RingCentral

RingCentral RingCX Service Privacy Datasheet

At RingCentral, we take the protection of personal data very seriously and have created this document to describe how RingCentral processes personal data when providing RingCX (the "Service" or "RingCX") to our customers. The purpose of this document is to help our customers and partners understand how the Service complies with privacy requirements and to provide them with background information that may be helpful to perform privacy reviews or privacy impact assessments of our Service.

Service Description

RingCX is a complete omnichannel contact center that manages all customer interactions across 20+ digital channels, voice, video, and AI-driven self-service (e.g., chatbots), and provides analytics and insights. RingCX integrates with and leverages RingEX for a more streamlined collaboration experience for agents. RingCX provides a unified dashboard to manage voice and digital interactions, real-time analytics and reporting, and advanced routing and queuing, among other key features. RingCX is available through the web-based application.

Data Collection

RingCX customer administrators set up each RingCX user, which include the RingCX customer's agents and managers ("RingCX User(s)"), through the RingEX platform. RingCX pulls the following information directly from RingEX: first and last names, email, extension number, time zone, language, home country code, time format, and regional data format. This information is used to provision the RingCX Users accounts. RingCX also collects personal data of RingCX Users through their use of the Service, which may include interaction recordings, interaction metadata, call summaries and transcripts, etc. RingCX does not push any information back to RingEX.

The Service also collects data about RingCX guests, which include the third parties interacting with our customers' agents through RingCX channels such as the customers of our customers ("RingCX Guests"). RingCX processes customer-generated content through all RingCX channels, including email, social media, RingCentral SMS/MMS, etc. The personal data processed about RingCX Guests through their use of the RingCX channels may include: interaction metadata, interaction recordings, digital interaction transcripts, call transcripts and call recording summaries, contact information (if provided by customer), etc.

RingCX also allows customer administrators to upload lists of RingCX Guests for marketing purposes and this information can include phone number and customer-provided unique ID in addition to any other information the customer chooses to include.

April 2024

Categories of Personal Data Processed by the Service

Categories of personal data processed for RingCX include Service account data, Service usage data, and customer generated content. The details of these data categories, including the AI inputs and outputs, for each category of data subject, and the purposes of processing are provided in Annex 1 of this document.

Special Categories of Data Processed by the Service

The Service uses the RingCX User's ID, where available, to associate the content of the communication with the RingCX User and does not rely on voiceprint or other biometric identifiers to identify the participants.

The Service is not designed to recognize and/or classify data as:
- Special categories of data or sensitive data (as defined in the GDPR or in other applicable data protection laws)
- Personal data concerning children or minors
- Data related to criminal convictions and offenses

Insofar as customers process special categories of personal data, customers undertake to process these categories of personal data lawfully, and in particular, to rely on a valid legal basis in accordance with applicable data protection laws.

Customer Choices for Data Processing

Opt-out of recordings

All calls are recorded by default unless the RingCX administrator disables this feature. If the RingCX administrator disables the feature, the options are: 1) to set automatic call recording for all calls and authorize the RingCX agent to pause the recording or start/stop the recording; or 2) to give RingCX agents the ability to record or not record from the outset of the call.

Use of Artificial Intelligence

The Service uses either RingCentral proprietary AI models and/or third-party AI services to provide some features of the Service. Please see our subprocessor list for more information regarding the third parties.

AI Model Training

We did not use RingCentral customer data to develop the RingCentral proprietary AI model. We do not use customer data to improve the proprietary AI model and do not permit our subprocessors to use customer data to improve their AI models.

How RingCX leverages AI to generate outputs

RingCX provides fully integrated summary and transcription features, which turn speech into text transcripts, which is then submitted to a third-party AI service to generate summaries. The third-party services do not retain any customer-generated content.

Third-Party Integrations

The customer may elect to implement a third-party integration, in which case the customer administrators can configure what data is pushed to and pulled from the third-party integration.

Access

Restricted Administrative Access by RingCentral

RingCentral accesses customer data to provide the Service (i.e., for customer support troubleshooting and remediation, product improvement, network management, network monitoring, and to provide customer analytics). We employ access control mechanisms which limit access to personal data to only those trained and authorized RingCentral and subprocessors' personnel who have a business need to access said data to perform RingCentral's Services. Such controls include multi-factor authentication (MFA), which is implemented for administrative access to the production environment, and Identity Access Management (IAM), which tightly controls access to RingCentral production environments.

Access by Customer Administrators and End Users

Customer Administrators can access data regarding the Service, including personal data, directly through the dedicated portal to administer user accounts and retrieve, update, or delete RingCX Users' personal data. RingCX Users may access certain of their personal data on the Service from the ServiceWeb portal.

How RingCentral Service Data Processing Fits with Data Protection Laws

Data Subject Rights

The Service provides technical means enabling customer administrators to take appropriate actions in response to requests from data subjects exercising their privacy rights. In addition, if RingCX users or guests submit a request through the RingCentral Data Subject Request Center we will direct them to contact the customer to exercise their rights.

Subprocessors

RingCentral uses other RingCentral affiliates and third-party service providers to assist in delivering the Service. RingCentral contracts only with third party service providers that provide equivalent levels of data protection and security as provided by RingCentral. For a current list of our subprocessors, please see the RingCentral Subprocessor List.

