency metrics, and high-level usage patterns) to improve performance, scaling, and reliability of the platform and to develop new features, as long as it cannot reasonably be linked back to you or your callers.

6. How We Share Personal Information

We do not sell personal information or share it for cross-context behavioral advertising as those terms are defined under California law.

We may share personal information with:

1. Service Providers and Sub-Processors

We rely on third parties to help us deliver VoiceRun, including:

- Cloud hosting and infrastructure providers;
- Telephony carriers and SIP providers;
- STT, TTS, and LLM providers;
- Payment processors;
- Email, support, logging, and monitoring tools.

2. These service providers are limited to using personal information to perform services on our behalf, under contracts that include confidentiality and data-protection obligations consistent with applicable law.

3. Your Organization and Workspace Administrators

- If you use VoiceRun under a workspace or enterprise account, certain Account Data, activity logs, and usage metrics may be visible to your organization's administrators and owners.
- If multiple users share a workspace, your name, email, and activity may be visible to other members of that workspace.

4. Third-Party Integrations You Enable

- If you connect VoiceRun to external systems (for example, a CRM or ticketing tool), we will send data to those systems according to your configuration. The third party's own privacy policy governs their use of that data.

5. Business Transfers

- In connection with a merger, acquisition, financing, reorganization, bankruptcy, or sale of some or all of our assets, personal information may be disclosed or transferred to a different entity as part of that transaction, subject to appropriate safeguards.

6. Legal and Safety Disclosures

- We may disclose information when we believe in good faith that such disclosure is reasonably necessary to:
 - Comply with any applicable law, regulation, legal process, or governmental request;
 - Enforce agreements and policies;
 - Protect the rights, property, or safety of VoiceRun, our users, or the public.

7. Data Retention

We retain personal information only for as long as reasonably necessary to:

- Provide VoiceRun to you and your organization;
- Meet our legal, tax, accounting, or reporting obligations;
- Resolve disputes and enforce our agreements.

In practice, retention periods vary based on data type and configuration. For example:

- Account Data is generally retained for the life of your account and then for a period reasonably necessary to comply with legal obligations or resolve disputes.
- Call transcripts, recordings, and logs are retained according to your organization's settings where available; otherwise, we apply default retention periods that are no longer than necessary for the purposes described in this Policy.
- Aggregated and de-identified telemetry may be retained for a longer period because it does not reasonably identify an individual.

You may request deletion of certain data as described in **Section 10 (Your Rights & Choices)**.

8. Cookies & Tracking Technologies

We use cookies and similar technologies on our websites and web apps for several purposes:

- **Essential Cookies**
 - Required for basic functionality such as sign-in, session management, and security.
- **Analytics Cookies**
 - Help us understand how users interact with VoiceRun so we can improve performance and usability (for example, page views, feature usage, navigation flows).
- **Preference Cookies**
 - Remember your preferences (for example, language, theme).
- **Marketing Cookies (Where Applicable)**
 - If we run marketing campaigns, we may use cookies or pixels to measure campaign performance or attribute sign-ups.

Where required by law, we will request your consent before placing non-essential cookies and provide options to withdraw or adjust your preferences.

You can manage cookies through your browser settings. If you disable certain cookies, parts of VoiceRun may not function properly.

9. Security

We take reasonable and appropriate technical and organizational measures to protect personal information against loss, misuse, and unauthorized access, disclosure, alteration, and destruction. These measures include (among others):

- Encryption in transit and at rest for appropriate data types;
- Logical and technical segregation of customer data;
- Role-based access controls and least-privilege permissions;
- Logging and monitoring of platform activity;
- Business continuity and disaster recovery plans;
- Vendor due diligence and contractual data-protection obligations for processors and sub-processors.

While we work hard to protect your information, no system can be guaranteed 100% secure. You are responsible for safeguarding your account credentials and for configuring security options (such as SSO and access controls) available to your organization.

10. International Data Transfers

VoiceRun is operated from the United States and may process personal information in the United States and other countries. Our sub-processors may also be located in various jurisdictions.

Where required by law, we implement appropriate safeguards for international transfers, such as:

- Standard contractual clauses or other approved transfer mechanisms for transfers from the EEA/UK/Switzerland; and
- Contractual restrictions on using “countries of concern” and certain high-risk recipients for sensitive U.S. personal data, consistent with applicable U.S. regulations.

