BroadCloud UC-One SaaS Service

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by the BroadCloud UC-One SaaS Service.

1. Overview of BroadCloud UC-One SaaS Service Capabilities

BroadCloud UC-One SaaS (the "Service") is a cloud-based business collaboration solution, combining advanced telephony from your BroadCloud system with comprehensive unified communications features, providing a single intuitive application experience for the end user. It is made available by Cisco and its resale and service provider partners ("Partners") to companies ("Customer," "you" or "your") who purchase it for their authorized users (each, a "user"). The Service is a subscription-based service hosted in Cisco's cloud that delivers all the essential unified communications and collaboration services such as: HD voice and video, instant messaging, presence, file sharing, screen sharing, audio/video conferencing, delivered to the end user through the desktop, mobile and tablet. For a detailed description of the Service, please go here.

The following describes Cisco's processing of personal data in connection with the Service, the location and transfers of that data, and how it is secured in accordance with privacy principles, laws, and regulations. Cisco will use your personal data consistent with this Privacy Data Sheet. Note that this Privacy Data Sheet is a supplement to the Cisco Privacy Statement.

2. Personal Data Processing

If you are a user of the Service, the information described in this Privacy Data Sheet is accessible by the Customer, Cisco, and the Partner as described below and is also subject to the Customer's policies regarding access, use, monitoring, deletion, preservation, and export of information associated with the Service. Cisco has no control over, and is not responsible or liable for, the privacy of any information that users have shared with others. Even after information has been removed from the Service, copies of that information may remain viewable elsewhere to the extent it has been shared with others, by a user or the Customer.

The table below lists the personal data used by the Service to carry out the services and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing

Registration Information	• User information
	  ○ Credentials - User ID, Password.
	  ○ Name and Aliases
	  ○ Email Address
	  ○ Company Name
	  ○ Service Provider to Which the User Belongs
	  ○ Session Language
	  ○ Contact Lists*
	
	*Only stored on user's device.
		We use Registration Information to:
		• Deliver and provide operational support for the Service
		• Communicate with you on status and availability of the Service
		• Support billing for the Service
		• Authenticate and authorize access to the Service

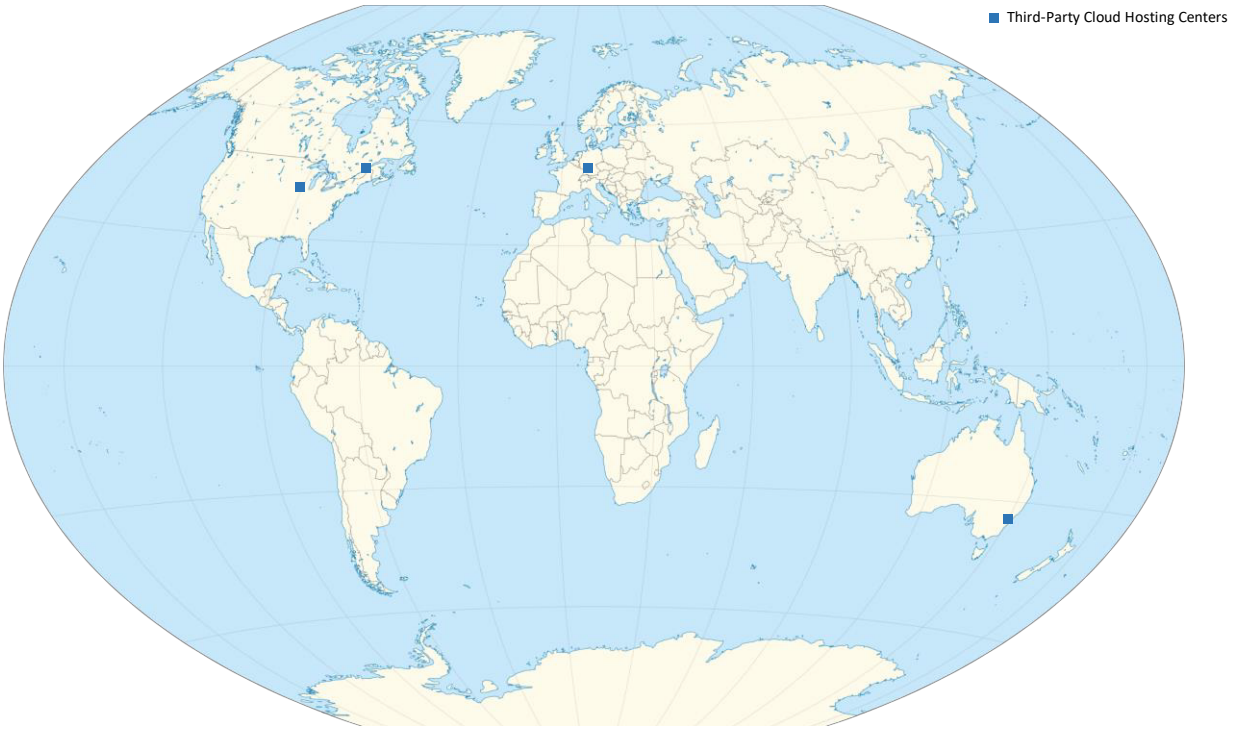
Host and Usage Information	• Session Information:
	  ○ Session ID
	  ○ Creation timestamp
	  ○ Update timestamp
	• Device agent information:
	  ○ OS type and version
	  ○ BroadSoft UC-One Communicator app version
	  ○ Last session date and time
	• Anonymized usage patterns via Google Analytics:
	  ○ Device Type
	  ○ Operating System
	  ○ Country (based on IP address)
	  ○ Language
	  ○ Screens viewed
	  ○ Actions taken
		We use Host and Usage Information to:
		• Provide the service and associated features
		• Understand how the Service is used, such as screens viewed, and events triggered
		• Support billing for the Service
		• Diagnose technical issues
		• Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service
		• Respond to Customer support requests
		• Enforce and monitor compliance with contractual terms and applicable laws in connection with legal claims, compliance, regulatory and investigatory purposes, including prevention and detection of fraud

