Webex Calling

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

Webex Calling (“the “Service” or “Webex Calling”) is a cloud-based business telephone system made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from 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

Webex Calling 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 Webex Calling and the Webex App with the options to add Webex Meetings and Dedicated Instance for Webex Calling, for a complete collaboration application suite. Webex Calling leverages common Webex portals such as the Control Hub and other common Webex services. Further information on the common portals and settings may be found in the 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	• Authentication Token • Name and Aliases • Email Address • Phone Number • Credentials – User ID, Password, PINs • Cookies • SIP Identifier • Voicemail Box Number • Device Activation Codes • Unique User ID (UUID) (a pseudonymized 128-bit number assigned to compute nodes on a network)	We use Registration Information to: • 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	• Credentials - SIP, Web Interface, XSI
	• Profile Data - Service Feature Settings
	• Connectivity Data:
	  ○ IP Address
	  ○ MAC Address
	  ○ Device Identifiers – IMEI
	  ○ MSISDN (eSIM phone number)
	  ○ Landline Number
	  ○ SIP Number
	• Usage Data - Communications Metadata, Call Logs
	• Call Detail Records (“CDRs”)
	• Portal Access Details
	  ○ 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
		We use Host and Usage Information to:
		• 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	• Uploaded Media Files Such as Voice Greetings • Voice Messages • Call Recordings • Text messages	We use User-Generated Information to: • Provide the Service, enabling collaboration among users in different locations • Provide customized Music on Hold • Provide voicemail and voicemail transcription services

		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
Webex- Generated Content	• Post-Call Summaries (optional, only applicable if the post-call summary feature is enabled by you)	• Provide you with the Service

Webex App
Personal Data Processing related to Webex App is detailed in the Webex App & Messaging Privacy Data Sheet.

Webex Meetings
Personal Data Processing related to Webex Meetings is detailed in the 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 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):

Webex Calling Data Centers

Geo	Location
North America	Chicago, IL, U.S.
	Dallas, TX, U.S.
	Vancouver, Canada
	Toronto, Canada
Europe	Amsterdam, Netherlands
	Frankfurt, Germany
	Manchester, UK
	London, UK
Asia Pacific	Melbourne, Australia
	Sydney, Australia
	Osaka, Japan
	Tokyo, Japan
	Jeddah, Saudi Arabia
	Riyadh, Saudi Arabia

Information is stored in the data center in Customer's region as provided to Cisco 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. Webex Data Residency

Webex Calling data residency provides Customer user administrators (or partner administrators on the Customer's behalf) the ability to choose where their organization's data is stored.

The first location that a Customer user administrator chooses to create in Control Hub is where the Customer's core calling and public switched telephone network ("PSTN") services are provisioned (such location is the Customer's "Calling Region"). For paid user accounts, including for EU Customers, personal data processed by Webex Calling will be stored in the Calling Region (other than as noted below). For free user accounts, personal data processed by Webex Calling may be stored in a Webex data center outside the account holder's region, including for EU Customers.

To facilitate certain operations and aspects of the Service, certain exceptions to Webex Calling data residency exist; specifically, cross-border transfers of personal data may still occur when (a) a user registers on any Cisco platform (for example, through www.cisco.com), (b) a Customer provides ordering information (business contact information); (c) a user engages in collaboration with users outside of their Calling Region (d) a user requests technical support, including through Cisco TAC (in which case the information that a user provides within the initial TAC request may be transferred outside the Calling Region; (e) a user enables certain optional functionalities; (f) a user enables cell phone "push" notifications (in which case the cell phone provider associated with iOS or Android functionality may transfer data outside of the Calling Region); or (g) some personal data, including logs, analytics, and user registration/directory information which are provided by core common Webex services will be stored where the Customer user administrator has configured their Control Hub to use these services.

Note that in order to provide our best-in-class experience, users' devices and clients may connect to the geographically closest Webex Calling data center to keep the call as local as possible to the user's current location. If an organization is using Cloud Connected PSTN (CCP) , this will also mean the PSTN breakout is in that geographically closest region. For more information on Regional Media see https://help.webex.com/en-us/article/nixlytw/Webex-Calling-Regional-Media-for-Cloud-Connected-PSTN-(CCP)..

5. 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 (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses
- EU-U.S. Data Privacy Framework and the U.K. Extension to the EU-U.S. Data Privacy Framework
- Swiss-U.S. Data Privacy Framework

6. 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 Control Hub portal	• Manage users and administer Service in accordance with Customer's policies • Modify, control and delete information
	Partners through the Control Hub portal	• 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	• View interaction information and usage history • Update information such as Service Feature Settings and Contact Lists
	Customer through the Control Hub portal	Manage users and administer the Service in accordance with Customer's policies
	Partners through the Control Hub portal	Bill and support the Service in accordance with contract terms
	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 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 Control Hub portal	Modify, control and delete features and phone number assignment
	Partners through the 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
Webex-Generated Content	Users through the End-User portal	Modify, control, and delete based on user's preference
	Customer through the Control Hub portal	Modify, control, and delete in accordance with Customer's personal data policy
	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer, and will only access it in accordance with Cisco's data access and security controls process

7. 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 8 below. Users have the ability to download 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.

8. 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 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	13 months 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. Account information provided to Cisco during the provisioning of the services is maintained for billing purposes.
Host and Usage Information	• 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 is deleted after 7 days. • CDRs and Call Logs are deleted after 23 months, except in EEA countries and Switzerland where data is deleted after 13 months. •	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 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 360 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	• 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
Webex-Generated Content	• At Customer's or user's discretion	Webex-Generated Content generally is not retained when Customer or user deletes this data.