By using VoiceRun, you acknowledge that your personal information may be transferred to and processed in jurisdictions that may have data-protection laws different from your home jurisdiction.

11. Your Rights & Choices

Your rights depend on your location and applicable law, but may include:

- **Access & Portability**
 - You can request a copy of the personal information we hold about you and, in some cases, receive it in a structured, commonly used, machine-readable format.
- **Correction**
 - You can request that we correct inaccurate or incomplete personal information.
- **Deletion**
 - You can request that we delete certain personal information, subject to legal and contractual limitations.
- **Restriction or Objection**
 - You may have the right to object to or request restriction of certain processing (for example, where we rely on legitimate interests).
- **Consent Management**
 - Where we rely on consent (for example, for certain cookies or marketing), you can withdraw that consent at any time. Withdrawing consent does not affect the lawfulness of processing before withdrawal.
- **Marketing Preferences**
 - You can opt out of marketing emails by clicking the “unsubscribe” link in those emails or by contacting us.

To exercise your rights, please contact us at privacy@voicerun.com and clearly describe your request. We may need to verify your identity before fulfilling your request, and in some cases we

may be unable to fully comply (for example, where we must retain data for legal reasons); if so, we will explain why.

If you are an end user of a VoiceRun-powered agent (for example, a caller to a number operated by one of our customers), please direct your request to that customer, as they are typically the controller of your data. We will support them in responding to your request where applicable.

12. Additional Disclosures for Certain U.S. States (Including California)

If you are a resident of California or certain other U.S. states with similar privacy laws, you may have additional rights.

12.1 Categories of Personal Information We Collect

In the past 12 months, we have collected the following categories of personal information (as defined under California law) from platform users and, where applicable, callers:

- Identifiers (e.g., name, email address, IP address, device ID);
- Commercial information (e.g., subscription plan, usage, transaction history);
- Internet or other electronic network activity information (e.g., usage logs, analytics);
- Audio and electronic information (e.g., call audio and transcripts, where enabled);
- Professional or employment-related information (e.g., role, organization);
- Inferences drawn from the above (in aggregated or de-identified form).

We collect these categories for the business purposes described in Sections 4–6.

12.2 Sale / Sharing

We do **not**:

- Sell personal information; or
- Share personal information for cross-context behavioral advertising.

We may “disclose” personal information to service providers and contractors for business purposes as described in Section 6.

12.3 Your State-Law Rights

Depending on your state, you may have the right to:

- Know what personal information we collect, use, and disclose;
- Access your personal information;

- Request deletion of your personal information;
- Correct inaccurate personal information;
- Obtain a portable copy of your personal information;
- Not be discriminated against for exercising your privacy rights.

You or your authorized agent can exercise these rights by emailing **privacy@voicerun.com**. If we deny your request (for example, because we cannot verify your identity or the request is not permitted by law), you may have the right to appeal; if applicable, we will tell you how to do so in our response.

13. Additional Information for EEA/UK/Swiss Users

If you are located in the EEA, the UK, or Switzerland:

- The controller of your personal information for Account Data is **VoiceRun, Inc.**
- For Customer Content processed on behalf of a business customer, that customer is the controller and we act as a processor/service provider.

You have the rights described in Section 11 and, additionally, the right to lodge a complaint with your local data protection authority. However, we encourage you to contact us first so we can try to resolve your concerns.

14. Children's Privacy

VoiceRun is **not intended for individuals under 18**, and we do not knowingly collect personal information from children. If we learn that we have collected personal information from a child under 18 without appropriate consent, we will take reasonable steps to delete it.

If you believe a child has provided us with personal information, please contact us at **privacy@voicerun.com**.

15. Changes to This Policy

We may update this Privacy Policy from time to time—for example, to reflect changes in our services, technology, or legal requirements. When we do, we will:

- Update the “Effective Date” at the top of this page; and
- Provide additional notice (such as an in-app notice or email) if required by law or if we make material changes.

Your continued use of VoiceRun after an update means you accept the revised Policy.

16. Contact Us

If you have any questions, requests, or concerns about this Privacy Policy or our data practices, you can contact us at:

Email: privacy@voicerun.com