Personal Data Transfer Risk Assessment: FAQ

RingCentral is a United States-based company that provides cloud-based communications and collaboration solutions (collectively "Services"). RingCentral, Inc. is a leading provider of unified communications (message, video, phone), customer engagement, and contact center solutions for businesses worldwide. As part of the Services, RingCentral processes personal data on behalf of its customers for purposes that include providing and maintaining the Services, performing customer analytics, and delivering customer support services. RingCentral is a global company that transfers and remotely accesses certain personal data outside of the European Economic Area (EEA).

In response to *Schrems II*, taking into account the European Union Commission Standard Contractual Clauses implementing decision 2021/914 (SCCs 2021/914), and the European Data Protection Board (EDPB) recommendations regarding supplemental transfer tools, RingCentral has performed a review of the data transfers involved in the Services. Our customers will need to carry out their own data transfer risk assessments. However, for informational purposes only, RingCentral has prepared this document as a resource for our customers.

When transferring personal data outside the EEA, RingCentral relies on the following mechanisms, as relevant:

- Certification of RingCentral, Inc. to the EU-U.S. Data Privacy Framework (DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), for the transfer of personal data from the EEA to the USA ; or

- SCCs 2021/914 for the transfer of personal data from the EEA and Switzerland to non adequate countries; or

- International Data Transfer Addendum (IDTA) to the European Commission's standard contractual clauses for international data transfer, for the transfer of personal data from the United Kingdom to non adequate countries.

RingCentral

Transfers and Access

What personal data do RingCentral Services collect?

RingCentral Services collect and may transfer the following personal data:

- Account information for anyone, including customer's employees who use the services at the request of and in connection with the business of the customer, including telephone number (fixed and mobile) and email address.
- Call detail records, including numbers of the calling and the receiving party, start date and time of the call, and duration of the call.
- For services such as RingCentral Contact Center, RingCentral Engage Digital and/or RingCentral Engage Voice, and RingCentral Engage Digital communities:
    - Account information for end users such as full name, contact information (address, telephone number (fixed and mobile), email address, fax number), employment information (job title), and company name.
    - Account information of customer's employees or authorized users or other third-party contributors, including name and email address.
    - Content published on communication channels connected to the services, including public information on social media channels connected to the service.
    - Content published on the online sharing space, including any public posts and private messages.
- Any other customer personal data that the customer, its authorized users, or third parties involved in the communications choose in their sole discretion to include in the content of the communications that are sent and received using the Services.
- Any other customer personal data that may be necessary for RingCentral to provide the Services as described in the Agreement.

Where does RingCentral process personal data?

RingCentral relies on European data centers for some of its data processing to ensure minimum latency. We store customer content (such as video recordings, messaging, and voicemail) and call detail records in the EEA.

RingCentral transfers certain personal data (account information) out of the EEA to the United States, where we process such personal data in order for us to operate, deliver, maintain, and support our Services. The United States is the only third country to which RingCentral moves EEA personal data. Data stored in the EEA and in the United States may be accessed remotely from other third countries including but not limited to Georgia, and the Philippines.

Has RingCentral performed a risk assessment of the data transfers and access?

This FAQ focuses on data transfers to the United States as this is where certain EEA data is stored. RingCentral has performed a data transfer risk assessment for all the countries to which we transfer personal data and all the countries within the EEA from which we access personal data. For our Data Transfer Risk Assessment pertaining to non-US countries, please email privacy@RingCentral.com.

Who are RingCentral's subprocessors and where are they located?

Please see RingCentral's Subprocessor List, which includes information regarding their location, applicable Services, and processing function.

Is the EEA personal data moved to the United States subject to any onward transfers?

RingCentral may transfer personal data to RingCentral's subprocessors and affiliates, none of which conduct onward transfers to any country not identified above.

Transfers to the United States

United States government and law enforcement agencies may request access to data stored in the United States. RingCentral is legally obligated to comply with lawful requests. RingCentral publishes as much information regarding government requests for customer data as legally permitted in our annual Transparency Report.

The Foreign Intelligence Surveillance Act of 1978 - section 702

As an electronic communication service provider, RingCentral is subject to legally valid requests from United States government agencies under Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA 702). FISA 702 authorizes government agencies to obtain foreign intelligence information to and from non-United States persons located outside of the United States.

What is foreign intelligence information?

