

Privacy Policy

Last updated: July 24, 2026

This Privacy Policy describes how RunCRM, Inc. ("RunCRM," "we," "us," or "our") collects, uses, and discloses personal information when you visit www.runcrm.ai, use the RunCRM platform at app.runcrm.ai, or otherwise interact with our AI-powered revenue operations services for lead qualification, customer reactivation, and accounts-receivable collection (collectively, the "Services").

RunCRM collects and uses personal information in two distinct capacities:

- 1. For our own business purposes** — for example, when you create a RunCRM account, visit our website, or communicate with us, we act as the "business" or "controller" of that information.
- 2. As a service provider (processor) on behalf of our business customers** ("Customers") — when a Customer connects its CRM, uploads contact and invoice data, or uses our AI agents to call, text, or email its own customers ("End Users"), we process that information on the Customer's behalf and under its instructions, pursuant to our agreement with that Customer.

If you received a phone call, text message, or email from a business that uses RunCRM: that business — not RunCRM — decides why and how your information is used. Requests about your information (including access or deletion requests) should be directed to that business. Where we can identify the relevant Customer, we will forward your request and assist the Customer in responding, consistent with our role as a service provider.

1. Personal Information We Collect

1.1 Information You Provide to Us

- **Account information:** first and last name, email address, password (stored in hashed form), phone number, job title, profile photo, time zone, and language preferences.

- **Organization information:** company name, business location names and addresses, team structure, roles, and the email addresses of teammates you invite.
- **Billing information:** our payment processor (Stripe) collects your payment card details. We do not store full card numbers; we retain your subscription plan, billing status, and the last four digits of your payment method.
- **Communications with us:** the contents of messages you send us, such as support requests, sales inquiries, and feedback.

1.2 Customer Data We Process on Behalf of Our Customers

When Customers use the Services, we receive and process information about their End Users under the Customer's direction ("Customer Data"), including:

- **CRM records** synced from systems the Customer connects (for example Salesforce, HubSpot, QuickBooks, Zoho, Pipedrive, and others): End User names, contact persons, email addresses, phone numbers, account status, industry, invoices, balances, payment history, and related notes.
- **Voice interactions:** audio of telephone calls placed or received by the Customer's AI agents (recorded only when the Customer enables recording), real-time and post-call transcripts, and structured call outcomes (for example payment commitments, callback requests, disputes, and do-not-call requests).
- **Messages:** the contents of SMS text messages and emails sent through the Services, such as payment reminders and payment links, together with delivery metadata.
- **Escalation records and notes** created by the Customer's team when a conversation is handed off to a human.
- **Communications metadata:** phone numbers dialed, call duration and status, message delivery status, timestamps, and carrier routing information.

1.3 Information We Collect Automatically

When you visit our website or use the platform, we automatically collect:

- **Log and device data:** IP address, browser type and version, operating system, device information, pages visited, features used, timestamps, and API request logs.

- **Cookies and similar technologies:** we use strictly necessary cookies for authentication, session management, and security (for example CSRF protection). Our marketing website does not currently use third-party advertising cookies or cross-context behavioral advertising trackers.

1.4 Information We Receive from Third Parties

- **Connected CRM and accounting platforms,** at the Customer's direction, as described above.
- **Telecommunications providers** (for example Twilio and underlying carriers): phone number validation, call and message delivery status, and related network metadata.
- **Payment processors** (Stripe): transaction status and billing verification data.

2. Call Recording, Transcription, and AI Processing

The Services place and answer telephone calls using AI voice agents. Call audio is processed in real time by our AI infrastructure providers to generate the agent's speech, understand the other party, and produce transcripts.

- **Recording controls.** Call recording is configured by each Customer per business location. When recording is enabled, the AI agent discloses at the beginning of the call that the call is on a recorded line.
- **Storage and retention.** Recordings are stored encrypted in Amazon Web Services (S3) in the United States and are automatically deleted at the end of the retention period selected by the Customer (90, 180, or 365 days). Transcripts and structured call outcomes are retained as described in Section 6.
- **No biometric identification.** We do not create voiceprints and we do not use call audio to biometrically identify individuals.
- **Expressive speech analysis.** Where a Customer enables an empathic voice provider (for example Hume AI), acoustic characteristics of speech may be analyzed in real time solely so the AI agent can respond appropriately in the conversation. These signals are not used to identify individuals.

- **Model training.** We do not use Customer Data to train general-purpose AI models. Our AI subprocessors are engaged under terms that restrict their use of Customer Data to providing services to us.

