

Cisco Webex Calling Service

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco Webex Calling Service.

Cisco Webex Calling Service is a cloud-based Cisco Webex Calling Service solution made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from Cisco Webex Calling Service in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the customer relationship. Cisco is the Data Processor for the personal data processed by Cisco Webex Calling Service in order to provide its functionality.

Note that this Privacy Data Sheet is a supplement to the [Cisco Privacy Statement](#).

1. Overview of Webex Calling Service Capabilities

Cisco Webex Calling (the “Service”) is a cloud-based business telephone system made available by Cisco and its resale and wholesale 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 provides a full business telephone system without the requirement of on-premises equipment, and with the added benefits of next generation mobility and scalability.

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.

For a detailed description of the Service, please go [here](#). The Service bundles Cisco Webex Calling and [Cisco Webex App](#), with the options to add [Cisco Webex Meetings](#) & [Dedicated Instance for Webex Calling](#), for a complete collaboration application suite. Webex Calling leverages common Webex portals such as the Cisco Control Hub and other common Webex services. Further information on the common portals and settings may be found in the [Cisco Webex App and Webex Messaging Privacy Data Sheet](#).

Dedicated Instance for Webex Calling is an optional cloud-based business telephone service made available by Cisco and its resale and service provider partners. See Addendum I below for further details.

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.

2. Personal Data Processing

The table below lists the personal data used by the Service to carry out the services and describes why the data is processed.

Webex Calling does not:

- Produce decisions that would result in legal or other significant effects impacting the rights of data subjects based solely by automated means.
- Sell your personal data.
- Serve advertisements on our platform.
- Track your usage or content for advertising purposes.
- Interfere with your calling traffic or content.

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	<ul style="list-style-type: none"> • Authentication Token • Name and Aliases • Email Address • Phone Number • Credentials – User ID, Password, PINs • Cookies • Company Name • Company Contact Name and Title • Company Physical Address • Company Time Zone • Organization ID • Customer Order Information • SIP Identifier • Voicemail Box Number • Device Activation Codes 	<p>We use Registration Information to:</p> <ul style="list-style-type: none"> • Deliver and provide operational support for the Service • Communicate with you on status, features and availability of the Service • Notify you about features and updates • Support billing for the Service • Authenticate and authorize access to the Service • Display Caller ID • Enable Directory Services within your organization • Route calls to your users and places • Allow internal and external dialing • Allow you to activate your IP Phones • Allow you to access your voicemail and voicemail transcriptions • Understand how the Service is used • Send you Cisco marketing communications based on your preferences
Host and Usage Information	<ul style="list-style-type: none"> • Credentials - SIP, Web Interface, XSI • Profile Data - Service Feature Settings • Connectivity Data: <ul style="list-style-type: none"> ○ IP Address ○ MAC Address ○ Device Identifiers – IMEI ○ MSISDN ○ Landline Number ○ SIP Number • Usage Data - Communications Metadata, Call Logs • Call Detail Records (“CDRs”) • Portal Access Details <ul style="list-style-type: none"> ○ Domain Name or IP Address of the User ○ File Name and URL Requested by the Client, ○ Website from Which the User Is Visiting the Service. • Geolocation – Based on IP Address or Device Location • Contact Lists • Cookies • Billing Files • Log Files Containing Communications Traffic Data • Device Name • Time Zone • Universal Unique Identifier • Text messages metadata 	<p>We use Host and Usage Information to:</p> <ul style="list-style-type: none"> • Provide telephone 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 • Support billing for the Service • Provide analytics and reporting capabilities for the organization administrators • Telephony fraud detection
User-Generated Information	<ul style="list-style-type: none"> • Uploaded Media Files Such as Voice Greetings • Voice Messages • Call Recordings • Text messages 	<p>We use User-Generated Information to:</p> <ul style="list-style-type: none"> • Provide the Service, enabling collaboration among users in different locations • Provide customized Music On Hold • Provide voicemail and voicemail transcription services <p>Note: We route audio and video call content and screen sharing content between call participants, but we do not retain or store the content, unless call recording is invoked</p>

Cisco Webex App

Personal Data Processing related to Cisco Webex App is detailed in the [Cisco Webex App and Webex Messaging Privacy Data Sheet](#).

