

Privacy Policy

Rose One LLC

Effective Date: January 1, 2026 | **Version:** 1.0

Welcome to Rose One ("App," "we," "us," or "our"). We are committed to protecting your personal information and your right to privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard information when you use our AI-powered personal chatbot subscription service, including all related payment processing and subscription management features.

This policy is designed to meet the requirements of applicable data protection regulations, including but not limited to the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA/CPRA), and the requirements of our payment processor, Stripe, Inc.

1. Information We Collect

1.1 Account and Identity Information

When you register for an account or subscribe to our service, we collect:

- Full name and email address
- Username and password (stored using industry-standard hashing)
- Profile preferences and settings
- Communication preferences

1.2 Payment and Billing Information

We use Stripe, Inc. as our sole payment processor. We do not store your full payment card details on our servers. The following applies to payment data:

- Payment card details (number, expiry, CVV) are collected and processed exclusively by Stripe and are never transmitted to or stored on our servers.
- We store a Stripe Customer ID, subscription status, plan tier, and billing cycle information to manage your subscription.
- Billing address and associated contact details are stored by Stripe in accordance with their Privacy Policy (available at stripe.com/privacy).
- Transaction identifiers, payment status, and invoice history are retained for accounting, fraud prevention, and legal compliance purposes.

1.3 Usage and Interaction Data

To provide, improve, and personalize our AI chatbot service, we collect:

- Chat session data, including messages and AI-generated responses
- Session timestamps, duration, and frequency of interactions

- Feature usage patterns and in-app navigation behavior
- Device type, operating system, browser type, and app version
- IP address and general geolocation (country/region level)
- Crash reports and error logs

1.4 Automatically Collected Technical Data

Our servers and third-party tools automatically collect certain technical data each time you access the App, including log files, cookies, pixel tags, and similar tracking technologies. See Section 6 for details on cookie controls.

2. How We Use Your Information

We process your personal data only when we have a lawful basis to do so. The purposes and corresponding legal bases are:

- **Service Delivery:** To provide, operate, and maintain the AI chatbot functionality you have subscribed to.
- **Subscription & Billing Management:** To process payments, manage subscription lifecycles, handle renewals and cancellations, and resolve billing disputes — in partnership with Stripe.
- **Fraud Prevention & Security:** To detect, investigate, and prevent fraudulent transactions, unauthorized access, chargebacks, and other security threats, including sharing relevant data with Stripe's fraud detection systems.
- **Legal & Regulatory Compliance:** To comply with applicable laws, regulations, court orders, and requests from law enforcement or governmental authorities, including PCI-DSS compliance obligations.
- **Service Improvement & Analytics:** To analyze aggregate usage patterns, improve AI model performance, and enhance user experience features. Where used for analytics, data is aggregated or pseudonymized where feasible.
- **Customer Support:** To respond to inquiries, troubleshoot issues, and communicate important service updates or changes.
- **Marketing (Opt-In Only):** To send promotional communications about new features or plans, only where you have provided explicit consent. You may withdraw consent at any time.

3. Payment Processing and Stripe

All payment transactions are processed by Stripe, Inc., a PCI-DSS Level 1 certified payment processor. Our integration with Stripe is designed to maximize security and minimize the personal data we handle directly.

3.1 Stripe's Role

Stripe acts as an independent data controller for the personal data it collects during payment processing. When you make a payment, you are also subject to Stripe's Privacy Policy and Terms of Service. We encourage you to review Stripe's policies at stripe.com/privacy.

3.2 What Stripe Receives

Through our integration, Stripe may receive or access:

- Payment card details (processed directly in Stripe's secure environment)
- Name and email address for receipt and identity verification
- Billing address for card verification and fraud screening
- Transaction amounts, currency, and subscription metadata
- Device fingerprint and IP address for fraud detection purposes

3.3 Stripe Radar and Fraud Prevention

We use Stripe Radar, Stripe's machine learning-based fraud detection tool. Stripe Radar may analyze transaction data, device signals, and behavioral patterns to assess fraud risk. Data shared with Stripe Radar is governed by Stripe's policies. By using our App, you consent to this processing as necessary for the legitimate interests of preventing financial fraud.

3.4 Subscription Management

Stripe manages recurring billing, subscription upgrades, downgrades, and cancellations. We retain subscription status and billing cycle data on our servers to deliver the appropriate service tier and to respond to your account inquiries.

4. Data Sharing and Disclosure

We do not sell your personal data. We may share your information only in the following circumstances:

- **Service Providers:** With vetted third-party vendors who assist us in operating the App (e.g., cloud hosting, analytics, customer support tools), under contractual data processing agreements that restrict their use of your data.
- **Payment Processor:** With Stripe, as described in Section 3, for the purpose of processing payments and managing subscriptions.
- **Legal Obligations:** When required by law, subpoena, or other legal process, or when we believe disclosure is necessary to protect our rights, prevent fraud, or ensure user safety.
- **Business Transfers:** In connection with a merger, acquisition, or sale of all or substantially all of our assets, provided the acquirer agrees to honor this Privacy Policy.
- **With Your Consent:** In any other circumstance, only with your explicit prior consent.

