Webex Meetings

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

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

Cisco will process personal data from Webex Meetings 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 Webex Meetings to provide its functionality.[1]

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

Webex Meetings (the "Service" or "Webex Meetings") is a cloud-based web and video conferencing solution made available by Cisco to companies or persons ("Customers," "you," or "your") who acquire it for use by their authorized users (each, a "user"). The Service enables global employees and virtual teams to collaborate in real time from anywhere, anytime, on mobile devices or video systems as though they were working in the same room. Solutions include meetings, events, training, and support services. For more information regarding optional features for Webex Meetings, please see the Addendums below.

Because the Service enables collaboration among its users, as described below, your personal data is required to use the Service. The following paragraphs describe Cisco's processing of personal data in connection with the delivery of 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 to serve the legitimate interests and fulfill the contractual obligations of providing the Service.

This Privacy Data Sheet covers Webex Meetings, Webex Webinars, Webex Training, and Webex Support. If you use the Service together with the Webex App, see the Webex App Privacy Data Sheet (available on The Cisco Trust Center) for descriptions of the data that may be collected and processed in connection with those services.

For a detailed overview of the Service, please visit the Cisco Web Conferencing homepage.

2. Personal Data Processing

The Service allows users to instantly connect in a way that is almost as personal as a face-to-face meeting. If you are a user and your employer is the Customer that acquired the Service, your employer serves as the "data controller" of data processed by the Service (see the Webex Meetings Privacy Data Map for a visualization of who is doing what with data). The information described in the table below and in this Privacy Data Sheet is accessible to your employer and is subject to your employer's policies regarding access, use, monitoring, deletion, preservation, and export of information associated with the Service.

Similarly, if users participate in meetings hosted by users in other companies, the meeting host and/or co-host will control any meeting recordings or files shared during the meeting, which will be subject to the host's corporate policies regarding access, use, monitoring, deletion, preservation, and export of information. The meeting host has the option to record meetings, which may be shared with others or discoverable in a legal matter. In addition, meeting co-hosts and participants may also have the option to record meetings, if this feature is enabled by the Customer in Webex Control Hub. The meeting host should inform all meeting attendees prior to recording and Webex Meetings displays a red circle and plays an audio prompt to all participants indicating that the meeting is being recorded. Note, Cisco has no control over, and is not responsible or liable for the privacy of

[1] Cisco may process some personal data from Webex Meetings to serve its legitimate interests to manage its business, improve offerings, and better understand customer needs and preferences. In such instances, Cisco is the Data Controller of data processed for these purposes. In doing so, Cisco has taken into account its interests and those of the individuals and balanced it against any potential impact or reasonable expectation of individual privacy. In such cases, individuals will have the right to object to such processing at any time under the conditions set out in the applicable laws. For details on how to exercise the right to object, please see Section 12 Exercising Data Subject Rights of this Privacy Data Sheet.

any information that you have shared with others. Even after you remove information from the Webex Meetings platform, copies of that information may remain viewable elsewhere to the extent it has been shared with others.

Webex Meetings 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.
- Monitor or interfere with you your meeting traffic or content.
- Monitor or track user geolocation.

The table below lists the personal data processed by Webex Meetings to provide its services and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
User Information	• Name • Email Address • Password • Browser • Phone Number (Optional) • Mailing Address (Optional) • Profile Picture or Avatar image (optional, only applicable if provided by you) • User Information Included in Your Directory (if synced) • Unique User ID (UUID) (a pseudonymized 128-bit number assigned to compute nodes on a network)	As a processor: • Provide you with the Service • Enroll you in the Service • Respond to Customer support requests • Authenticate and authorize access to your account • Display directory information to other Webex users • Display your user avatar and profile to other users (Avatar may be cached locally on devices of other Webex users that attend meetings with you for a period of 2 weeks) As a controller: • Make improvements to the Service and other Cisco products and services • Customer relationship management (e.g., transactional communication) • Bill you for the Service
Host and Usage Information	• IP Address • User Agent Identifier • Hardware Type • Operating System Type and Version • Client Version • IP Addresses Along the Network Path MAC Address of Your Client (as applicable) • Service Version • Actions Taken • Geographic Region (i.e., Country Code) • Meeting Session Information (e.g., date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity) • Number of Meetings • Number of Screen-Sharing and NonScreen-Sharing Sessions • Number of Participants • Screen Resolution • Join Method • Performance, Troubleshooting, and Diagnostics Information	As a processor: • Provide you with 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 Cisco may use metadata from Webex Meetings (e.g., meeting participants, frequencies) to: • Help organize, sort, and/or prioritize your Webex App messages or spaces in a way that is relevant to you and your work • Provide you the Collaboration Insights feature (including Personal Insights) (optional) As a controller: • Make improvements to the Service and other Cisco products and services • Understand how the Service is used