Cisco Webex Meetings

Personal Data Processing related to Cisco Webex Meetings is detailed in the [Cisco Webex Meetings Privacy Data Sheet](#). Voicemail transcription information will be processed for all Customers using the Webex Assistant service. Personal Data Processing related to Webex Assistant is detailed in the [Cisco Webex Meetings Privacy Data Sheet](#).

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. Data Center Locations

The Service 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):

Service Component	Data Center Locations
Core Calling	Melbourne, Australia
	Sydney, Australia
	Frankfurt, Germany
	Osaka, Japan
	Tokyo, Japan
	London, UK
	Chicago, IL, USA
	Council Bluffs, IA, USA
	Los Angeles, CA, USA
	New York, NY, USA
	Dallas, Texas, USA
	Vancouver, Canada
	Toronto, Canada
	Singapore
Common Webex Services	Amsterdam, Holland
	London, UK
	California, USA
	Northern Virginia, USA
	Ohio, USA
	Texas, USA

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. Information will also be accessible to personnel in locations where Cisco has operations.

4. Cross-Border Data Transfer Mechanisms

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

- [Binding Corporate Rules](#)
- [APEC Cross Border Privacy Rules](#)
- [APEC Privacy Recognition for Processors](#)
- [EU Standard Contractual Clauses](#)

5. Access Control

The table below lists the personal data used by Cisco Webex Calling Service to carry out the service, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
Registration Information	Users through the End-User portal	Modify, control, and delete information
	Customer through the Cisco Control Hub portal	<ul style="list-style-type: none"> • Manage users and administer Service in accordance with Customer's policies • Modify, control and delete information
	Partners through the Cisco Control Hub portal	<ul style="list-style-type: none"> • Provision, bill and support the Service in accordance with contract terms • 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	Users through the End-User portal	<ul style="list-style-type: none"> • View interaction information and usage history • Update information such as Service Feature Settings and Contact Lists
	Customer through the Cisco Control Hub portal	Manage users and administer the Service in accordance with Customer's policies
	Partners through the Cisco Control Hub portal	Bill and support the Service in accordance with contract terms
	Cisco	<ul style="list-style-type: none"> • 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 End-User portal	Users may access, modify or delete content that they generated or received in accordance with Customer's personal data policy
	Customer through the Cisco Control Hub portal	Modify, control and delete features and phone number assignment
	Partners through the Cisco Control Hub portal	To comply with customer data extract requests, audit requests or rights of end-users
	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

6. Data Portability

The following personal data is made available in machine readable format: Registration Information, User-Generated Information (excluding Voice Messages), Call Logs, Contact Lists, Service Feature Settings, and 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 7 below. Users have the ability to download Call Logs and Voice Messages through the End-User Portal. Users who want to obtain all other types of available personal data must request it through their organization’s administrator.

7. 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 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 within Webex Calling, the reason why we retain it and the retention period are described in the table below. Data deletion and retention information for Webex App and Webex Meetings can be found in the [Cisco Trust Center](#).

The table below lists the personal data used by Cisco Webex Calling Service, the length of time that data needs to be retained, and why we retain it.

Personal Data Category	Retention Period	Reason for Retention
Registration Information	7 years from when the Service is terminated, or a user is deactivated.	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	<ul style="list-style-type: none"> Credentials, Profile Data, Contact Lists, Geolocation, Connectivity Data and Usage Data are deleted as soon as the Service is terminated, or a user is deactivated. Portal Access Details are deleted after 90 days Log Files Containing Communications Traffic Data are deleted after 30 days, except in the EEA countries and Switzerland where data are deleted after 7 days. CDRs and Call Logs are deleted after 23 months, except in EEA countries and Switzerland where data are deleted after 6 months. Billing Files are deleted after 7 years. 	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	<ul style="list-style-type: none"> User may delete voicemails at any time Data such as voicemails are deleted as soon as the Service is terminated, or a user is deactivated Call recordings are deleted after 40 days Uploaded Media Files are deleted as soon as the Service is terminated, or a user is deactivated Text messages are deleted after 400 days 	<ul style="list-style-type: none"> Communication recordings, texts, and histories are retained to provide the Service Customers can set organization-wide retention periods for voice communication recordings Uploaded Media Files are not retained on the Service when Customer or a user deletes this data

8. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

The Service is ISO 27001: 2013 and SOC 2 Type I certified 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 for Webex Calling is summarized below. Information about encryption architecture for Webex App may be referenced in the [Cisco Webex App and Webex Messenger Privacy Data Sheet](#).

Personal Data Category	Security Controls and Measures
Registration Information	<ul style="list-style-type: none"> • Encrypted in transit across all regions. • Encrypted at rest across all regions. • All authentication passwords are protected via encryption or hashing algorithms.
Host and Usage Information	<ul style="list-style-type: none"> • Encrypted in transit and at rest across all regions. . • All authentication passwords are protected via encryption or hashing algorithms
User-Generated Information	<ul style="list-style-type: none"> • Encrypted in transit across all regions, dependent on the IP device’s encryption support capabilities. • Voicemail files and transcription files are encrypted at rest for all regions.

The Service uses different kinds of encryption to protect different kinds of data in transit and in storage. In this section, “you” and “your” refers to the user.

Media encryption

Media encryption is used to protect the audio, video, screen sharing data, call recordings and voicemails that you transmit during a call. When you make a call, media is encrypted from your device to our servers. It may be decrypted on our servers so that we can manage the call. It is re-encrypted before being sent to the other participants on the call unless they are connected via the public telephone network or do not support encryption. Voicemails and voicemail transcriptions transmitted via email are not encrypted.

Transport encryption

Transport encryption (also known as HTTPS) is used to protect all connections to and from the Service other than voice and video calls.

Additional controls include:

- All backups are encrypted.
- Access to call recording files are limited and controlled based on least privilege.
- All Cisco employees, vendors and contractors are authenticated prior to gaining access to information systems.
 - Regular audits are conducted to address the ongoing confidentiality, integrity, availability and resilience of Cisco processing systems and services

9. 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. We do not rent or sell your information. A current list of third-party service providers with access to personal data can be provided upon request.

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	Registration Information, Host and Usage Information, User-Generated Content	Data Center and Hosting Provider	United States Germany Netherlands United Kingdom Brazil Australia Japan Singapore

Dubber	Registration Information	Call Recording Cloud Solution- only if the call recording solution is enabled by the customer	United States United Kingdom Germany Japan Australia
LogiSense	Registration Information, Host and Usage Information	Billing Solution Provider-only if the billing service is purchased by the customer	United States United Kingdom
RedSky	Registration Information	E911 Service Provider for USA and Canada	United States
Tango Networks	Registration Information	Webex Go/ eSIM Provider	United States United Kingdom
Telynx	Registration Information	Cisco Calling Plan Service Provider – only if the Cisco Calling Plan service is purchased by the customer	United States United Kingdom

10. 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.

11. Certifications and Compliance with Privacy Laws

The Security & 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. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

In addition to the Cross-Border Data Transfer Mechanisms/Certifications listed in Section 4, Cisco has the following:

- [EU-US Privacy Shield Framework](#)
- [Swiss-US Privacy Shield Framework](#)

Further, in addition to complying with our stringent internal standards, Cisco also 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
- HIPAA Attestation

12. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.

We will confirm identification (typically with the email address associated with a Cisco account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the

Customer/Controller, may be redirect to their employer for a response.