Data Deletion and Retention

Customer account data will be processed for up to 30 days during the term of the Service, or as otherwise required by law or agreed with the customers. Upon termination an account will be disabled on the last day of the billing cycle. Once the account is disabled, the account will be deleted within 30 days, unless otherwise agreed with the customers.

Location of Data Storage

RingCentral data centers where we store personal data as part of the Service are located in the following countries.

Customer account location*	Service account data	Usage data	Customer-generated content
United States	United States	United States	United States
United Kingdom	United States and United Kingdom	United States and United Kingdom	United Kingdom
Europe	United States and Germany	United States and Germany	Germany

* The customer account location is determined by the customer's contracting entity.

Transparency

RingCentral processes personal data both as a controller and as a processor for the purpose of the Service.

The processing activities by RingCentral acting as a data controller are subject to the [RingCentral Privacy Notice](#). Additional information related to RingCentral as a data controller is provided in our [RingCentral as a Data Controller Whitepaper.](#)

Processing activities performed by RingCentral acting as processor on behalf of our customers are governed by the [RingCentral Data Processing Addendum](#) (DPA) incorporated into the RingCentral Master Service Agreement (MSA).

Cross-Border Transfers

RingCentral may transfer and process customer personal data outside the European Economic Area ("EEA"), Switzerland, or the United Kingdom, to locations where RingCentral, its affiliates or its subprocessors maintain data processing operations. Please see the [RingCentral Personal Data Transfer FAQ](#) for more information

With respect to transfers out of the EEA, United Kingdom, and Switzerland to the United States, RingCentral has self-certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles), the UK Extension to the EU-U.S. DPF (UK Extension), and the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles), respectively. Please see our [Notice of Certification](#) for more information.

To the extent that RingCentral processes (or causes to be processed) any personal data originating from the EEA, Switzerland, or the United Kingdom in a country that has not been recognized by competent authorities as providing an adequate level of protection for personal data, RingCentral relies on the European Commission's Standard Contractual Clauses, its additional safeguards, and the additional Swiss and UK-specific clauses, to transfer such personal data.

Automated Decision-Making

The Service is not designed to make any decision based solely on automated processing, particularly those that produce legal effects on individuals.

Security Measures

RingCentral is committed to security and has implemented technical, organizational, and contractual safeguards to protect the data of customers. Please see our [Security Addendum](#) and our [Trust Center](#) for information on the commitments we make to our customers about security.

About This Datasheet

The information provided in this Datasheet 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 datasheet from time-to-time.

Annex 1: Categories of Personal Data processed by the Service

Ring CX Administrator

Category of Personal Data	AI Processing	Purpose of Processing
Service account data • Login • Name • Email address • Extension number • User ID • Application settings	None	• Create a customer account • Provide access to the Service and configuration of associated features • Enable Service administration • Enable access to information relating to the Service, such as usage and adoption • Respond to support requests • Provide Service-related notifications
Usage data • Device and operating system information (such as device and operating system type, client version, IP address and ISP, etc.) • System logs, including usage logs (e.g., audit logs of admin activity), backend logs, client logs • Cookie identifiers	None	• Provide access to the Service and configuration of associated features • Enable Service administration • Enable access to information relating to the Service, such as usage and adoption • Respond to support requests • Provide Service-related notifications

RingCX User (customer's agents and/or managers)

Category of Personal Data	AI Processing	Purpose of Processing
Service account data • Name • Email address • RingCX User ID • RingEX account extension ID • Application settings	None	• Set up RingCX User accounts • Provide access to the Service and configuration of associated features • Enable provision of the Service • Respond to support requests • Provide Service-related notifications • Monitor and improve the quality of the Service • Conduct analytics for customers • Conduct business intelligence • Comply with applicable laws, including those regulating CDRs • Perform billing for the Service
Usage data • Device information (such as IP address, ISP, device type, operating system and client version, type of microphone or speakers, etc.) • System logs, including usage logs, backend logs, client logs • Cookie identifiers • Interaction metadata (e.g., call queue, whether call was transferred) • Communication metadata (e.g., CDRs, traffic data, originating and terminating, numbers called date and time, duration of calls) • Quality of Service data	None	• Provide access to the Service and configuration of associated features • Enable provision of the Service • Respond to support requests • Provide Service-related notifications • Conduct analytics for customers • Conduct business intelligence • Comply with applicable laws, including those regulating CDRs • Perform billing for the Service
User-generated content • RingCX Users' names • Interaction recordings (e.g., emails, social media posts, call recordings, chat, etc.) • Summaries of call recordings • Transcripts • Any information processed by third-party integrations chosen by the customer	• RingCX Users' names (input) • Interaction recordings (input) • Transcription (output) • Summaries (output)	• Enable provision of the Service • Respond to support requests • Comply with applicable laws, including those regulating CDRs

RingCX Guest

Category of Personal Data	AI Processing	Purpose of Processing
Guest data • Login • Name • Email address • Extension number • User ID • Application settings	None	• Create a customer account • Provide access to the Service and configuration of associated features • Enable Service administration • Enable access to information relating to the Service, such as usage and adoption • Respond to support requests • Provide Service-related notifications
Usage data • Device and operating system information (such as device and operating system type, operations system and client version, IP address and ISP, etc.) • System logs, including usage logs (e.g., audit logs of admin activity), backend logs, client logs • Cookie identifiers	None	• Provide access to the Service and configuration of associated features • Enable Service administration • Enable access to information relating to the Service, such as usage and adoption • Respond to support requests • Provide Service-related notifications