Foreign intelligence information is limited to information necessary to protect the United States, including intelligence necessary to protect the United States against actual or potential attacks, sabotage, international terrorism, or clandestine intelligence activities by a foreign power, the proliferation of weapons of mass destruction, or information that is necessary to protect the United States national defense or the conduct of United States foreign affairs.

FISA 702 requests are limited to foreign intelligence information coming to or from a targeted individual. The requests cannot include information about a targeted individual.
Is public authority access under FISA subject to prior approval? If so, who approves?

Generally, the Foreign Intelligence Surveillance Court (FISC) must approve a FISA 702 request. To obtain a FISC order, government agencies must submit a certification attesting that the request does not target United States citizens or individuals in the United States, that it minimizes the information sought, and that it seeks foreign intelligence information.

In exigent circumstances, the Attorney General and Director of National Intelligence may authorize the collection of data prior to obtaining a FISC order. Such authorization must comply with query, minimization, and targeting procedures that are adopted by the Attorney General and are subject to review by the FISC.

Is there oversight over FISA 702 procedures and requests for information?

The FISC, United States Department of Justice, Office of the Director of National Intelligence, inspector generals of applicable United States government agencies, and the United States Congress are actively involved in ensuring that individuals are properly targeted under FISA 702. The government is required to record the reasoning for which each person was targeted and to provide a connection between the foreign intelligence purpose and the individual being targeted. Each applicable intelligence agency annually reviews its procedures for targeting based on the required recordkeeping and must provide reports to the FISC, the Attorney General, the Director of National Intelligence, and the United States Congress.

Each intelligence agency is required to ensure that FISA requests comply with legal standards and must report material noncompliance to the United States Congress. In addition, at least once every six months, the United States Department of Justice and Office of the Director of National Intelligence must assess whether the government is compliant with the legal standards and report their findings to the FISC and the United States Congress.

Do individuals who have had data accessed have any remedy for any breach of laws?

FISA provides a private right of action to seek compensatory damages, punitive damages, and attorney's fees against individuals who violated FISA 702. The Electronic Communications Privacy Act provides a separate private right of action for wilful violations of certain FISA provisions. The Administrative Procedure Act also allows for challenges to unlawful government access to personal data, including under FISA, for an order enjoining access. Aggrieved persons, including non-United States persons, have a private right of action for violations of FISA 702.

Is RingCentral subject to the CLOUD Act?

As an electronic communication service, RingCentral is subject to legally valid requests from the United States government pursuant to the Clarifying Lawful Use of Overseas Data (CLOUD) Act. The CLOUD Act was passed in 2018 and amended the Stored Communications Act. It requires providers of remote computing services and electronic communication services to the public that are subject to United States jurisdiction to comply with United States law enforcement orders to disclose information that may be located within or outside of the United States.

The CLOUD Act also authorizes the United States President to enter into agreements with foreign nations that allow foreign nations to seek information located in the United States regarding non-United States persons. The foreign nations must have robust human rights and privacy protections and may only seek information related to ongoing investigations into serious crimes, including terrorism. Such requests are governed by the law of the foreign nation, not United States law, but are subject to review by United States courts.

Is public authority access subject to prior approval? Who approves?

The CLOUD Act requires a United States court order issued by a court of competent jurisdiction for the United States government to compel disclosure of certain categories of data protected by the Stored Communications Act and by an entity subject to United States jurisdiction.

Is there oversight over CLOUD Act procedures and requests for information?

United States law enforcement must apply for a warrant before requesting information that has been stored for six months or less. The warrant must specify the target and include,

"specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." Law enforcement cannot seek a wide swath of information based on unsupported, vague statements. Absent a non-disclosure order, providers are allowed to inform a customer that the provider received a CLOUD Act warrant for information that has been stored for less than six months.

When law enforcement seeks to access data that has been stored for six months or more, law enforcement either may (1) seek a warrant or (2) serve an administrative subpoena on the service provider so long as law enforcement notifies the target prior to subpoena issuance.

CLOUD Act warrants and subpoenas are subject to judicial review.

CLOUD Act & GDPR

In invalidating the EU-United States Privacy Shield, the European Court of Justice (ECJ) in the *Schrems II* decision did not take issue with the CLOUD Act as a United States law that may not provide adequate protection of personal data. Further, the 2021 SCCs were adopted to address, in part, government access and the obligations imposed on data importers, including to challenge valid government requests where there are legal grounds. RingCentral has agreed to the 2021 SCCs and will comply with the 2021 SCCs requirements regarding challenging government requests and minimizing disclosures.

Are RingCentral's United States subprocessors subject to FISA 702 or the CLOUD Act?

