RingCentral

RingCentral Channel Partner Program
United States Privacy Agreement

This United States Privacy Agreement ("US Privacy Agreement") forms part of the RingCentral Partner Terms and Conditions (the "Terms") governing your participation in the RingCentral Channel Partner Program (the "Program"). This US Privacy Agreement reflects the Parties' agreement with regard to the access, processing, and storage of Personal Information in connection with your performance of the Program as described in the Terms.

Capitalized terms used but not defined in this US Privacy Agreement shall have the same meanings as set out in the Terms.

1. **Definitions**
   - **1.1.** **Contractor** shall mean a person to whom RingCentral makes available a RingCentral Personal Information for the business purpose described in the Program.
   - **1.2.** **Personal Information** shall mean and refer to any information relating to an identified or identifiable person or individual and also includes personal data, as defined by applicable US State Privacy Laws.
   - **1.3.** **RingCentral Personal Information** shall mean and refer to any Personal Information provided to you by RingCentral that you process as a Service Provider or a Contractor under the Terms.
   - **1.4.** **Sell** shall have the same meaning as set forth in California Privacy Law.
   - **1.5.** **Service(s)** shall mean the service(s) performed by you as part of the Program.
   - **1.6.** **Share** shall have the same meaning as set forth in California Privacy Law.
   - **1.7.** **Security Incident** shall mean any destruction, loss, alteration, disclosure of, or access to RingCentral Personal Information that is accidental, unlawful, or unauthorized.
   - **1.8.** **Service Provider** shall mean and refer to a service provider or subcontractor, as defined by applicable US State Privacy Laws, that processes RingCentral Personal Information on RingCentral's behalf, where you are a Service Provider to RingCentral, for the purposes of the Terms.
   - **1.9.** **US State Privacy Laws** shall mean and refer to all United States data protection and privacy laws which may be applicable to you in the processing of RingCentral Personal Information as part of the performance of the Services, including but not limited to the California Consumer Privacy Act of 2018 and its implementing regulations, the California Privacy Rights Act of 2020 and its implementing regulations ("California Privacy Law"), the Virginia Personal Information Privacy Act of 2021 and its implementing regulations, the Colorado Privacy Act of 2021 and its implementing regulations, etc.

2. **Roles and Responsibilities**
   - **2.1.** **Your Obligations.**
     - **2.1.1.** **Purpose Limitation**. You shall process the RingCentral Personal Information for the purposes of the performance of the Program except where otherwise required or permitted by US State Privacy Laws.
     - **2.1.2.** You will:
       - **2.1.2.1.** Operate as applicable as a Service Provider or Contractor and comply with the applicable US State Privacy Law obligations.
       - **2.1.2.2.** Provide the same level of privacy protection as required by the applicable US State Privacy Law.

2.1.2.3. Notify RingCentral if you can no longer meet your applicable US State Privacy Law obligations.

2.1.2.4. Not Sell or Share RingCentral Personal Information including, for the avoidance of doubt, not use RingCentral Personal Information for cross-context behavioral advertising.

2.1.2.5. Not retain, use, or disclose RingCentral Personal Information for any other purpose other than as agreed upon in the Terms, outside the direct business relationship between the Parties, or as permitted by applicable US State Privacy Law.

2.1.2.6. Not combine RingCentral Personal Information you receive from, or on behalf of, RingCentral with Personal Information you receive from, or on behalf of, another person, or collects from your own interaction with the end user, subject to the exceptions under applicable US State Privacy Law.

2.1.2.7. Cooperate with RingCentral, upon RingCentral's reasonable notice, to determine reasonable and appropriate steps to stop and remediate unauthorized use of RingCentral Personal Information.

2.1.3. **Cooperation.** You will cooperate with RingCentral to make available all information in your possession to demonstrate compliance with US State Privacy Laws.

2.1.4. **Certification.** When acting as Contractor, you certify that you understand the restrictions in §1798.140(j)(1)(A) and comply with them.

2.2. **RingCentral rights**. RingCentral may take reasonable and appropriate steps to ensure that you use RingCentral Personal Information in a manner consistent with your obligations under US State Privacy Laws.

3. Security

You shall ensure that any person that you authorize to process the RingCentral Personal Information shall be subject to a duty of confidentiality (either a contractual or a statutory duty). You shall implement appropriate technical and organizational measures to protect RingCentral Personal Information from Security Incidents. At a minimum, such measures shall include the measures identified in Annex I.

