Previous versions of the RingCentral Customer DPA: 2024, 2023, 2022, 2021

RingCentral Data Processing Addendum

This Data Processing Addendum (DPA) is made by and between RingCentral and Customer (each a "**Party**", together the "**Parties**"), and is supplemental to the agreement executed between the Parties to which it is attached ("**Agreement**") for the provision of the Services to Customer.

This DPA applies to the Services ordered by Customer after the date in the footer. RingCentral may update the terms of the DPA as needed in accordance with the Agreement ("Updated DPA") and, unless otherwise specified in an Order Form, the Updated DPA will apply to the Services ordered by Customer (including renewals) following the date mentioned in the Updated DPA.

1. Definitions

Capitalised terms used but not defined in this DPA have the same meanings as set out in the Agreement.

1.1 For the purposes of this DPA:

(a) "**Affiliate**" means a person or entity that is controlled by a Party hereto, controls a Party hereto, or is under common control with a Party hereto, and "control" means beneficial ownership of greater than fifty percent (50%) of an entity's then-outstanding voting securities or ownership interests.

(b) "**Agreement**" means the main written or electronic agreement between Customer and RingCentral for the provision of any of the RingCentral Services.

(c) "**Applicable Data Protection Laws**" means all data protection and privacy laws (including the GDPR) applicable to RingCentral in the processing of Personal Data under this DPA.

(d) "**Controller**" shall have the same meaning under Applicable Data Protection Law.

(e) "**Customer Personal Data**" means any Personal Data that RingCentral processes as a Processor under the Agreement.

(f) "**Personal Data**" means any information relating to an identified or identifiable natural person, as defined by Applicable Data Protection Law.

(g) "**GDPR**" means (i) the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (ii) any Applicable Data Protection Laws implemented by European Union member states, (iii) the UK Data Protection Act (DPA 2018), as amended, and the GDPR as incorporated into UK law as the UK GDPR, and (iv) the Swiss Federal Acts on Data Protection (the "FADP"); all as amended from time to time.

(h) **"Processor"** shall have the same meaning under Applicable Data Protection Law.

(i) "**Security Incident**" means a breach of security leading to any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Customer Personal Data that compromises the privacy, security, or confidentiality of such Personal Data.

(j) **"Services"** means the RingCentral services as described in Annex I.

2. Scope of DPA

2.1 This DPA will apply to the extent that RingCentral processes Customer Personal Data on behalf of a Customer as a Processor, where such processing is further detailed in Annex 1. Any processing of Personal Data as a Controller by RingCentral is out of scope of this DPA.

3. Roles and Responsibilities

3.1 Parties' Roles. As between the Parties and for the purposes of this DPA, Customer shall be the Controller of the Customer Personal Data processed by RingCentral under the Agreement as a Processor. RingCentral will comply with the obligations of a Controller to the extent it processes Personal Data as a Controller for RingCentral's legitimate business purposes, including as necessary for the operation of the Services, and as necessary to comply with applicable law.

3.2 Obligations of the Customer. Customer undertakes to:

(a) Ensure that it may lawfully disclose the Customer Personal Data to RingCentral for the purposes set out in the Agreement.

(b) Comply with applicable data protection laws in its use of the Services, and its own collection and processing of Personal Data including Customer Personal Data. Customer acknowledges and confirms, as relevant, that Customer has informed its employees (current and future) and its works council as applicable, that as part of the Services, Customer has access to the traffic data; and

(c) Process special categories of Personal Data or sensitive data (as defined by Applicable Data Protection Laws), or Personal Data concerning children or minors, or related to criminal convictions and offences, lawfully and relying on a valid legal basis in accordance with Applicable Data Protection Laws. The Parties acknowledge that the Services are not designed to recognize and/or classify such data.

3.3 Purpose Limitation.

Except where otherwise required by applicable law, RingCentral shall process the Customer Personal Data (i) in accordance with Customer's documented instructions (which instructions are set out in the Agreement, this DPA and Customer's configuration and use of the Services, in accordance with the applicable terms of use), (ii) for the purposes of providing, monitoring, supporting, improving, and maintaining the Services. Where required by Applicable Data Protection Laws, RingCentral will promptly inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Laws.

