RingCentral MVP Service Privacy Data Sheet

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 RingCentral MVP (the “Service”). 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

RingCentral MVP is a cloud-based service powered by the market-leading RingCentral unified communications platform. It combines reliable high-quality team messaging, virtualized modern online video meetings, and an enterprise-grade VoIP phone system into one seamless, secure, and collaborative online hub. The Service can be used on any device through the browser, desktop or mobile app.

Data Collection

In connection with the Service, personal data may be collected either directly from data subjects or automatically through the Service. For instance, data about users is provided when system administrators set up accounts and when users are added to an account. Data, especially on Service usage, is collected also when users or system administrators use the Service. We collect data also when users or system administrators request support.

Categories of Personal Data Processed by the Service and Purpose of Processing

Categories of personal data processed for each component of MVP are broken down into the three tables below.

Messaging

Categories of Data Subjects	Categories of Personal Data	Purpose of Processing
Customer Administrators	Business contact information: • Login credentials (user ID, log in, account, passwords) • Name • Physical address (admin only) • Telephone number (fixed and mobile) • Email address • Title (if provided) • Role (if provided) • Company • Profile picture (if provided)	• Create a customer account • Provide the Service • Enable Service administration • Enable access to information relating to the Service, such as usage, adoption, and quality • Respond to support requests and provide notifications • Promote additional products or services to the customer, as permitted by applicable law
Customer end users, including customer's employees and authorized users of the Service	Account setting data: • Name • Email address • Phone number • Profile picture (if provided) • Location by country • Login credentials (user ID, log in, account, passwords)	• Set up customer end user accounts • Provide access to the Service and associated features • Enable provision of the Service • Communicate with end users • Respond to support requests and provide notifications • Conduct analytics with aggregated data • Monitor and improve the quality of the Service
Customer end users, including customers' employees and authorized users of the Service	Usage data: • Internet Protocol (IP) address and Internet Service Provider (ISP) • Device and operating system information (such as device and operating system type, operations system and client version, etc.) • User feedback ratings • Usage logs	• Provide the Service • Provide customer analytics using aggregated data about the Service • Respond to support requests and provide notifications • Monitor and improve the quality of the Service • Monitor security of the network

Messaging

Categories of Data Subjects	Categories of Personal Data	Purpose of Processing
Customer end users, including customers' employees and authorized users of the Service	• Cookie identifiers • Traffic data • Fraud data • Metadata (such as session logs, etc.) • Quality of Service data	• Conduct fraud and threat analysis, and detect and prevent spam or unlawful or abusive activity or other violations of our Authorized Usage Policy • Comply with applicable laws, including those regulating CDRs • Perform billing for the Service
All end users, including: • Customer's employees and authorized users of the Services Email address • Other individuals that are part of the communications taking place through the Service • Individuals whose personal data is included in the customer-generated content of the communications	Customer generated content: • Messages • Shared files, pictures, and links • Message attachments, such as notes, tasks, events, code snippets, and .gifs	• Enable the transmission of the content • Store content • Maintain records of communications as requested by the user • Respond to support requests and provide notifications

Video

Categories of Data Subjects	Categories of Personal Data	Purpose of Processing
Customer administrators	Business contact information: • Login credentials (user ID, log in, account, passwords) • Name • Email address • Physical address (admin only) • Telephone number (fixed and mobile) • Title (if provided) • Role (if provided) • Company • Profile picture (if provided)	• Create a customer account • Provide the Service • Enable Service administration • Enable access to information relating to the Service, such as usage, adoption, and quality • Respond to support requests and provide notifications • Promote additional products or services to the customer, as permitted by applicable law

Video

Categories of Data Subjects	Categories of Personal Data	Purpose of Processing
Customer end users, including customer's employees and authorized users of the Service	Account data: • Name, email address, phone number, address • Profile picture (if provided) • URL (to locate and join the meeting) • IP addresses • MAC addresses • Other forms of personal data collected on behalf of the relevant customer such as title, role, organization • Login credentials (user ID, log in, account, passwords)	• Set up customer end user account • Provide access to the Service and associated features • Enable provision of the Service • Communicate with users • Respond to support requests and provide notifications • Conduct analytics with aggregated data • Monitor and improve the quality of the Service
All end users, including: • Customers' employees and authorized users of the Services • Other individuals that are part of the of communications taking place through the Service • Individuals whose personal data is included in the customer-generated content of the communications	Customer generated content: • Any content shared by users during video meetings • Access tokens for calendar integration • Avatars and profile pictures • Audio/video streams • Transcriptions of meeting (closed captions) • Meeting notes • Cloud recordings • Meeting history • Delegates and delegator's relationships • Participants' names • Meeting recordings • Call logs (originating and terminating, numbers called date and time) • Chat messages • Analytics reports • Application settings	• Provide the Service • Respond to support requests and provide notifications • Generate analytics reports as requested by customer • Store meeting recordings, including transcripts and notes • Maintain records of meeting as requested by the user