	• Meeting Host Information[2]
	  ○ Host Name and Email Address
	  ○ Meeting Site URL
	  ○ Meeting Start/End Time
	• Meeting Title
	• Call Attendee Information, including Email Addresses, IP Addresses, Usernames, Phone Numbers, Room Device Information
	• Information Submitted Through Attendee Registration Form (optional, only applicable if provided by you)	

User-Generated Information	• Meeting Recordings (if enabled by Customer) • Transcriptions of Meeting Recordings (optional, only applicable if enabled by you) • Uploaded Files (for Webex Webinars and Training only) • Whiteboard content (optional, only applicable if enabled by you)	As a processor: • Provide you with the Service No uses as a controller

Calendar
If you use a Webex plug-in with your Calendar service or utilize Webex Hybrid Calendar Services, we will only use the data set forth above regarding meeting dates, times, title and participants. For more information on Webex Hybrid Calendar Service see the Office 365 and Google Calendar integration references.

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.

Control Hub
Webex Control Hub analytics provides usage trends and valuable insights that can be used to help with strategies to promote and optimize adoption across teams. Webex Control Hub analytics uses Host and Usage Information to provide advanced analytics capabilities and reports.

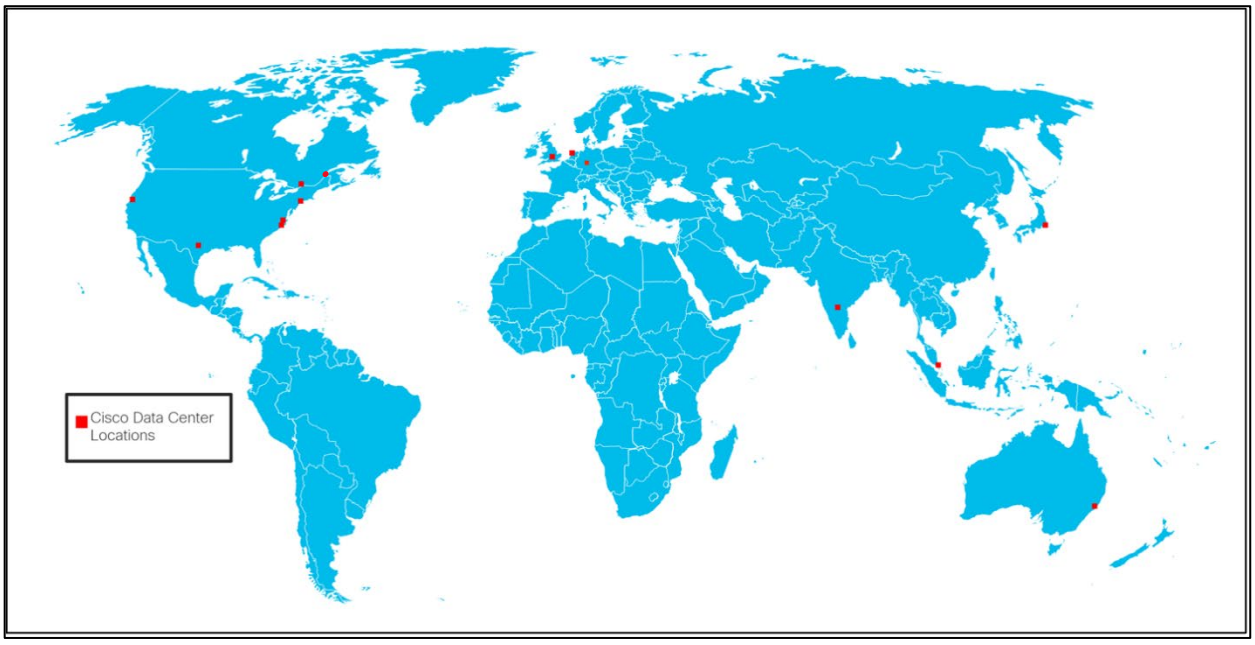
Polling
As a presenter, you can use a poll to create and share questionnaires. Any polling data collected from participants will be deleted once the meeting has ended. Some Webex Meetings may feature Slido, which is a cloud-based polling and Q&A solution; for details around the processing of personal data by the Slido feature, please see Addendum 6 to this Privacy Data Sheet.

