Cisco Unified Communications Manager Cloud

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco UCM Cloud.

1. Overview of Cisco UCM Cloud

Cisco UCM Cloud (the "Service") is a cloud-based business telephone service 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 provides a full-suite of unified communication capabilities hosted in Cisco's cloud. 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.

UCM Cloud is part of Cisco's Cloud Calling portfolio powered by Cisco's call control engine – CUCM. UCM Cloud is bundled as part of Cisco Collaboration Flex set of offers which includes key Cisco commercial and administrative tools to facilitate the go-to-market and common subscription plans including Webex App and Webex Meetings.

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 e to carry out the service and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
Direct Personally Identifiable Information	• Customer Data • Direct Phone number (Mobile) • Direct Phone number (Work) • Name (First, Middle, Last name) • User Login Credentials • Username	We use Direct Personally Identifiable Information to: • Authenticate and authorize access to the Service • Provide telephone service and associated features • Display identity to other users

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Data	• Administrative Login Credentials • Company/Organization Email Address • Company/Organization Time Zone • Company Organization Account ID • Company Organization Name • Company Organization Phone Number • Company Organization Physical Address • Device Activation Codes • End User Login Credentials • Login/Alias ID • SIP Identifier • User Email Address • User Profile Picture • Voicemail Box Number • Voicemail PIN	We use Registration Information to: • Deliver and provide operational support for the Service • Communicate with you on status and availability of the Service • Display identity to other users • Notify you of features and updates • Billing and Invoicing • Customer contact enablement, incident response, and customer relationship management • Send you Cisco marketing communications • Authenticate and authorize access to the Service
Host and Usage Data	• Actions Taken • Call Manager Configuration • Call Manager Database • Client Version • Cookies • Device Information • End User IP address (Personal devices) • End User MAC address (Personal devices) • Geolocation • Login Time • MAC address (Non Personal Device) • Operating system (type and version) • System Logs • User Agent Indentifier	We use Host and Usage Information to: • Understand how Service is used • Respond to support requests and diagnose problems • Conduct analytics and aggregate statistical analysis • Improve the Service and other Cisco products and services • Geolocation is used to assign the location details to devices, such as IP phones, to route calls through appropriate Cisco infrastructure
Support Information	• Contact Name (First and Last) • Customer Case Attachments • Customer Support Ticket Number • Organization/Company Name	We use Support Information to: • Deliver and provide operational support for the Service • Diagnose technical issues
System Generated Data	• Call Data Records • Call Details • Device access information	We use System Generated Data to: • To allow customer to generate billing, perform traffic analysis and device usage
User-Generated Data	• Instant messages/chats/conversations • Voice messages	We use User-Generated Information to: • Provide the Service, enabling collaboration among users in different locations

Customer may also collect information, such as call-logs, through on-premise devices (e.g., phones). This information is managed and retained per the Customer's policies.

Cisco Collaboration Flex

With the Flex Plan, you can choose the right subscription based on your business size and needs. The subscription may include Webex Teams and Meetings which collect and process personal information to deliver the respective service. The Webex App and Webex Meetings Privacy Data Sheets describe Cisco's processing of such data.

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 delivers the Service from its own Cisco Webex data centers. 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):

Cisco Data Center Locations
Los Angeles, CA, USA
Reston, VA, USA
San Jose, CA, USA
Dallas, TX, USA
London, UK
Amsterdam, Netherlands
Singapore
Tokyo, Japan
Melbourne, Australia
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

Personal Data Category	Who has access	Purpose of the access
Registration Information	Users through the End-User Portal	Modify, control, and delete information
	Customers and Partners through the Admin Portal	• Manage users and administer Service in accordance with Customer's policies • Modify, control and delete information
	Cisco	Support the Service in accordance with Cisco's data access and security controls process
Host and Usage Information	Customers and Partners through the Admin Portal	• Manage users and administer Service in accordance with Customer's policies • View Call Record Information
	Cisco	• Deliver, support and improve the Service in accordance with Cisco data access and security controls process
User-Generated Information	Users through the End-User Portal	Users may access, modify or delete content that they generate or received in accordance with Customer's personal data policy
	Customers and Partners through the Admin Portal	Modify, control and delete features and phone number assignment
	Cisco	Cisco routes audio and video call content and screen sharing content between call participants, but we do not retain or store the content

5. Data Portability

Personal data is made available in machine readable format through Call Detail Records (CDRs). 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 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	Deleted within 3 months of service termination	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	• Log Files Containing Communications Traffic Data are deleted after 7 years or upon service termination • Call Detail information are deleted after 13 months, or deleted upon request during service termination • All other Host and Usage Information is deleted within 3 months of service termination	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	• User-Generated Information can be deleted at Customer's or user's discretion • Deleted within 3 months of Service Termination	• Recordings are retained in order to provide the Service • Customers have the ability to set organization-wide retention periods for voice communication recordings

7. Personal Data Security

Additional information about our encryption architecture is summarized below:

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

8. Third Party Service Providers (Sub-processors)

Cisco uses suppliers to help provide managed services. With respect to personal data, Cisco supplier agreements requires a substantially similar level of data protection and information security to that of Cisco. In addition, UCM Cloud uses contractors to augment its current staff. Cisco Contractors are required to provide substantially similar security and privacy controls and typically use Cisco technology, tools, and processes. A current list of sub-processors for the service is below:

Sub-processor	Personal Data	Service Type and additional Security Information	Location of Data Center
ServiceNOW	Customer contact information (name, telephone, and email), IP address, device name	Operational Capabilities: https://www.servicenow.com/company/trust.html#	Global
ScienceLogic	IP address; device name	Service Performance: https://sciencelogic.com/product/resources/sciencelogic-platform-security-posture	Global
Splunk	IP address, device name	Service Performance: https://www.splunk.com/en_us/legal/splunk-data-security-and-privacy.html	Global

9. Information Security Incident Management

Breach and Incident Notification Processes

The Information Security 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 and other privacy laws around the world.

Cisco leverages the following privacy transfer mechanisms related to the lawful use of data across jurisdictions:

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

In addition to complying with our stringent internal standards, Cisco also continually maintains third-party validations to demonstrate our commitment to information security. This Service has received the following certifications:

• ISO 27001
• SOC 2 Type II

• SOC 3

11. General Information and GDPR

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

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. For the most current version, go to the Personal Data Privacy section of the Cisco Trust Center.