3.4 Confidentiality of Processing. RingCentral shall ensure that any person that it authorises to process the Customer Personal Data shall be subject to a duty of confidentiality (either a contractual or a statutory duty).

3.5 Security. RingCentral will maintain appropriate technical and organisational security measures to safeguard the security of Customer Personal Data. RingCentral's security measures are set out in the RingCentral Security Addendum. RingCentral will maintain an information security and risk management program based on commercial best practices to preserve the confidentiality, integrity and accessibility of Customer Personal Data with administrative, technical and physical measures conforming to generally recognized industry standards and practices.

3.6 Security Incidents. Upon becoming aware of a Security Incident, RingCentral shall notify Customer without undue delay at the contact information that Customer has provided in the Administrative Portal and shall provide such timely information as Customer may reasonably

require, including to enable Customer to fulfil any data breach reporting obligations under Applicable Data Protection Laws.

3.7 Provision of Security Reports. RingCentral will select an independent, qualified third-party auditor to conduct, at RingCentral's expense, at least annual audits of the security of the Services and environments, in accordance with internationally recognized standards such as ISO27001, the SOC 2, Type II standards or its equivalent. Upon Customer request and under Non-Disclosure Agreement, RingCentral will provide a copy of the most recent audit reports (or similar security attestation) to document compliance with the foregoing requirement, where such certification is available. Such audit report is RingCentral's Confidential Information and Customer will not distribute to any third party without RingCentral's written approval.

3.8 Audits.

(a) Both Parties acknowledge that it is the Parties' intention ordinarily to rely on the provision of the security reports at Section 3.7 above to verify RingCentral's compliance with this DPA.

(b) Additionally, upon request from Customer, but not more than once during each twelve (12) month period, RingCentral shall complete a Customer provided information security program questionnaire, limited in scope to the actual services/environments related to the Services provided to Customer (**"Security Review"**).

(c) After Customer's review of RingCentral's audit report or similar attestation, and of the completed information security questionnaire (including any changes introduced by RingCentral to address any gaps), if, to the extent required by Applicable Data Protection Laws, additional information is reasonably necessary to demonstrate compliance with RingCentral's obligations pursuant to Applicable Data Protection Laws and this DPA, Customer may request in writing to perform an audit (including inspections) of RingCentral pursuant to the audit request procedure below, no more than once every twelve (12) month period, unless a supervisory authority specifically requires that an audit is carried out of RingCentral or in response to a Security Incident.

(d) In order to exercise its right to audit pursuant to this section, Customer must provide RingCentral with a written, detailed request, including the explanation of gaps in RingCentral's provided audit reports and in the Security Review that render the audit necessary to demonstrate RingCentral's compliance with this DPA or with applicable law.

(e) The audit may be performed by Customer or a third-party auditor (any such third party under strict confidentiality obligations, including requirements that individual auditors appointed have not performed audits of any of RingCentral's competitors in the previous twelve (12) months and that they will be prohibited from performing such audits in the twelve (12) months following RingCentral's audit) solely at Customer's expense. RingCentral may object in writing to any third-party auditor if the auditor is, in RingCentral's reasonable opinion, not suitably qualified or independent, a competitor of RingCentral, or otherwise manifestly unsuitable. Any such objection by RingCentral will require the Customer to appoint another auditor or conduct the audit itself.

(f) RingCentral and Customer will agree in advance upon the scope and timing of the audit, not to occur sooner than thirty (30) days from the date of the written request for an onsite audit under 3.8 (d), to protect the confidential and proprietary Information of RingCentral and other Parties, to minimise disruption to RingCentral's business, to limit

the scope to the actual services/environments related to the Services provided to Customer under the Agreement, and to agree on a reasonable duration of the audit. In the event the Customer requests to perform an on-site audit, Customer agrees that RingCentral charges a reasonable fee for costs incurred in connection with such on-site audit based on RingCentral's professional services rates, unless the audit shows an evidenced material breach on the part of RingCentral. RingCentral will provide the Customer with details of any applicable fee, and the basis of its calculation, in advance of any such audit.