Even if the government takes a broad reading of which entities are subject to FISA 702 and the CLOUD Act, and believes that RingCentral's subprocessors are subject to these Acts, we believe it is unlikely that the government would be able to obtain data directly from subprocessors because our subprocessors have limited or no ability to associate any data with a specific customer or user.

Accordingly, we expect that the United States government would request data and information directly from us, not from our United States subprocessors.

To the extent that our United States subprocessors do receive a government request directly, they are required to abide by the commitments in the 2021 SCCs, which obligate them to:

> "Review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity." (2021 SCCs, Article 15.2.)

Is RingCentral subject to Executive Order 12333?

RingCentral does not provide any assistance to government agencies that collect information pursuant to Executive Order (EO) 12333, and EO 12333 does not impose any obligations on RingCentral. RingCentral encrypts personal data in transit over a public network and does not affirmatively cooperate with any activities under EO 12333.

Are there limitations to EO 12333, and do they apply to non-United States residents and citizens?

EO 12333 limits the amount of time data collected about United States persons can be retained and used. Presidential Policy Directive 28 (PPD-28), effective since 2014, directs that limitations in EO 12333 apply to foreigners on an equal basis as they apply to United States persons.

In addition, PPD-28 limits the use of signals intelligence collected in bulk in order to protect privacy and civil liberties of all persons regardless of nationality or residence. Bulk signals are permitted only under six limited purposes of detecting and countering: 1) espionage and other threats and activities directed by foreign powers or intelligence services against the United States and its interests; 2) threats to the United States and its interests from terrorism; 3) threats to the United States from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to United States or allied Armed Forces or other United States or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section. This list is reviewed annually. PPD-28 also sets forth safeguards for the method of collection through signals intelligence including data minimization, dissemination, retention, security and access, data quality, and oversight.

The National Intelligence Priorities Framework is established by the Director of National Intelligence to ensure that targeting and collection, including under EO 12333, are proportional to specific national intelligence priorities.

Does RingCentral receive requests for bulk data, for example data that is not customer specific?

As of December 2021, RingCentral has not received any requests for bulk data and does not assist the United States government in obtaining bulk data pursuant to EO 12333.

What about the Trans-Atlantic Data Privacy Framework?

On 25 March 2022, the European Commission and the United States announced that they have agreed in principle on a new Trans-Atlantic Data Privacy Framework.

On 7 October 2022, President Biden signed an Executive Order on 'Enhancing Safeguards for United States Signals Intelligence Activities' (hereafter "Executive Order"). This Executive Order is a key step towards the implementation of the new Trans-Atlantic Data Privacy Framework announced in March as it allows the EU Commission to draft the adequacy decision and further launch its adoption procedure which is expected to take 4-6 months.

In substance, the Executive Order addresses the points raised in the Court of Justice of the European Union (CJEU) Schrems II decision by establishing:

(1) binding safeguards limiting access to EU data by United States intelligence services to what is necessary and proportionate to protect national security;

(2) an independent and impartial multi-step redress mechanism to investigate and resolve complaints raised by individuals regarding access to their data by United States national security authorities and consisting of an initial layer of review of complaints by the existing Civil Liberties Protection Officer, which will be subject to appeal with the new Data Protection Review Court.

As a result the United States intelligence agencies have been required to review their policies and procedures to implement these new safeguards.

On July 10, 2023, the adequacy of the EU-US Data Privacy Framework (DPF) was approved by the EU Commission. Under this adequacy decision personal data transfers from controllers and processors in the EU to certified organizations in the US may take place without the need to obtain any further authorization and to put into place transfer mechanisms such as Standard Contractual Clauses.

Is RingCentral certified to the Data Privacy Framework?

Yes. RingCentral has self-certified compliance with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework. Please consult our certification listed here and RingCentral Notice of Certification for more details.

Note that RingCentral continues to rely on the 2021 Standard Contractual Clauses (incl. the UK IDTA) for data transfers out of the EEA, UK, and Switzerland to other non-adequate third countries.

Government Access and RingCentral

How does RingCentral respond to government access requests for personal data, and has RingCentral received requests from United States public authorities to access transferred personal data?

The RingCentral Legal Department reviews all government requests for data to ensure they are legitimate and proportionate. RingCentral will not respond to any government access requests that could infringe on the privacy rights of a customer not subject to the request. RingCentral will notify our customers or partners of any request for data to enable them to respond to the request directly, unless legally prohibited from doing so by law or a valid nondisclosure order.