Requests can be made by submitting a request via:

- 1) the Cisco [Privacy Request form](#)
- 2) by postal mail:

Chief Privacy Officer Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES		
Americas Privacy Officer Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES	APJC Privacy Officer Cisco Systems, Inc. Bldg 80, Lvl 25, Mapletree Biz City, 80 Pasir Panjang Road, Singapore, 117372 SINGAPORE	EMEAR Privacy Officer Cisco Systems, Inc. Haarlerbergweg 13-19, 1101 CH Amsterdam-Zuidoost NETHERLANDS

We will endeavor to timely and satisfactorily respond to inquiries and requests. If a privacy concern related to the personal data processed or transferred by Cisco remains unresolved, contact Cisco's [US-based third-party dispute resolution provider](#). Alternatively, you can contact the data protection supervisory authority in your jurisdiction for assistance. Cisco's main establishment in the EU is in the Netherlands. As such, our EU lead authority is the Dutch [Autoriteit Persoonsgegevens](#).

13. General Information

For more general information and FAQs related to Cisco's Security and Privacy Program 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.

Addendum I: Dedicated Instance for Webex Calling

This Addendum describes the processing of personal data (or personal identifiable information) for Dedicated Instance for Webex Calling.

1. Overview

Dedicated Instance for Webex Calling 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”).

Dedicated Instance for Webex Calling is part of Cisco’s Cloud Calling portfolio powered by Cisco’s call control engine – CUCM. Dedicated Instance for Webex Calling is bundled as part of Cisco Collaboration Flex Plan 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

The table below lists the personal data used by the Service to carry out the services and describes why the data is processed.

Dedicated Instance for Webex Calling does not:

- Produce decisions that would result in legal or other significant effects impacting the rights of data subjects based solely by automated means.
- Sell your personal data.
- Serve advertisements on our platform.
- Track your usage or content for advertising purposes. Interfere with your calling traffic or content.

If you are a user of the Service, the information described in this Addendum 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

Registration Information	<ul style="list-style-type: none"> 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 Phone Number (Mobile, Work) User Name 	<p>We use Registration Information to:</p> <ul style="list-style-type: none"> 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 Provide the Service
Host and Usage Information	<ul style="list-style-type: none"> 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 Identifier 	<p>We use Host and Usage Information to:</p> <ul style="list-style-type: none"> 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
User-Generated Information	<ul style="list-style-type: none"> Instant messages/chats/conversations Voice messages 	<p>We use User-Generated Information to:</p> <p>Provide the Service, enabling collaboration among users in different locations</p>
System Generated Information	<ul style="list-style-type: none"> Call Data Records Call Details Device access information 	<p>We use System Generated Data to:</p> <p>To allow customer to generate billing, perform traffic analysis and device usage</p>
Support Information	<ul style="list-style-type: none"> Contact Name (First and Last) Customer Case Attachments Customer Support Ticket Number Organization/Company Name 	<p>We use Support Information to:</p> <ul style="list-style-type: none"> Deliver and provide operational support for the Service Diagnose technical issues

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.

3. Data Center Locations

Dedicated Instance for Webex Calling 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):

Data Center Locations
Melbourne, Australia
Sydney, Australia
Tokyo, Japan

Data Center Locations
Singapore
Amsterdam, Holland
London, UK
Los Angeles, CA, USA
Dallas, Texas, USA

Information is stored in the data center closest to a Customer’s principal geographic region as provided to Cisco by the Partner during the ordering process. TAC Information is stored in Cisco data centers. Information will also be accessible to personnel in locations where Cisco has operations.