3. How We Use Personal Information

We use the personal information we collect to:

- provide, operate, maintain, secure, and improve the Services;
- create and administer accounts, authenticate users, and manage teams and permissions;
- place, route, and deliver voice calls, text messages, and emails on behalf of our Customers;
- generate transcripts, summaries, call outcomes, and reporting for our Customers;
- process payments, administer subscriptions, and calculate usage-based charges;
- provide customer support and respond to inquiries;
- monitor, detect, and prevent fraud, abuse, security incidents, and violations of our Terms of Service (including telemarketing and debt-collection misuse);
- analyze usage in aggregated or de-identified form to improve conversation quality, reliability, and product features;
- send administrative and service communications (for example billing notices, security alerts, and changes to our terms);
- send marketing communications about our own products, from which you may opt out at any time;
- comply with applicable laws, regulations, telecommunications-industry requirements, and legal process; and
- fulfill any other purpose disclosed to you at the time of collection or with your consent.

We do not sell personal information, and we do not share personal information for cross-context behavioral advertising.

We do not sell, rent, or share mobile phone numbers with third parties or affiliates for their marketing or promotional purposes. Mobile numbers collected for text messaging are used only to deliver the SMS messages described in Section 5 and to operate related account, authentication, and service functions.

Where we process Customer Data as a service provider, we use it only to provide the Services to the relevant Customer, consistent with our agreement with that Customer, and for no other commercial purpose.

4. How We Disclose Personal Information

We disclose personal information to the following categories of recipients:

- **Service providers and subprocessors** that perform functions on our behalf, under contracts restricting their use of the information, including:
 - **Twilio** — telephony, call routing, and SMS delivery (phone numbers, call audio in transit, message contents, delivery metadata);
 - **OpenAI** — speech processing, transcription, and language understanding for AI conversations and post-call analysis;
 - **ElevenLabs** — conversational voice synthesis and dialogue audio;
 - **Hume AI** — empathic speech-to-speech processing, where enabled;
 - **Amazon Web Services** — cloud hosting, storage, and email delivery infrastructure;
 - **Stripe** — payment processing and subscription billing;
 - **Sentry** — error monitoring (configured not to receive personal information by default).
- **Telecommunications carriers**, which may process call and message metadata as independent controllers for network routing, interconnection, billing, and fraud prevention.
- **Connected CRM and accounting platforms**, when a Customer directs us to sync data to or from those systems.
- **Affiliates and subsidiaries**, for purposes consistent with this Privacy Policy.

- **Parties to a business transaction**, such as a merger, acquisition, financing, or sale of assets, in which personal information may be transferred or disclosed during diligence, subject to appropriate protections.
- **Law enforcement, regulators, and courts**, where we believe disclosure is required by law or legal process, or is necessary to protect the rights, property, or safety of RunCRM, our Customers, End Users, or the public.
- **Others with your consent** or at your direction.

We may also disclose aggregated or de-identified information that cannot reasonably be used to identify you.

5. Text Messaging (SMS)

The Services may send SMS text messages to mobile phone numbers you provide, or to mobile numbers our Customers provide for their End Users, including payment reminders, account notices, authentication codes, and other service-related messages.

- **Message frequency varies.** You may receive recurring messages; the number of messages depends on your account activity, the communications you consent to, and (where applicable) the reminder and follow-up schedules configured by the business that contacted you. Typical programs send a small number of messages per week when reminders are active, and fewer or none when no action is scheduled.
- **Message and data rates may apply.** Standard message and data rates from your wireless carrier may apply to messages you send or receive. Check your mobile plan for details.
- **No sharing of mobile numbers for marketing.** We do not sell, rent, or share your mobile phone number with third parties or affiliates for their marketing or promotional purposes.
- **Opt out.** Reply **STOP** to any SMS from us (or from a program operated on the Services) to cancel further text messages from that program. Reply **HELP** for help. You may also contact privacy@runcrm.ai. After you opt out, you may receive one confirmatory message acknowledging your request. Transactional messages required for account security may still be sent where permitted by law.

If you received a text from a business that uses RunCRM, that business is the sender of record for the program; RunCRM processes the message as a service provider. Opt-out and HELP keywords are still honored as described above.

6. Your Choices

- **Account information.** You may review and update your account information in your profile settings, and you may delete your account from account settings or by contacting us.
- **Marketing emails.** You may opt out of marketing emails using the unsubscribe link in any such email. We will still send transactional and service messages while you have an account.
- **Text messages.** Reply STOP to cancel SMS messages as described in Section 5. Message frequency varies. Message and data rates may apply.
- **Cookies.** You can configure your browser to refuse cookies, although parts of the Services that rely on authentication cookies will not function without them.

7. Data Retention

We retain personal information only as long as necessary for the purposes described in this Privacy Policy:

- **Call recordings:** deleted automatically at the end of the retention period selected by the Customer (90, 180, or 365 days).
- **Transcripts, call outcomes, CRM records, and messages:** retained for as long as the Customer's account is active or as the Customer directs; deleted or de-identified following account termination, subject to a reasonable wind-down period and legal retention obligations.
- **Account and billing records:** retained for the life of the account plus the period required for tax, accounting, and audit purposes.
- **Log data:** retained for shorter periods appropriate to security and reliability operations.