Video

Categories of Data Subjects	Categories of Personal Data	Purpose of Processing
End users, including: • Customers' employees and authorized users of the Service • Other individuals that are part of the communications taking place through the Service	Usage data: • Service usage data – IP address and ISP – Device and operating system information (such as device and operating system type, operations system and client version, etc.) – User feedback ratings – Usage logs – Cookie identifiers – Traffic data – Fraud data – Metadata (such as session logs, etc.) • Quality of Service data • Call Detail Records	• Provide the Service • Respond to support requests and provide notifications • Monitor and improve the quality of the Service • Conduct analytics using aggregated data • Monitor security of the network • Conduct fraud and threat analysis, and detect and prevent spam or unlawful or abusive activity or other violations of our AUP • Comply with applicable laws, including those regulating CDRs • Perform billing for the Service

Phone

Categories of Data Subjects	Categories of Personal Data	Purpose of Processing
Customer administrators	Business contact information: • Login credentials (user ID, log in, account, passwords) • Name • Email address • Physical address (admin only) • Telephone number (fixed and mobile) • Title (if provided) • Role (if provided) • Company • Profile picture (if provided)	• Create a customer account • Provide the Service • Enable Service administration • Enable access to information relating to the Service, such as usage, adoption, and quality • Respond to support requests and provide notifications • Promote additional products or services to the customer, as permitted by applicable law

Phone

Categories of Data Subjects	Categories of Personal Data	Purpose of Processing
Customer end users, including customer's employees and authorized users of the Service	Account data: • Name • Email address • Phone number • Physical address • Title (if provided) • Company • Profile picture (if provided) • Login credentials (user ID, log in, account, passwords) • Emergency address	• Set up customer end user account • Provide access to the Service and associated features • Enable provision of the Service • Communicate with users • Respond to support requests and provide notifications • Conduct analytics with aggregated data • Monitor and improve the quality of the Service • Emergency call routing

	Usage data:
	• Internet Protocol (IP) address
	• MAC address
	• Other device ID (UDID), device type
	• Operating system type and version, client version, type of microphone or speakers
	• Connection type and related information
	• Traffic data
	• Internal feature usage analytics, usage logs, cookie identifiers
	• Call Detail Records (CDRs)
	• Call metadata including:
	  – User ID
	  – Phone numbers
	  – Numbers dialed
	  – Session logs
	• Access log data including: IP address, browser type, operating system, data/time stamp
	• Fraud data such as blacklist history of previous frauds and security logs
		• Provide the service
		• Provide customer facing dashboards and reports
		• Respond to support requests and provide notifications
		• Monitor and improve the quality of the Service
		• Monitor performance of data centers and networks
		• Conduct analytics to improve RingCentral's website, app and service performance
		• Monitor security of the network
		• Conduct fraud and threat analysis, and detect and prevent spam or unlawful or abusive activity or other violations of our AUP
		• Comply with applicable laws, including those regulating CDRs
		• Perform billing for the Service

Phone		
Categories of Data Subjects	**Categories of Personal Data**	**Purpose of Processing**
All end users, including: • Customers' employees and authorized users of the Services • Other individuals that are part of the communications taking place through the Service • Individuals whose personal data is included in the customer-generated content of the communications	Customer generated content: • Text of inbound and outbound faxes • Voicemails • Text of inbound and outbound SMS • Call Recordings (automatic or on demand)	• Enable communications between end users • Provide voicemail delivery and transcription service • Store customer-generated content as requested by users • Respond to support requests and provide notifications

Special Categories of Data Processed by the Service

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), nor as personal data concerning children or minors, or as 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.

Security Measures and Certifications

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

Independent Verification

The Service undergoes independent verification and audits of security controls by major partners and third parties to meet regulatory and compliance needs. Current list of certificates and reports is the following: ISO 27001; ISO 27017 & ISO 27018; SOC2+ FINRA CSR, HIPAA; SOC3, PCI (as a merchant); HITRUST; McAfee Enterprise-Ready; C5 (Cloud Computing Compliance Controls Catalog); and Cyber Essentials Plus.

