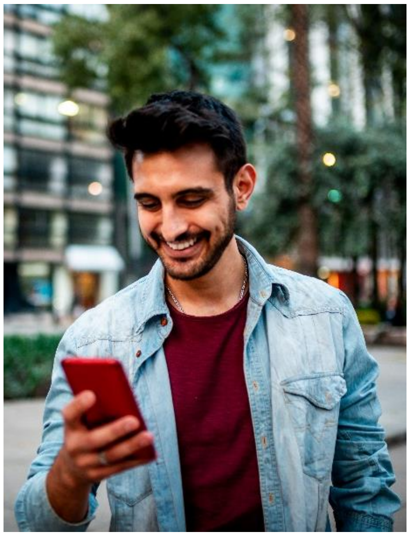
RingCentral®

RingCentral Artificial Intelligence Transparency Whitepaper



At RingCentral, customer trust is a priority and we have created this document to describe RingCentral's approach to trustworthy artificial intelligence (AI). The purpose of this document is to help our customers and partners understand RingCentral's approach to AI and how our products use and feature AI. This whitepaper may be helpful for customers to perform AI reviews or security and privacy impact assessments of RingCentral products and services.

RingCentral Services and Artificial Intelligence

RingCentral leverages proprietary and trusted third-party AI technologies to provide services and features to our users. These include AI intelligence features such as conversational intelligence, productivity and efficiency enhancements for the workplace, and sales intelligence. For example, RingCentral can generate summaries and highlights from recorded calls, and create action items and next steps, providing a seamless experience for call participants. RingCentral also uses AI to provide core features of RingCentral MVP such as protection from robocalls and SMS spam. For our events-focused services, RingCentral leverages AI to assist event hosts in creating descriptions of the events and organizing questions and answers.

RingCentral Artificial Intelligence Governance

RingCentral has developed an AI governance program to support and develop trustworthy AI while fostering customer-centric innovation. The program includes a cross-functional AI Governance Council and an internal AI Policy based on the NIST AI Risk Management Framework focused on core AI principles for development and deployment of AI solutions that further responsible and ethical use of AI.

Below are the core RingCentral principles for trustworthy AI and how we align with each:

- **Safe:** At RingCentral we believe AI-enabled systems should not endanger human life, property, privacy, or the environment.
- **Secure:** AI-enabled systems should maintain confidentiality, integrity, and availability through protection mechanisms that prevent unauthorized access and use.
- **Transparent:** Information about AI-enabled systems and their outputs should be available to users interacting with the systems.
- **Explainable and Interpretable:** AI-enabled systems should enable the provision of information that describes how they function.
- **Privacy enhanced:** AI-enabled systems should be developed and used in compliance with privacy laws and RingCentral privacy policies.
- **Fair:** Development and use of AI-enabled systems at RingCentral should consider equality and equity by addressing issues such as harmful bias and discrimination.

March 2024

AI Models and Customer Data

RingCentral may use proprietary and/or third-party AI models to provide RingCentral's AI features. RingCentral does not use customer data to train its AI models and does not allow our third-party vendors to use our customers' data to train the third-party's AI models. If the service or feature allows, customers may use their data to customize their experience when using AI within their account (i.e., using the customers' data to fine-tune the AI models within their environment), which may enhance their experience and increase efficiency when using the service.

We provide our customers with detailed information on how AI uses their data and for which purposes for each service in the relevant Product Privacy Datasheets on our Trust Center and Data Processing Addendum.

Third-Party Vendors

When RingCentral uses third-party vendors to provide AI functionalities or features, such as providing suggested descriptions of events or performing deal analysis, we apply a third-party risk management framework to assess vendors and to ensure proper contractual guarantees are provided before onboarding a vendor. We contract only with third-party service providers that provide equivalent levels of data protection and security as we provide. We do not permit our third-party vendors to use customer data to train or improve the third-party's AI underlying models.

For example, third-party AI systems used may depend on the service or feature, and include Microsoft Azure OpenAI, Google Translate and Google Speech-to-Text. Please visit the RingCentral Subprocessor List which identifies and describes third-party subprocessors, including AI vendors, as they are changed or added.

Customer Choices

RingCentral empowers account owners to make informed decisions about their selection of RingCentral AI enabled systems by way of clear notice of AI integration and opt-in capabilities. Additionally, at the individual user level, we provide user autonomy to leverage AI tools. For example, our products provide a feature for transcribing calls and meetings, which requires a user to affirmatively enable transcription. Once enabled, AI is used to turn speech into text which is then turned into a transcript. Should customers choose to enable this feature, a notice of transcription to call participants is provided so end users can make an informed decision to continue participation.

Automated Decision-Making and Human Review

RingCentral AI products are designed to include human review of outputs for accuracy, and customers should not use outcomes or metrics generated by the service to make decisions, for instance, concerning employment, creditworthiness or insurability. Please see RingCentral's Terms of Service and Acceptable Use Policy for more information about customer obligations to comply with applicable law in connection with using the services.

Bias

Assessing potential bias in our AI systems is a critical component of our development process. AI feature development should be balanced across demographic groups, and accessible to individuals with disabilities, and should not exacerbate existing disparities or systemic biases. RingCentral tests our AI features for potential bias and undesirable outputs, and tests for equality and accessibility of the tools across various demographics. Each AI feature and service is reviewed by our legal team and relevant stakeholders to assess the inclusiveness for all customers.

Security

RingCentral is committed to security and maintains technical, organizational, and contractual safeguards to protect customers' data processed by our services, including with AI capabilities. We apply the same security requirements for our AI products as we do for all our products.

RingCentral's approach to AI and security focuses on these tenets:

- AI use restrictions by RingCentral personnel
- Training model secure design restrictions to ensure separation of tenant level data and security from potential data poisoning attempts
- Operational security for access and management of the AI models

RingCentral's AI use requirements and restrictions cover proper licensing of AI solutions, what types of data may be used as inputs, scope of usage for AI system outputs internally, and use of source code from generative AI systems. With respect to training model restrictions, RingCentral's AI systems development standards set forth restrictions around AI model training, including data used for training, proper recordkeeping, storage, and access restrictions. Furthermore, RingCentral implements operational security for access to and management of backend resources to prevent access to data by unauthorized personnel or modifications without permission.

Please see our Security Addendum and our Trust Center for information on the general commitments we make to our customers about security.

Shared Responsibilities

Implementation of AI is a shared responsibility with our customers. While RingCentral has based the development of our services on the core principles for trustworthy AI as described above, customers also share a responsibility to use the products safely and securely, and to ensure human oversight into how the services are being used within their organization.

RingCentral is responsible for the architecture and security of the service and the physical and environmental security of the infrastructure employed to deliver our service. Customers likewise have responsibilities, including managing their configuration settings, account policies, granting the correct roles and permissions to users; properly implementing security features such as MFA/SSO; tracking administrative changes made on their RingCentral account; and working with RingCentral to identify suspicious activity. Ultimately, just as RingCentral is responsible for preventing disclosures of customer account information and call data, users are also responsible for preventing disclosures of their settings and their information.

Contact Us

Should you find an answer to your question missing from our various resources, feel free to contact us.

About This Whitepaper

The information provided in this Whitepaper does not constitute legal or professional advice, warranty of fitness for a particular purpose or compliance with applicable laws. RingCentral reserves the right to update this Whitepaper from time-to-time.

March 2024