4. Security Incidents

4.1. Notice.

4.1.1. In the event you discover any past or ongoing Security Incident or have reason to believe any Security Incident is likely to have occurred or is occurring, which involves RingCentral Personal Information, you shall promptly and without undue delay (and in any event, no later than 72 hours after you or any of your employees, representatives, or agents discovers the Security Incident) notify RingCentral at privacy@ringcentral.com.

4.1.2. You shall cooperate with RingCentral in any communication efforts, including legally required notifications to law enforcement agencies, data protection authorities and/or impacted customers and individuals, resulting from or relating to the Security Incident. You agree that any decision to notify individuals or public authorities of the Security Incident shall be made

between both parties, and any notice, public or otherwise, relating to such Security Incident shall be reviewed in advance by RingCentral.

4.2. **Response.** You shall use your commercially reasonable efforts to cooperate with RingCentral in responding to a Security Incident, including without limitation providing copies of all relevant log, IDS, and security event data to RingCentral, making your staff with information security experience available to work with RingCentral in understanding the details of any Security Incident, and allowing RingCentral forensic investigation personnel and/or RingCentral audit personnel to work directly with your staff in joint investigation activities, or to conduct audits of RingCentral Personal Information security and control measures. You shall do and perform, or cause to do and perform, such further acts and things as RingCentral requests in responding to the Security Incident.

4.3. **Costs.** You agree to indemnify and hold RingCentral harmless for any and all claims, losses, costs, expenses, damages, or other liabilities (including reasonable legal fees) suffered or incurred by RingCentral as a result of the accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure of, or access to RingCentral Personal Information as caused by you or your Service Providers.

5. Service providers

5.1. **Notification.** Where required by US State Privacy Laws, you will notify RingCentral before you engage another Service Provider. Where required by US State Privacy Laws, you will allow RingCentral thirty (30) calendar days to object to such engagement on reasonable grounds relating to the protection of RingCentral Personal Information. If RingCentral refuses to consent to your appointment of a Service Provider, then RingCentral may elect to suspend or terminate the Terms without penalty.

5.2. **Agreements.** you shall impose data protection terms on such Service Providers that protect RingCentral Personal Information to an equivalent standard provided for by this US Privacy Agreement. You remain fully liable for any breach of this US Privacy Agreement that is caused by an act, error, or omission of your Service Providers.

5.3. **Disclosure.** You will not disclose or transfer or allow access to RingCentral Personal Information by any third party except (i) to a Service Provider in a manner that complies with the terms of this Section 5; and (ii) as required by applicable law, provided that, you will promptly notify RingCentral of such a required disclosure (save where prohibited by law), make all reasonable attempts to delay disclosure to the degree necessary for RingCentral to meaningfully participate in your response (save where prohibited by law), and will cooperate with RingCentral to contest or minimize the scope of the disclosure.

6. Audits

6.1. Where required by US State Privacy Laws, you will cooperate with RingCentral to make available all information in your possession to demonstrate compliance with your obligations in applicable US State Privacy Law.

6.2. Additionally, you agree that RingCentral (or its appointed representatives) may, upon reasonable notice, during regular business hours and without unreasonably interrupting your business operations, carry out an on-site inspection and audit of your compliance with this US Privacy Agreement. You shall permit RingCentral (or RingCentral's appointed third party auditors) to audit your compliance with this US Privacy Agreement, and shall make available to RingCentral all information, systems, staff and on-site facilities necessary for RingCentral (or RingCentral's third party auditors) to conduct such audit.

RingCentral

7. Data Retention

Upon termination or expiration of the Terms, or at any time upon RingCentral's request, you will promptly (and in no event more than thirty (30) days post termination, expiry or request) cease to process RingCentral Personal Information and will promptly return or destroy the RingCentral Personal Information (including all copies) in your possession or control (including any RingCentral Personal Information held by Service Providers) as instructed by RingCentral. Upon request, you will certify to RingCentral in writing that all RingCentral Personal Information has been destroyed. This requirement shall not apply to the extent that You are required by applicable laws to retain some or all of the RingCentral Personal Information, in which event you shall isolate and protect the RingCentral Personal Information from any further processing except to the extent required by such law.

8. Disclosure of US Privacy Agreement

You acknowledge that RingCentral may disclose this US Privacy Agreement and any relevant privacy provisions in the Terms to (i) the US Department of Commerce, the Federal Trade Commission, or any other data protection authority of competent jurisdiction upon their request and (ii) to RingCentral Customers and (iii) in connection with any legal suit to which the existence and terms of this US Privacy Agreement are relevant. Any such disclosure shall not be deemed a breach of any confidentiality provisions contained in this US Privacy Agreement or the Terms.