5. Data Retention

We retain personal data only for as long as necessary to fulfill the purposes described in this policy or as required by law:

- Account data is retained for the duration of your active subscription plus 12 months following account closure, to allow for dispute resolution.
- Payment transaction records are retained for a minimum of 7 years to comply with financial record-keeping requirements.
- Chat interaction data is retained for 90 days by default; you may request earlier deletion at any time (see Section 7).
- Fraud and security logs may be retained for up to 5 years to support fraud investigation and prevention obligations.
- Aggregated and anonymized analytics data may be retained indefinitely as it cannot be used to identify you.

6. Cookies and Tracking Technologies

We use cookies and similar technologies to operate and improve the App. Categories include:

- **Essential Cookies:** Required for authentication, session management, and security. Cannot be disabled without impacting core App functionality.
- **Functional Cookies:** Remember your preferences and settings to provide a personalized experience.
- **Analytics Cookies:** Help us understand aggregate usage patterns. We use privacy-respecting analytics tools configured to anonymize IP addresses.
- **Stripe Cookies:** Stripe sets cookies on our payment pages to enable fraud detection and secure payment processing. These are governed by Stripe's cookie policy.

You may manage cookie preferences through your browser settings or our in-app cookie consent manager. Disabling non-essential cookies will not affect your ability to use core subscription features.

7. Your Privacy Rights

Depending on your jurisdiction, you may have some or all of the following rights regarding your personal data:

- **Right to Access:** Request a copy of the personal data we hold about you.
- **Right to Rectification:** Request correction of inaccurate or incomplete data.
- **Right to Erasure:** Request deletion of your personal data, subject to legal retention obligations.
- **Right to Portability:** Receive your data in a structured, machine-readable format.
- **Request that we limit how we use your data in certain circumstances.** Right to Restrict Processing:

- **Right to Object:** Object to processing based on legitimate interests or for direct marketing purposes.
- **Right to Withdraw Consent:** Where processing is based on consent, withdraw it at any time without affecting the lawfulness of prior processing.
- **Right to Non-Discrimination (CCPA):** We will not discriminate against you for exercising your privacy rights.

To exercise any of these rights, please contact us at bentson@roseone.ai. We will respond to verified requests within 30 days (or as required by applicable law). We may need to verify your identity before processing your request.

8. Data Security

We implement industry-standard technical and organizational measures to protect your personal data against unauthorized access, alteration, disclosure, or destruction, including:

- TLS/SSL encryption for all data in transit
- AES-256 encryption for sensitive data at rest
- Role-based access controls limiting employee access to personal data
- Regular security assessments and penetration testing
- PCI-DSS compliant payment infrastructure through Stripe
- Multi-factor authentication for administrative access

In the event of a personal data breach that poses a risk to your rights and freedoms, we will notify the applicable supervisory authority within 72 hours and affected users without undue delay, as required by applicable law.

9. International Data Transfers

Our services are operated from The United States of America. If you are located outside this region, your data may be transferred to and processed in countries that may have different data protection laws than your own jurisdiction.

Where we transfer personal data from the European Economic Area (EEA), United Kingdom, or Switzerland to countries without an adequacy decision, we rely on appropriate safeguards such as Standard Contractual Clauses (SCCs) as approved by the European Commission, or other lawful transfer mechanisms. Stripe's cross-border transfers are governed by Stripe's own SCCs and Data Processing Agreement.

10. Children's Privacy

Our App is not directed to individuals under the age of 18. We do not knowingly collect personal data from minors. If we become aware that we have inadvertently collected personal data from a minor, we will take prompt steps to delete such data. If you believe we have collected data from a child, please contact us immediately at bentson@roseone.ai.

11. Third-Party Links and Services

The App may contain links to third-party websites or integrations with third-party services. This Privacy Policy does not apply to those third parties. We encourage you to review the privacy policies of any third-party services you access through our App. We are not responsible for the privacy practices of third parties.

12. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or for other operational reasons. When we make material changes, we will:

- Post the revised policy within the App with an updated Effective Date
- Notify registered users via email at least 30 days before material changes take effect
- Where required by law, seek your renewed consent

Your continued use of the App after the effective date of any updates constitutes acceptance of the revised Privacy Policy. We encourage you to review this page periodically.

13. Contact Us

If you have questions, concerns, or requests relating to this Privacy Policy or our data practices, please contact us:

Rose One LLC

Privacy Officer / Data Protection Contact

Email: bentson@roseone.ai

If you are located in the EEA or UK and believe we have not adequately addressed your privacy concerns, you have the right to lodge a complaint with your local data protection supervisory authority.

This document constitutes the complete Privacy Policy of Rose One.