Where we act as a service provider, the Customer determines retention of Customer Data within the options the platform provides.

8. Security

We maintain administrative, technical, and physical safeguards designed to protect personal information, including encryption in transit (TLS) and at rest, encrypted storage of integration credentials, role-based access controls, expiring session tokens, and optional two-factor authentication for user accounts. No method of transmission or storage is completely secure, and we cannot guarantee absolute security. If you have reason to believe your interaction with us is no longer secure, please contact us immediately at privacy@runcrm.ai.

9. Your U.S. State Privacy Rights

Depending on where you live, state privacy laws (including the California Consumer Privacy Act as amended by the CPRA, and comparable laws in Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Montana, Florida, Iowa, Delaware, New Hampshire, Nebraska, New Jersey, Tennessee, Minnesota, Maryland, Indiana, Kentucky, Rhode Island, and other states) may give you the right to:

- **know** what personal information we collect, use, and disclose about you;
- **access** and obtain a **portable copy** of your personal information;
- **correct** inaccurate personal information;
- **delete** your personal information, subject to legal exceptions;
- **opt out** of the sale of personal information, sharing for cross-context behavioral advertising, and certain profiling (as described above, we do not sell or share personal information for these purposes);
- **limit the use of sensitive personal information** (we use sensitive information only to provide the Services); and
- **not receive discriminatory treatment** for exercising your rights.

Categories of personal information collected. In the preceding 12 months we have collected the categories described in Section 1: identifiers (name, email, phone number, IP address); commercial information (subscription and invoice records); internet and network activity (log data); coarse geolocation inferred from IP address; professional information (employer, job title); audio and electronic information (call recordings and transcripts processed on behalf of Customers); and inferences limited to service operation (for example call outcomes).

How to exercise your rights. Email privacy@runcrm.ai with the subject line "Privacy Request." We will verify your identity by matching information you provide against our records, and we will respond within 45 days (extendable once by 45 days where reasonably necessary). You may authorize an agent to submit a request on your behalf with proof of written authorization. If we decline your request, you may appeal by replying with the subject line "Privacy Appeal"; if your appeal is denied, you may contact your state attorney general.

End User data. Where your information was collected by a business that uses RunCRM, that business is responsible for responding to your request, and we will assist it as its service provider. We will forward verifiable requests we receive to the relevant Customer where we can identify it.

We honor opt-out preference signals such as Global Privacy Control where required by applicable law. Because we do not sell personal information or engage in cross-context behavioral advertising, these signals do not change how our Services currently operate.

10. European and United Kingdom Users

The Services are operated from the United States and are designed for businesses collecting from U.S. consumers. If the EU or UK General Data Protection Regulation applies to our processing of your personal data:

- We process personal data on the lawful bases of **contract performance** (providing the Services), **legitimate interests** (securing and improving the Services, business administration, and marketing to business contacts), **legal obligation**, and **consent** where required.

- You may have rights of access, rectification, erasure, restriction, portability, and objection, and the right to withdraw consent, by contacting privacy@runcrm.ai.
- Where we transfer personal data from the EEA, UK, or Switzerland to the United States, we rely on appropriate safeguards such as the European Commission's Standard Contractual Clauses and the UK International Data Transfer Addendum.
- You have the right to lodge a complaint with your local supervisory authority.

11. Biometric Information

We do not collect, capture, or store biometric identifiers or biometric information as defined under laws such as the Illinois Biometric Information Privacy Act, the Texas Capture or Use of Biometric Identifier Act, or Washington RCW 19.375. In particular, we do not create voiceprints or use voice recordings to identify individuals. Customers are prohibited under our Terms of Service from using the Services to collect biometric identifiers.

12. Children

The Services are business tools that are not directed to children. We do not knowingly collect personal information from anyone under 16, and Customers may not use the Services to direct communications to children. If we learn that we have collected personal information from a child under 16, we will delete it.

13. International Data Transfers

RunCRM is based in the United States, and personal information is stored and processed in the United States (primarily in AWS us-east-1). If you access the Services from outside the United States, you understand that your information will be transferred to and processed in the United States, where data protection laws may differ from those in your jurisdiction.

14. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. If we make material changes, we will notify you by posting the updated policy on this page with a new "Last updated" date and, where appropriate, by additional notice such as email or in-app notification. Your continued use of the Services after the effective date of an updated policy constitutes your acknowledgment of the changes.

15. Contact Us

If you have questions, concerns, or complaints about this Privacy Policy or our data practices, contact us:

RunCRM, Inc. Email: privacy@runcrm.ai Website: <https://www.runcrm.ai>