9. Miscellaneous

9.1. Unless the above explicitly states otherwise, the terms shall apply to the US Privacy Agreement. In case of any conflict between the Terms and the terms of this US Privacy Agreement, the terms of this US Privacy Agreement prevails with regard to data processing activities subject to US State Privacy Laws.

9.2. The governing law and forum that apply to the Terms also apply to this US Privacy Agreement.

9.3. Contact information for privacy inquiries: privacy@RingCentral.com.

RingCentral

ANNEX I - TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

This Annex I sets out the minimum technical and organizational measures that You will implement to protect RingCentral Personal Information.

1. Information Security Management. You will maintain appropriate cybersecurity measures to safeguard the security of RingCentral Personal Information. In no event shall You take precautions any less stringent than those employed to protect its own proprietary and confidential information. In addition, You agree to develop and maintain any additional cybersecurity measures as may be required by applicable Privacy Laws. You will maintain a cybersecurity and risk management program based on commercial best practices to preserve the confidentiality, integrity and accessibility of RingCentral Personal Information with comprehensive administrative, technical, procedural and physical measures conforming to generally recognized industry standards and best practices that include the following:

i. **Cybersecurity Program.** You must keep RingCentral Personal Information secure from accidental, unauthorized or unlawful access, use, disclosure, alteration, destruction and / or loss by using administrative, technical, procedural, and physical safeguards that are reasonable and appropriate to the circumstances, taking into account the nature of RingCentral Personal Information and the scope, context and purposes of the processing (individually, a "**Safeguard**"; all Safeguards collectively, the "**Cybersecurity Program"**).

ii. **Documentation.** You will maintain documentation that describes in detail Your Cybersecurity Program and the specific Safeguards You employ ("**Written Security Policy, Procedure, and Standards, Technical implementation details**").

iii. **Changes.** You will refrain from making any changes to Your Cybersecurity Program or specific Safeguards that reduce the level of security provided to RingCentral Personal Information.

iv. **Network Security.** You agree to maintain network security that includes industry standard firewall protection and periodic vulnerability scans for the relevant Computing Systems.

v. **Server and Endpoint Security.** You agree to ensure that Your Computing Systems are patched and up-to-date with all appropriate security updates as designated by the relevant manufacturer or authority (e.g. Microsoft notifications, etc.) and are free of known viruses, worms, spyware, adware, malware, and other malicious and unwanted software and programs.

vi. **Application Security.** You agree to use commercially reasonable efforts to regularly identify software vulnerabilities and, in the case of known software vulnerabilities, to provide relevant updates, upgrades, and bug fixes for any software provided to RingCentral or RingCentral's customers, or in which any RingCentral Personal Information is stored or processed, in the course of fulfilling their obligations under the Standard Terms of Use.

vii. **Independent security assessments.** You agree to use independent third parties to perform annual penetration tests and security audits covering the systems, environments and networks where RingCentral Personal Information is stored, processed and accessed. You agree to remediate all medium and higher severity findings and observations from such assessments.

viii. **Strong Authentication.** You will enforce Strong Authentication for any remote access to RingCentral Personal Information and any remote use of Nonpublic Information

Resources. Additionally, You will enforce Strong Authentication for any administrative and/or management access to Your security infrastructure and Your log data including but not limited to firewalls, Identity and Access Management systems, security monitoring infrastructure, and computing logs such as firewall logs, server logs, DNS logs, etc.

ix. **Physical and Environmental Security.** You will have in place physical premise security and environmental protections for Your Computing Systems, meeting ISO 27001/27002 standards.

x. **Data Security and Data Transparency:** Upon request from RingCentral, You agree to provide RingCentral with an inventory or data map of RingCentral Personal Information that is in Your possession or control, including locations of such data, and control measures that are in place for the protection of RingCentral Personal Information.

xi. **Personnel confidentiality:** You will ensure that any person that You authorize to process RingCentral Personal Information (including Your staff, agents and subcontractors) will be subject to a strict duty of confidentiality (whether contractual or statutory).

xii. **Cybersecurity Awareness and Training:** You will have a cybersecurity awareness and training program in place that includes how to implement and comply with Cybersecurity Program and promote a culture of security awareness through periodic communications from the organization's senior leadership.