Extended Security Pack
If you purchase the extended security pack, please see the Cloudlock Privacy Data Sheet for Cloudlock data privacy information.

3. Data Center Locations

The Service leverages its own data centers to deliver the Service globally. If you join a meeting using Webex App, please see the Webex App Privacy Data Sheet for applicable privacy information, including data center locations. The Webex Meetings data centers are currently located in the following countries (data center locations may change from time to time and this Privacy Data Sheet will be updated to reflect those changes):

[2] Used for billing purposes.



User-Generated Information is stored in the data center in Customer's region as provided during the ordering process. Data is replicated across data centers within the same region to ensure availability.

An Internet Point of Presence (iPOP) Location is used to route traffic geographically from nearby areas to a Cisco Data Center Location. It is intended to route Webex Meetings traffic through Cisco's infrastructure and improve performance. Data routed through iPOP Locations remains encrypted and is not stored in that location.

For free user accounts, the data defined in this Privacy Data Sheet may be stored in a Webex data center outside the account holder's region.

Cisco Data Center Locations	Internet Point of Presence (iPOP) Locations
Amsterdam, Netherlands	Amsterdam, Netherlands
Bangalore, India	California, USA
California, USA	Illinois, USA
Frankfurt, Germany	New Jersey, USA
London, UK	Sydney, Australia
Montreal, Canada	Texas, USA
New York, USA	
North Carolina, USA	
Singapore, Singapore	
Sydney, Australia	

Texas, USA	
Toronto, Canada	
Virginia, USA	

4. Webex Data Residency

Webex data residency provides Customer user administrators the ability to choose where their organization's data is stored. Data residency is currently available for Customers in the European Union (EU) ("EU Customers") and Customers in Canada ("Canadian Customers") for personal data processed by Webex Meetings, including User Information, Host & Usage Information, and User-Generated Information (other than as noted below).[3] EU Customers that became Webex Meetings Customers after July 2021, can choose to provision their data in the EU. For EU Customers who were provisioned before July 2021, user administrators were offered the option to migrate their user data to the EU, and this was completed as of December 2021. Canadian Customers that became Webex Meetings Customers after July 2022, can choose to provision their data in Canada. For Canadian Customers who were provisioned before July 2022, user administrators were offered the option to migrate their user data to Canada.

To facilitate certain operations and aspects of the Service, certain exceptions to Webex 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.webex.com or www.cisco.com) or through any Cisco service to learn more about Cisco products or events; (b) a Customer provides ordering information (business contact information); (c) a user engages in collaboration with users outside of their 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 region); (e) a user enables certain optional functionalities; or (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 region).

For free user accounts, the data defined in this Privacy Data Sheet may be stored in a Webex data center outside the account holder's region, including for EU and Canadian Customers.

5. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

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

6. Access Control

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

Personal Data Category	Who has Access	Purpose of the Access
User Information	• User through My Webex Page	• Modify, control, and delete User Information
	• Customer through the Site Admin Page or Webex Control Hub	• Modify, control, and delete in accordance with Customer's personal data policy
	• Cisco	• Support the Service in accordance with Cisco's data access and security controls process
Host and Usage Information	• Host through the My Webex Page	• View meeting session information
	• Customer may view this information through the Site Admin Page, Webex Control Hub,	• View usage, meeting session and configuration information

[3] For Canadian Customers, certain Usage Information, including Usage Information related to billing will continue to be stored in the US.

	or may be otherwise provided by Cisco	
	• Cisco	• Support and improvement of the Service by the Webex Meetings support and development team
User-Generated Information	• User through the My Webex Page	• Modify, control, and delete based on user's preference
	• Customer using APIs provided with the Service or through the Site Admin Page or Webex Control Hub	• 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
	• Other Customers and users (when shared during a meeting)	• Content you choose to share during a meeting may be accessed by users in the meeting, wherever they are located. Even after you remove information from the Service, copies of that content may remain viewable elsewhere to the extent it has been shared with others

7. Data Portability

The Service allows Customers and users to export all User-Generated Information. A Customer's administrator may do so using APIs provided with the Service (recordings only) or through the Site Admin Page; while individual users may do so through the My Webex Page. Meeting recordings are available in standard mp4 format.

Customers are permitted to export personal data collected about their users on the Webex Meetings platform using APIs or via the Site Admin Configuration.

