RingCentral

GDPR Compliance Guide

March 2023

As a leading global communications and collaboration cloud service provider, RingCentral is committed to processing customer personal data in compliance with applicable data protection laws.

In this whitepaper we provide key information to allow our customers and prospects to assess the compliance of our services with the General Data Protection Regulation (GDPR) when we process data on their behalf as a data processor.

It is important to note that as an electronic communications service provider, RingCentral acts both as a data controller and as a data processor. For more information about our data processing as a data controller, please see our whitepaper, RingCentral as a Data Controller.

RingCentral Privacy Program, the Foundation of our Compliance	RingCentral relies on its Privacy and Data Protection Program to ensure the compliance of its services, policies and processes with the GDPR and other applicable data protection laws. The pillars of RingCentral Privacy and Data Protection Program include:

Accountability

The office of the Chief Privacy Officer establishes policies and procedures necessary to comply with applicable privacy laws. All personnel at Ringcentral are accountable for complying with privacy requirements. Our Privacy Program includes regular mandatory and tailored Privacy and Data Protection training for all RingCentral personnel.

We process Personal Data only on lawful bases in compliance with applicable legal requirements, including with data subjects' consent when required.

We have established a network of Privacy Champions to promote a strong privacy culture throughout the RingCentral organization. The Privacy Champions are key to ensure distributed accountability for privacy.

Transparency

RingCentral is committed to provide full transparency about its privacy and data protection practices. In our Trust Center we provide extensive information to our customers and users about the processing activities pursued by RingCentral in the provision of our services.

Privacy by Default and Design - Data Minimisation

We have developed a robust privacy by design program that allows us to ensure implementation of privacy by default and by design principles, and in particular data minimisation.

Categories of Personal Data Processed as part of RingCentral Services

The RingCentral services involve the processing of three categories of personal data as follows:

1. Account information: relates to all data that allows the identification of customers, account administrators, and end-users.

2. Customer-generated content: relates to *any* customer-generated content that users include in their communications.

3. Usage and traffic data and customer-facing analytics: relates to data about calls made, including Call Detail Records

	(CDRs).
Data Storage and Services Operated in Europe	We offer to our Europe-based customers storage of both their customer generated content, usage, and traffic data in Europe. The RingCentral Europe-based storage infrastructure is managed and supported locally within Europe. In addition, RingCentral Customer Analytics data are processed in Europe.
RingCentral Data Processing Addendum	We offer to our customers a Data Processing Addendum that allows them to meet their obligations in compliance with the requirements of GDPR Article 28. Our Data processing Addendum is available in several languages.
Subprocessors	RingCentral relies on third party service providers as part of the performance of its services. We provide full transparency on subprocessors our Subprocessor List and FAQ. We have selected these subprocessors following a rigorous and thorough qualification process including in-depth privacy and security assessment. We ensure that all our subprocessors are bound by data processing terms aligned with GDPR Article 28 requirements that provide obligations equivalent to those agreed to with our customers.
Data Transfers Outside the EEA, the UK and Switzerland	Only account information is stored outside Europe. Transfers to and remote access from outside Europe of customer generated content, usage data, and traffic data are limited. They are allowed only to enable specific functionalities and to provide customer support services. When it is necessary to transfer personal data to third countries, RingCentral is committed to comply with GDPR and applicable data protection laws on the transfer of personal data. When transferring personal data out of the EEA, UK, and Switzerland we rely on the applicable 2021 EU Standard Contractual Clauses (SCCs) and we have put measures in place to ensure that the transferred personal data remain protected. RingCentral has performed and maintains data transfer risk assessments relating to the transfer and remote access of personal data from outside the EEA, UK, and Switzerland. As a result,

	RingCentral implements additional security measures to ensure that the personal data we need to transfer are being adequately protected. For more information about how RingCentral protects the personal data it transfers, please refer to the Personal Data Transfer Impact Assessment FAQ. Customers based outside Europe can rely on our Customer Data Transfer Agreement that includes the 2021 SCCs as well as the UK IDTA.
Enhanced Encryption	RingCentral also protects customer data against third countries government access as appropriate through a combination of measures, including encryption in transit using TLS encryption, encryption at rest, SRTP for securing voice communication, and E2EE for RCV meetings as enabled by the account owner. More information about our enhanced encryption techniques can be found on our Trust Center.
Transparency Report	RingCentral is committed to maintaining the privacy and trust of our customers by giving full visibility into required disclosures to government agencies. Our annual Transparency Report describes how we respond to requests for customer data submitted by law enforcement and government agencies around the world. For any questions related to our Transparency Report, please contact privacy@ringcentral.com.
Data Subject Rights	Our services allow customers to submit and manage their data subject rights requests directly and easily through the administration platform. Customers can contact RingCentral customer support for assistance. Additionally, data subjects can exercise their rights by submitting their request to the RingCentral Data Subject Request Center.
Uncompromised Security	RingCentral has put security, privacy, and compliance at the center of its infrastructure investments and innovation strategy to make RingCentral's unified cloud communications platform among the most

	reliable and secure on the market. Please can see the full list of our independent certifications. RingCentral technical and organizational security measures are described in detail in our Security Addendum included as part of RingCentral Data Processing Addendum. The latest news and information about our Security program is available on our Security Trust Center.
External Data Protection Officer	RingCentral has appointed an external Data Protection Officer to guarantee an independent and impartial insight into its privacy and data protection practices. RingCentral DPO contact details are: HewardMills Ireland Ltd. Fitzwilliam Hall, Fitzwilliam Place, Dublin 2 DO2 T292 Ireland privacy@ringcentral.com
More Resources	Trust Center: https://www.ringcentral.com/trust-center.html#privacy
Contact Us	RingCentral Privacy Department: privacy@ringcentral.com

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