(g) The audit performance will occur during regular business hours for the RingCentral personnel involved and the Parties agree that RingCentral will make available material for Customer's review, but not for Customer to retain.

(h) RingCentral will investigate, prioritize, and remediate in a timeframe defined by industry best practices any findings identified through these assessments, taking into consideration RingCentral Services and security framework requirements.

(i) All information provided or made available to Customer pursuant to this section shall be deemed Confidential Information of RingCentral.

3.9 Cooperation and Data Subjects' Rights. It is the Customer's responsibility to respond to any data subject request. Some of the RingCentral Services may provide direct technical means to enable Customer to fulfil its duties to respond to requests from data subjects under Applicable Data Protection Laws. If Customer is unable to address the data subject's request through such technical means, or where such functionality is not available, RingCentral shall, taking into account the nature of the processing, provide reasonable assistance to Customer, to enable Customer to respond to such data subject requests. In the event that such request is made directly to RingCentral, RingCentral shall promptly direct the data subject to contact the Customer.

3.10 Deletion or Return of Data. Upon termination or expiry of the Agreement, RingCentral shall delete Customer Personal Data (including copies) in RingCentral's possession or, at Customer's request, provide options to return the Personal Data to the customer, save to the extent that RingCentral is required by applicable law to retain some or all of the Customer Personal Data.

4. Data Processing Obligations

4.1 Subprocessors. Customer agrees that RingCentral and its Affiliates may engage RingCentral Affiliates and third- party subprocessors (collectively, "**Subprocessors**") to process the Personal Data on RingCentral's behalf. Depending on the scope and the nature of the subprocessing, RingCentral shall impose data protection terms on such Subprocessors that protect Customer Personal Data to an equivalent standard provided for by this DPA and shall remain liable for any breach of the DPA caused by a Subprocessor. The Subprocessors engaged by RingCentral in respect of each of the Services at the time of the Agreement are noted on the RingCentral Subprocessor list available at https://www.ringcentral.com/legal/dpa-subprocessor-list.html, or are otherwise specified in the Agreement.

4.2 Subprocessor Notification. RingCentral may, by giving reasonable notice to the Customer, add or replace the Subprocessors. If the Customer objects to the appointment of an additional Subprocessor within thirty (30) calendar days of such notice on reasonable grounds relating to the protection of the Customer Personal Data, then the Parties will discuss such concerns with a view to achieving resolution. If such resolution cannot be reached, then RingCentral will either not appoint the Subprocessor or, if this is not possible, Customer will be entitled to suspend or

terminate the affected RingCentral Service without penalty with a thirty (30) day written notice to RingCentral. Notwithstanding the foregoing, in the event of an unforeseeable force majeure (such as a RingCentral Subprocessor failure) that can provoke a degradation or interruption of the Service, RingCentral reserves the right to immediately change the failing Subprocessor in order to maintain or restore the standard conditions of the Service. In this situation, the notification of Subprocessor change may be exceptionally sent after the change.

4.3 Data Protection Impact Assessments. RingCentral shall, to the extent required by the GDPR, and upon Customer's request and at Customer's expense, provide Customer with reasonable assistance with data protection impact assessments or prior consultations with data protection authorities that Customer is required to carry out under GDPR in relation to the scope of the Services provided to Customer under the Agreement.

4.4 International Transfers. RingCentral may transfer and process Customer Personal Data outside the European Economic Area (**"EEA"**), Switzerland, or the United Kingdom, in accordance with the applicable Subprocessor list, to locations where RingCentral, its Affiliates or its Subprocessors maintain data processing operations.

(a) *Data Privacy Framework.* RingCentral complies with and has certified to the U.S. Department of Commerce its adherence to the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF). RingCentral's Notice of Certification applies to the Services.

(b) *Standard Contractual Clauses.* To the extent that RingCentral processes (or causes to be processed) any Customer Personal Data originating from the EEA, Switzerland, or the United Kingdom in a country that has not been recognized by the European Commission as providing an adequate level of protection for Customer Personal Data, and that the Data Privacy Framework as described above does not apply, RingCentral will put in place such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Laws, which include the execution of the applicable EU Commission's Standard Contractual Clauses, and the UK International Data Transfer Addendum to the EU Standard Contractual Clauses, or the putting in place of any other valid transfer mechanism.