9. 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 Webex App & Webex Messaging Privacy Data Sheet.

Personal Data Category	Security Controls and Measures
Registration Information	• 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	• Encrypted in transit and at rest across all regions. • All authentication passwords are protected via encryption or hashing algorithms
User-Generated Information	• Encrypted in transit across all regions, dependent on the IP device's encryption support capabilities. • Voicemail messages, voicemail transcriptions, voice recordings and fax messages are encrypted at rest for all regions. • Cisco encryption keys are stored and managed by the Webex Cloud Key Management System (KMS) by default. Customers with the Pro Pack for Control Hub add-on may choose to upload and manage their own encryption keys to KMS though Control Hub or use their own key management system (hybrid data security) and keys.
Webex-Generated Information	• Encrypted in transit and at rest across 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 use opportunistic encryption.

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 is 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

10. 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	Host and Usage Information, User-Generated Content	Data Center and Hosting Provider	United States Germany Netherlands United Kingdom Brazil Australia Japan Singapore

Call Cabinet	Registration Information	Call Recording Cloud Solution- only if the call recording solution is enabled by the customer	United States United Kingdom Europe Australia
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
Imagicle	Registration Information	Attendant Console for Webex Calling – only if purchased by the customer Call Recording Cloud Solution- only if the call recording solution is enabled by the customer	United States Canada United Kingdom Germany Japan Australia
Intelepeer	Registration Information	Cisco Calling Plan Service Provider – only if the Cisco Calling Plan service is purchased by the customer	United States
LogiSense	Registration Information, Host and Usage Information	Billing Solution Provider-only if the billing service is purchased by the customer	United States United Kingdom
Microsoft Azure	Registration Information, Host & Usage Information, User Generated Information, Webex Generated Content	Microsoft is leveraged to provide certain AI features (call summary, call transcription or action-items)– only if these features are enabled by the customer	Germany Japan United Kingdom United States Canada Australia
RedSky	Registration Information	E911 Service Provider for USA and Canada	United States
Sinch	Registration Information	Cisco Calling Plan Service Provider – only if the Cisco Calling Plan service is purchased by the customer	United States
Spark NZ	Registration Information, Host and Usage Information, User-Generated Content	Webex Go/ eSIM Provider	United States Canada United Kingdom France Germany New Zealand
Tango Networks	Registration Information, Host and Usage Information, User-Generated Content	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
TransUnion	Registration Information	TransUnion is used to lookup the caller name, which is required for delivery of the Calling service.	United States

11. 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.

12. 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.

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:

- EU Cloud Code of Conduct Adherence by SCOPE Europe
    - For more information about the EU Cloud of Conduct see: Cisco Webex EU Cloud Code of Conduct and the Verification of Declaration of Adherence.
-
- ISO27001ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27701:2019 Certification
- ISO 22301 (Business Continuity Management System)SOC 2 Type II Report
-
- BSI Cloud Computing Compliance Criteria Catalogue (German C5)
- CSA STAR Level 2 Certification
- FedRAMP
- HIPAA Attestation
- Spanish Esquema Nacional de Seguridad Certification
- Australian IRAP (Information Security Registered Assessors Program) Certification
- Digital Trust Label (Switzerland)
- Electronic Transactions Development Agency Certification (Thailand)
- French Health Data Hosting (Hébergeurs de Données de Santé – HDS) Certification
    - The HDS certification (found on the Cisco Trust Portal) applies to the Webex service provisioned in the European Economic Area (EEA).

13. 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 redirected 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	**EMEA 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 Autoritiet Persoonsgegevens.

14. 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 (Cisco Unified Communications Manager). 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	• 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	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 • Provide the Service

Host and Usage Information	• 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	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
User-Generated Information	• Instant messages/chats/conversations • Voice messages •	We use User-Generated Information to: Provide the Service, enabling collaboration among users in different locations
System Generated Information	• 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
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

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
Amsterdam, Netherlands
Dallas, Texas, USA
Frankfurt, Germany
London, UK
Los Angeles, CA, USA
Melbourne, Australia
Singapore, Singapore
Sydney, Australia
Tokyo, Japan
Washington, District of Columbia, 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 Control Hub portal	· Manage users and administer Service in accordance with Customer's policies · Modify, control and delete information
	Partners through the Control Hub portal	· 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	· View interaction information and usage history · Update information such as Service Feature Settings and Contact Lists
	Customer through the Control Hub portal	Manage users and administer the Service in accordance with Customer's policies
	Partners through the Control Hub portal	Bill and support the Service in accordance with contract terms
	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 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 Control Hub portal	Modify, control and delete features and phone number assignment
	Partners through the 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	• 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 13 months or upon service termination • Call Detail information is 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.
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 to provide the Service • Customers have the ability to set organization-wide retention periods for voice communication recordings
System Generated Info	• 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	• 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.
Support Information	• Tickets and associated events are retained for 13 months • Standard reports are retained for up to 3 years.	• 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 Webex App and Webex Messenger Privacy Data Sheet.

Personal Data Category	Security Controls and Measures
Registration Information	• 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	• Encrypted in transit and at rest across all regions. • All authentication passwords are protected via encryption or hashing algorithms

User-Generated Information	• 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	• Encrypted in transit across all regions. • Encrypted at rest across all regions. • All authentication passwords are protected via encryption or hashing algorithms.
Support Information	• 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.

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 is 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 require 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.