User-Generated Information	• Instant Messages • Call Logs* • Voice Messages* • Shared files* * Not stored within the service. Only transferred via the service.	We use User-Generated Information to: • Provide the Service

Technical Support Assistance
If a Customer reaches out to Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from the Service. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data.

3. Cross-Border Transfers

Cisco leverages its own data centers as well as third-party hosting providers and business partners to deliver the Service globally. These entities are currently located in the following locations (data center locations may change from time to time and this Privacy Data Sheet will be updated to reflect those changes):



Third-Party Data Center Locations
Iowa, USA
Frankfurt, Germany
Montreal, Québec, Canada
Sydney, Australia

Information is stored in the data center closest to a Customer's principal place of business as provided to Cisco by the Partner during the ordering process. TAC Information is stored in Cisco data centers.

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions. In particular:

- Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- EU Standard Contractual Clauses

4. Access Control

Users, Customers, Partners and Cisco can access personal data on the Service as described in the table below.

Personal Data Category	Who has access	Purpose of the access
Registration Information	Users through the Desktop or Mobile Client	• View profile and settings information • Modify, control, and delete information • Enable or disable third party application integrations such as MS Outlook or device controls • Configure settings for integrated third-party applications • Delete all profile data from local device
	Customer through the UC-One SaaS Portal	• Manage users and administer Service in accordance with Customer's policies • Modify, control and delete information
	Partners through the UC-One SaaS Portal	• Provision enterprises/ customers, end-users and subscribers • Partners do not have access to Authentication Tokens or Credentials
	Cisco	Support the Service in accordance with Cisco's data access and security controls process
Host and Usage Information	Cisco	• Deliver, support and improve the Service in accordance with Cisco data access and security controls process • Detect and prevent fraud
User-Generated Information	Users through the Device Clients	Users may access content that they generated or received in accordance with Customer's personal data policy
	Cisco	Cisco will not access this data unless it is shared with Cisco by the Customer to support the Service, and will do so in accordance with Cisco's data access and security controls process

5. Data Portability

The following personal data is made available in machine readable format: Registration Information, and User-Generated Information such as instant messages. Customers may obtain any of the above data by submitting a request to their Partner who must submit a request to Cisco. The availability of the data is subject to the deletion and retention policies described in Section 6 below.