xiii. **Contingency Planning:** You will have policies and procedures for responding to emergencies, cybersecurity incidents and other events (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage or remove access to RingCentral Personal Information.

xiv. **Storage and Transmission Security:** You will have security measures to guard against unauthorized access to RingCentral Personal Information that is being transmitted over a public electronic communications network or stored electronically. Such measures include requiring encryption of any RingCentral Personal Information stored on desktops, laptops, smartphones, tablets and other mobile devices and removable storage media.

xv. **Secure Disposal:** You will have policies and procedures regarding the secure disposal of tangible property containing RingCentral Personal Information, considering available technology, so that RingCentral Personal Information cannot be practicably read or reconstructed.

xvi. **Monitoring and Logging.** You will have intrusion detection systems, full audit trail logging, and security event detection and monitoring in place for networks, servers, and applications where RingCentral Personal Information is stored, processed, or transmitted. You will log and maintain for 12 months all physical and logical access to RingCentral Personal Information, including command history logging of all logical access. You will also log and store all security events for 12 months, including but not limited to ACL logs, IDS logs, and SIM/SIEM events.

xvii. **Passwords:** When passwords are used to access RingCentral Personal Information, You will enforce Strong Authentication in all instances. Where practicable, You will use a second authentication factor before granting access to RingCentral Personal Information with a password.

a) Passwords must be complex and meet the following password construction requirements:
    1. Be a minimum of eight (8) characters in length.
    2. Include characters from at least two (2) of these groupings: alpha, numeric, and special characters.

3. Not be the same as the UserID with which they are associated.

b) Non-random PINs must meet the following:
   1. Be a minimum of four (4) numbers; and
   2. Not contain more than two (2) sequential numbers.

c) Require passwords and PIN expiration at regular intervals not to exceed ninety (90) calendar days.

d) When providing users with a new or reset password, or other authentication credentials, use a secure method to provide this information and maintain a written policy requiring reset at first login whenever a temporary credential is used.

xviii. **Encryption:** You agree to use Strong Encryption with minimum key lengths of 256-bits for symmetric encryption and 2048-bits for asymmetric encryption to protect RingCentral Personal Information:

a) when transmitted over any network;
b) when stored (at rest); or
c) whenever authentication credentials are stored.

xix. **Least privilege:** You agree to enforce the rule of least privilege by requiring application, database, network and system administrators to restrict user access to only the commands, data and Information Resources necessary for them to perform authorized functions.

xx. **Access Management:** You agree to have formal processes in place to grant, prevent and terminate access to RingCentral Personal Information. The access should be limited to users who are required this access to perform their job responsibilities. You agree to have documented Access Management procedures in place.

2. Adequate Security Measures and Procedures. Upon RingCentral's request, and following all necessary confidentiality undertakings, You will provide RingCentral, at Your expense, a third-party certification, third-party audit report, or written statement of a You officer certifying that You and your affiliates, agents, contractors, consultants, joint ventures and other Third Parties having access to or control of RingCentral Personal Information have complied with all of the requirements of this Security Attachment (the "Certification"). Such Certification must have been conducted within the last twelve (12) months of the request. If RingCentral believes such internal controls and cybersecurity measures as expressed in this documentation are inadequate to safeguard the RingCentral Personal Information, RingCentral may require the adoption of additional reasonable controls, security measures, and procedures. If You fail to do so within a reasonable time, such failure shall be deemed to be a material breach of the Agreement, and RingCentral shall be permitted to terminate the Agreement immediately.

3. Definitions. For the purposes of this Annex**:**

a) "**Computing Systems"** shall be defined as networks, servers, computers (inclusive of smartphones and tablet computers), applications, and other technology infrastructure that You use to deliver services in fulfillment of their obligations under the Agreement.

b) **"Nonpublic Information Resources"** means those Information Resources used under the Agreement to which access is restricted and cannot be gained without proper authorization and identification.

c) **“Sensitive Authentication Data”** means the most current PCI Security Standards Council definition, as updated or amended from time to time. In determining whether a breach of this Security Attachment has occurred, “Sensitive Authentication Data” shall mean the definition of the PCI Security Standards Council in effect at the time of the breach.

d) “**Strong Authentication**” means the use of authentication mechanisms and authentication methodologies stronger than the passwords required by the applicable requirements herein. Examples of Strong Authentication mechanisms and methodologies include digital certificates, two-factor authentication, and one-time passwords.