4.5 Data Disclosure Requests. If RingCentral receives a request from a law enforcement or other government authority to disclose Personal Data that RingCentral is processing on the Customer's behalf, RingCentral will notify and provide the Customer with the details of the data disclosure request prior to disclosing any Personal Data, unless legally prohibited or where an imminent risk of serious harm exists that prohibits prior notification.

5. Miscellaneous

5.1 Unless the above explicitly states otherwise the terms and conditions of the Agreement shall apply to the DPA. In case of any conflict between the terms of the Agreement, any security related terms included in the DPA or the Agreement, and the terms of this DPA, the terms of this DPA prevail with regard to data processing activities.

5.2 The governing law and forum that apply to the Agreement also apply to this DPA.

5.3 Contact information for privacy inquiries: privacy@ringcentral.com.

Annex 1

DESCRIPTION OF THE PROCESSING

Purpose of Processing

The purpose of the processing activities carried out by RingCentral is the provision of any of the following:

1. Cloud-based communications and collaboration services for high-definition voice, video, SMS, chat messaging and collaboration, conferencing, online meetings, and fax.
2. Customer contact centre services and an omni-channel customer communication management platform that unifies all customer-facing communication channels, including voice, email, SMS, website, mobile app, chat and social media communications, onto a single platform, enabling community responses to customer service inquiries.
3. Virtual events and presentation services.
4. Professional services;
5. Any other Services as specified in the Agreement unless otherwise governed by specific data protection terms.

All the above as specified in the Agreement, collectively (the "**Services**").

Services may include dashboards providing various metrics and insights on customer communications, some of which are based on a conversation intelligence platform involving artificial intelligence.

Data Subjects

The data processing impacts the following categories of data subjects:

- Customer's employees and authorised users who use the Services in connection with the business of the Customer.
- Any other individuals who are involved in or referred to in the content of communications or collaborations taking place through the Customer's use of the Services.

Customer Personal Data

As applicable to the Services, the categories of Customer Personal Data processed may include, but are not limited to:

- Service account data which may comprise any of the following: name; telephone number; email address; physical address; title; role; profile information; application settings, login credentials (user ID, log in, account, passwords);
- Usage data which may comprise any of the following: device information (such as IP address, ISP, device and operating system type, operations system and client version, client version, type of microphone or speakers, connection type and related information, etc.); connection type and related information (e.g., connected over WiFi); system logs, including usage logs, backend logs, client logs; cookie identifiers; communications metadata, including Call Detail Records (CDRs) and traffic data;
- User generated content which may comprise any of the following: participants' names or phone numbers; chat messages; text of inbound and outbound faxes; voicemails; text of inbound and outbound SMS; meetings notes; audio/video streams in transit; meeting or call recordings; content of contact center interactions (e.g., emails, social media posts, call recordings, chat, etc.); transcriptions of recorded calls or meetings; summaries of recorded calls or meetings; meeting history; shared files, pictures, and links; message attachments, such as notes, tasks, events, code

snippets, and .gifs; folder creations; search history; online presence and status messages; user feedback;

- Any other type of Personal Data as needed for the performance of the Services.

Special Categories of Customer Personal Data

The Services are 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 related to criminal convictions and offences. Insofar as Customer processes special categories of Personal Data, Customer undertakes to process this category of Personal Data lawfully, and in particular to rely on a valid legal basis in accordance with Applicable Data Protection Laws.

Processing Operations

RingCentral processes Customer Personal Data for the purposes of providing and maintaining the Services to which the Customer has subscribed, including any ancillary or related Services under the scope of the Agreement, which may include collection, storage, transmission, recording, transcription, publishing, displaying; retrieval; consultation; combination; structuring; adaptation.

Duration of the Processing

Customer Personal Data will be processed for the term of the Agreement, or as otherwise required by law or agreed between the Parties.