If we are prohibited from notifying our customers of the data request, we will use all reasonable lawful efforts to invalidate or waive the nondisclosure obligation and will communicate as much information as permitted to the customer as soon as possible. RingCentral will review the legality of each request for data, and specifically whether the party making the request has a valid legal right to make such a request. RingCentral will exhaust all available remedies to challenge the request if, after a careful assessment, it concludes that there are grounds for challenge under applicable laws.

RingCentral will refuse to provide information in response to any request in which it identifies inconsistencies or inaccuracies. We will provide the narrowest possible set of information permissible when responding to a request based on a reasonable interpretation of the request. RingCentral will reject requests that have been improperly served or requests that we deem to be incomplete, overly broad or vague, or unduly burdensome.

Does RingCentral have any backdoors that may allow government access?

RingCentral Services do not contain any feature or defect that allows for surreptitious unauthorized access to customer data, except for access points for law enforcement as required by law.

Does RingCentral publish a Transparency Report?

RingCentral provides an annual Transparency Report that describes how we respond to customer data requests submitted by law enforcement and government agencies around the world. The report covers the total number of global government requests and identifies the number of requests that resulted in the disclosure of data, the requesting country, and the categories of data that we provided to authorities.

Security

What security measures are in place to protect customers' data?

- **Encryption:** RingCentral encrypts customer data in transit with Advanced Encryption Standard (AES) 256 and at rest using disk encryption. RingCentral uses enterprise-grade security protocols to provide additional security for IP phone calls including Transport Layer Security (TLS) authentication 1.2 and Secure Real-Time Transport Protocol (SRTP) encryption. In addition, all internet-facing portals have https (e.g., https:// service.ringcentral.com); all non-voice customer data is TLS encrypted; and hard phones use digital certificates to establish secure connections to download their provisioning data.
- **Audit logging:** RingCentral ensures generation of audit logs for all systems, devices, or applications associated with the access, processing, storage, communication, and/or transmission of personal data.
- **User authentication:** RingCentral ensures that its users have individual accounts for unique traceability; shared accounts are not typically permitted. User passwords are configured to align with National Institute of Standards and Technology (NIST) guidance. RingCentral requires multi-factor authentication or two-factor authentication.
- **Customer account control:** RingCentral provides customers with the ability to view and manage their account policies including the below:
    - Role-based access controls can be customized, or customers can use one of our standard, ready-to-use roles.
    - Audit trails to track configuration changes, login attempts, phone number changes, admin/employee settings, and permissions.
    - Single Sign-on (SSO): customer admins can define policies to enforce unique controls for each individual SSO application.

- **Toll fraud mitigation control:** RingCentral prevents toll fraud through access control, detection controls, and usage throttling and gives customers granular control over who gets to make international calls and to where.
- **Multi-tenancy model:** Our multi-tenant maintains a high degree of security to ensure that one customer's data is never available to another customer. We use a multi-tenant architecture and dynamic database views to form application layer boundaries between customer instances.

Please see RingCentral's Security Addendum for more information.

RingCentral's Safeguards

Does RingCentral offer additional safeguards?

Please visit RingCentral's Trust Center for more information regarding our privacy and security.

We offer supplemental contractual measures through our Customer Data Transfer Agreement, which is based on the EU Commission's Standard Contractual Clauses including:

- Notification of third-party requests for disclosure of personal data and commitment to challenge such requests where there are valid grounds for challenge
- No backdoor access

RingCentral offers technical and organizational security measures as further discussed above.

Does RingCentral adopt any international standards and best practices?
RingCentral is certified to be compliant with SOC 2 and ISO 27001 security standards. RingCentral's ISO 27001 certificate is available on RingCentral's Trust Center. RingCentral can share its SOC 2 report under a Non-Disclosure Agreement.

RingCentral conducts audits against ISO 27001, 27017, 27018, SOC 2 Type 2 including S2T2+FINRA controls, S2T2+HIPAA controls, HITRUST, and BSI C5:2020.

How does RingCentral handle data subject access requests?

RingCentral has established a Data Subject Request Center and a process to review and respond to all data subject requests.

Who do I contact for additional questions?

For more information, please email privacy@ringcentral.com.

Please note that the information in this document is for general awareness only and is not provided as legal advice. This information is provided for customers on RingCentral's data transfers and the measures that RingCentral has put in place with respect to those transfers and does not constitute warranty of compliance with applicable laws. The content of this document may be subject to change.