6. Data Deletion & Retention

Customer may request deletion of personal data retained on the Service by sending a request to their Partner, who must contact Cisco via privacy@cisco.com or by opening a TAC request. When a Customer makes a request for deletion, Cisco endeavors to delete the requested data from its systems within 30 days, unless the data is required to be retained under applicable law or for Cisco's legitimate business purposes. If we are required to retain certain categories of data, the reason why we retain it and the retention period are described in the table below.

Personal Data Category	Retention Period	Reason for Retention
Registration Information	• Data is deleted as soon as service is terminated, or a user is deactivated. • This Service does not use cookies to enable and support certain functionality. •	Data collected as part of registration, including information provided by Customers as part of Cisco's financial due diligence, constitute Cisco business records and are kept to comply with Cisco financial and audit policies, as well as tax requirements.
Host and Usage Information	• Data is deleted as soon as service is terminated, or a user is deactivated. • Log Files are deleted after 30 days (except in Germany where data is stored for up to 7 days).	• Third party integration settings are retained in order to provide the Service • Information generated by instrumentation and logging systems created through the use and operation of the Service is kept as part of Cisco's record of Service delivery, compliance with Cisco financial and audit policies, as well as tax requirements
User-Generated Information	• Data is deleted as soon as service is terminated, or a user is deactivated. • Instant messages and chat history is stored for up to a maximum of 1000 messages.	Third party integration settings are retained in order to provide the Service

7. Personal Data Security

The Service is operated under ISO 27001: 2013 standards, and in accordance with those standards, adopts technical and organizational security measures to protect your personal data from unauthorized access use or disclosure as required by law. The Service also incorporates the NIST 800-53 control families. This signifies that the Service has implemented a broad-based, balanced information security program that addresses the management, operational and technical aspects of protecting information and information systems.

Additional information about our encryption architecture is summarized below.

Personal Data Category	Type of Encryption
Registration Information	• Encrypted in transit and at rest
Host and Usage Information	• Encrypted in transit and at rest • All authentication passwords are protected via encryption or hashing algorithms
User-Generated Information	• Encrypted in transit and at rest

Additional controls include:

- Authentication tokens encrypted
- Data access is limited based on policies of least privilege and need-to-know, enforced with role-based access controls.
- Highly-secure cloud protection mechanisms and operational procedures are implemented.
- Cloud hosting providers are ISO 27001 and SOC 2 Type II certified.
- Regular audits to address the ongoing confidentiality, integrity, availability and resilience of Cisco processing systems and services.
- Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

8. Third Party Service Providers (Sub-processors)

We may share User-Generated Information, Registration Information, Host Information and/ or Usage Information with other Cisco entities and/or service providers, contractors or other third parties to assist in providing and improving the Service. The data shared may include aggregate statistics or individualized data. All sharing of information is carried out consistent with the Cisco Privacy Statement and we contract with third-party service providers that can provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for the service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Google Cloud Platform	N/A	Cloud Hosting	USA, Canada, Germany, Australia.
Google, Inc.	• Device Type • Token used to identify the end-user device • Message Content • Caller/ sender's name and phone number • Receiver's name and phone number	Google Firebase Cloud Messaging (FCM) to send push notifications for mobile applications.	Global Google Data Centers
Apple, Inc.	• Device Type • Token used to identify the end-user device • Message Content • Caller/ sender's name and phone number • Receiver's name and phone number	Apple Push Notification Service (APNS) to send push notifications for mobile applications.	Global Apple Data Centers

9. Information Security Incident Management

Breach and Incident Notification Processes

The Data Protection & Privacy team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's response, leveraging diverse teams including the Cisco Product

Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The Cisco Security Center details the process for reporting security incidents.

The Cisco Notification Service allows Customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows Customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber's relationship with Cisco. If you have questions or concerns about any product or security notifications, contact your Cisco sales representative.

10. Certifications and Compliance with Privacy Laws

The Security and Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. Cisco and its underlying processes are designed to meet Cisco's obligations under the EU General Data Protection Regulation(GDPR), APEC Privacy Framework, and other privacy laws around the world. See Section 3, Cross-Border Data Flows.

11. General Information and FAQs

For more general information and FAQs related to Cisco's Security Compliance Program please visit The Cisco Trust Center.