Confidential reports are available upon request to your Account Manager or Sales Representative and for current customers via the self-service Trust Portal. Additional information about our current certifications, attestations, and adherence to global compliance frameworks can be found on our Trust Center.

Access

Restricted Administrative Access by RingCentral

We access personal 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 in order to enable RingCentral to perform its obligations towards customers. 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

Customers can access data regarding the Service, including personal data, directly through the dedicated portal to administer user accounts and retrieve, update, or delete the personal data of end users. End users may access their personal data on the Service from the ServiceWeb portal.

Data Subject Rights

The Service provides technical means enabling customer's administrators to take appropriate actions in response to requests from data subjects exercising their privacy rights. In addition, if end users 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 & Retention

Customer personal data will be processed for the term of the Service, or as otherwise required by law or agreed with our 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 our customer. For more information, please refer to RingCentral Data Retention Policies.

Location of Data Storage

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

Messaging	Video	Phone
• US • Germany	• US • Canada • Germany • United Kingdom	• US • Canada • Germany • The Netherlands • Switzerland • United Kingdom

The country associated with customer's accounts determines in which region customer generated content, traffic data, and CDRs are stored.

How RingCentral Service Data Processing Fits with Data Protection Laws in Europe

Transparency

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

The processing activities performed by RingCentral acting as controller are subject to RingCentral Privacy Notice available here.

The processing activities performed by RingCentral Inc. and/or its affiliates acting as processor on behalf of its customers are governed by the RingCentral Data Processing Addendum incorporated into RingCentral Master Service Agreement.

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. 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. Please see the RingCentral Personal Data Transfer FAQ for more information.

Automated Decision-Making

The Service is not designed to create decisions based on automated decision making (i.e. making a decision by automated means without any human involvement) or profiling (i.e. analyzing aspects of an individual's personality, behavior, interests and habits to make predictions or decisions about them).

Additional Resources

Trust Center - Privacy	Location of all customer facing privacy resources.
Privacy and Data Protection at RingCentral	Our Privacy White Paper. Describes data protection policies, processes, and controls established and operated by RingCentral.
Transparency Report	White Paper detailing how we respond to various government requests for personal data. We publish a new report each year.
Privacy Notice	Details what data we collect, how we use the data, etc., in alignment with applicable laws and best practices.
Customer Data Processing Addendum (DPA)	Our data processing addendum for customers.
RingCentral Subprocessor List	A current list of subprocessors for RingCentral.
RingCentral as a Data Controller White Paper	Information related to RingCentral acting as data controller.
Global Data Transfers	Webpage with a collection of resources on international data transfers.
Personal Data Transfer Impact Assessment FAQ	Information for customers on RingCentral's data transfers and the measures that RingCentral has put in place with respect to those transfers.
RingCentral Data Retention Policies	Information on RingCentral's Data Retention Policies.
Privacy Regulations Worldwide	Webpage with a collection of resources that detail how RingCentral complies with country-specific privacy regulations around the world.
RingCentral Data Subject Request Center	Portal for end users that wish to exercise their data subject rights.
Children's Privacy Notice	Privacy notice that specifically addresses the privacy concerns around children who may be using our products.
Cookie Notice	Details on types of cookies we use, and how customers can manage cookie preferences.
Security Addendum	Information on the promises 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 Data Sheet from time-to-time.

For more information, please contact a sales representative. Visit ringcentral.com or call 855-774-2510.

RingCentral, Inc. (NYSE: RNG) is a leading provider of business cloud communications and contact center solutions based on its powerful Message Video Phone™ (MVP®) global platform. More flexible and cost effective than legacy on-premises PBX and video conferencing systems that it replaces, RingCentral empowers modern mobile and distributed workforces to communicate, collaborate, and connect via any mode, any device, and any location. RingCentral offers three key products in its portfolio including RingCentral MVP™, a unified communications as a service (UCaaS) platform including team messaging, video meetings, and a cloud phone system; RingCentral Video®, the company's video meetings solution with team messaging that enables Smart Video Meetings™; and RingCentral cloud Contact Center solutions. RingCentral's open platform integrates with leading third-party business applications and enables customers to easily customize business workflows. RingCentral is headquartered in Belmont, California, and has offices around the world.

RingCentral

RingCentral, Inc. 20 Davis Drive, Belmont, CA 94002. ringcentral.com

1131393641 06/23