4. Access Control

The table below lists the personal data used by Dedicated Instance for Webex Calling to carry out the service, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
Registration Information	Users through the End-User portal	Modify, control, and delete information
	Customer through the Cisco Control Hub portal	<ul style="list-style-type: none"> Manage users and administer Service in accordance with Customer’s policies Modify, control and delete information
	Partners through the Cisco Control Hub portal	<ul style="list-style-type: none"> Provision, bill and support the Service in accordance with contract terms 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	Users through the End-User portal	<ul style="list-style-type: none"> View interaction information and usage history Update information such as Service Feature Settings and Contact Lists
	Customer through the Cisco Control Hub portal	Manage users and administer the Service in accordance with Customer’s policies
	Partners through the Cisco Control Hub portal	Bill and support the Service in accordance with contract terms
	Cisco	<ul style="list-style-type: none"> 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 End-User portal	Users may access, modify or delete content that they generated or received in accordance with Customer’s personal data policy
	Customer through the Cisco Control Hub portal	Modify, control and delete features and phone number assignment
	Partners through the Cisco Control Hub portal	To comply with customer data extract requests, audit requests or rights of end-users

	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
System Generated Information	Cisco	Used for on-going operation of the service and may include accessing logs, debug information and monitoring data
Support Information	Cisco	Used to resolve service issues and requires access to tickets created by users and associated event data provided by the user

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 the Data Deletion & Retention section.

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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> User-Generated Information can be deleted at Customer's or user's discretion Deleted within 3 months of service termination 	<ul style="list-style-type: none"> Recordings are retained in order to provide the Service Customers have the ability to set organization-wide retention periods for voice communication recordings
System Generated Info	<ul style="list-style-type: none"> Traps and logs are retained for 18 months or within 3 months of service termination Diagnostic data retained for 24 months or within 3 months of service termination 	<ul style="list-style-type: none"> 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 operations and audit policy.

Personal Data Category	Retention Period	Reason for Retention
Support Information	<ul style="list-style-type: none"> Tickets and associated events are retained for 7 years Standard reports are retained for up to 3 years. 	<ul style="list-style-type: none"> Information generated by support ticketing systems and standard reports is kept as part of Cisco's record of Service delivery and audit policy.

7. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

The Service is ISO 27001: 2013 and SOC 2 Type I certified 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 for Webex Calling is summarized below. Information about encryption architecture for Webex App may be referenced in the Cisco Webex App and Webex Messenger Privacy Data Sheet Cisco Webex App and Webex Messenger Privacy Data Sheet.

Personal Data Category	Security Controls and Measures
Registration Information	<ul style="list-style-type: none"> Encrypted in transit across all regions. Encrypted at rest across all regions. All authentication passwords are protected via encryption or hashing algorithms.
Host and Usage Information	<ul style="list-style-type: none"> Encrypted in transit and at rest across all regions. . All authentication passwords are protected via encryption or hashing algorithms
User-Generated Information	<ul style="list-style-type: none"> Encrypted in transit across all regions, dependent on the IP device's encryption support capabilities. Voicemail files and transcription files are encrypted at rest for all regions.
System Generated Information	<ul style="list-style-type: none"> Encrypted in transit across all regions. Encrypted at rest across all regions. All authentication passwords are protected via encryption or hashing algorithms.
Support Information	<ul style="list-style-type: none"> Encrypted in transit across all regions. Encrypted at rest across all regions. All authentication passwords are protected via encryption or hashing algorithms.

The Service uses different kinds of encryption to protect different kinds of data in transit and in storage. In this section, "you" and "your" refers to the user.

Media encryption

Media encryption is used to protect the audio, video, screen sharing data, call recordings and voicemails that you transmit during a call. When you make a call, media is encrypted from your device to our servers. It may be decrypted on our servers so that we can manage the call. It is re-encrypted before being sent to the other participants on the call unless they are connected via the public telephone network or do not support encryption. Voicemails and voicemail transcriptions transmitted via email are not encrypted.

Transport encryption

Transport encryption (also known as HTTPS) is used to protect all connections to and from the Service other than voice and video calls.

Additional controls include:

- All backups are encrypted.
- Access to call recording files are limited and controlled based on least privilege.
- All Cisco employees, vendors and contractors are authenticated prior to gaining access to information systems.
 - Regular audits are conducted to address the ongoing confidentiality, integrity, availability and resilience of Cisco processing systems and services

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, Dedicated Instance for Webex Calling 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. Exercising Data Subject Rights

Users whose personal data is processed by the Service can contact their Partner to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.