8. Data Deletion and Retention

Subject to their employer's corporate retention policies, users with an active subscription can delete User-Generated Information from their account through the My Webex Page at any time during the term of their subscription. Users with an active enterprise or paid online subscription may also request their organization's full administrator(s) to delete their host and usage information. Enterprise Customers have the ability to set organization-wide retention periods for recordings using APIs. Cisco provides free account users up to 6 months of free storage.

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

Users seeking deletion of User Information and User-Generated Information retained on their employer's Webex Meetings site must request deletion from their employer's site administrator.

Type of Personal Data	Retention Period	Reason for Retention
User Information	Active Subscriptions: • User Information will be maintained as long as Customer maintains active subscription (paid or free) Terminated Service: • Deleted once the Service is terminated • Name and UUID are maintained 7 years from termination	Name and UUID are maintained 7 years from termination as part of Cisco's business records and are maintained to comply with Cisco's financial and audit requirements. Any billing information is also subject to this retention period.

Host and Usage Information	13 months	Host and Usage Information such as analytics and troubleshooting is kept to provide technical support when requested by customers and to improve the experience for Webex users. * Any billing information is retained for 7 years as part of Cisco's business records and are maintained to comply with Cisco's financial and audit requirements. Once the specified retention period has expired, data will be deleted.
User-Generated Information	Active Subscriptions: • At Customer's or user's discretion Terminated Service: • Deleted within 60 days	User-Generated Information, except for recordings, is not retained on the Webex Meetings platform when Customer or user deletes this data. Recordings are "soft deleted" and retained for 30 days before being removed from the platform, to allow a Customer or user to retrieve a recording they have inadvertently deleted. User-Generated Information is retained for 60 days after services are terminated to give Customers opportunity to download.

9. Personal Data Security

The Service adopts technical and organizational security measures designed to protect your personal data from unauthorized access use or disclosure. Additional information about our encryption architecture is summarized in the table and paragraphs below.

Personal Data Category	Security Controls and Measures
User Information	Encrypted in transit and at rest
Passwords (stored if Single Sign On is not configured)	Encrypted and hashed in transit and at rest
Host and Usage Information	Encrypted in transit and at rest
User-Generated Information	Recordings prior to May 2018 were encrypted in transit with the option to encrypt at rest. Recordings created after May 2018 are encrypted in transit and at rest by default. Recordings created in the Webex Meetings FedRAMP-Authorized service after October 2019 are encrypted in transit and at rest.

Protecting Data at Rest

The Service encrypts User Information, Passwords and User-Generated Information, as described above, at rest.

Encryption of Data in Transit

All communications between cloud registered Webex App, Webex Room devices and Webex services occur over encrypted channels. Webex uses the TLS protocol with version 1.2 or later with high strength cipher suites for signalling.

After a session is established over TLS, all media streams (audio VoIP, video, screen share, and document share) are encrypted.

Encrypted media can be transported over UDP, TCP, or TLS. Cisco prefers and strongly recommends UDP as the transport protocol for Webex voice and video media streams. This is because TCP and TLS are connection orientated transport protocols, designed to reliably deliver correctly ordered data to upper-layer protocols. Using TCP or TLS, the sender will retransmit lost packets until they are acknowledged, and the receiver will buffer the packet stream until the lost packets are recovered. For media streams over TCP or TLS, this behaviour manifests itself as increased latency/jitter, which in turn affects the media quality experienced by the call's participants.

Media packets are encrypted using either AES 256 or AES 128 based ciphers. The Webex App and Webex Room devices use AES-256-GCM to encrypt media; these media encryption keys are exchanged over TLS-secured signalling channels. SIP and H323 devices that support media encryption with SRTP can use AES-256-GCM, AES-128-GCM, or AES-CM-128-HMAC-SHA1 (AES-256-GCM is the Webex preferred media encryption cipher).

Zero Trust Security Based End-to-End Encryption

For standard Webex Meetings, where devices and services use SRTP to encrypt media on a hop by hop basis, Webex media servers need access to the media encryption keys to decrypt the media for each SRTP call leg. This is true for any conferencing

provider that supports SIP, H323, PSTN, recording and other services using SRTP.

However, for businesses requiring a higher level of security, Webex also provides end-to-end encryption for meetings ("Webex Zero Trust Security end-to-end encryption"). With this option, the Webex cloud does not have access to the encryption keys used by meeting participants and cannot decrypt their media streams. Webex Zero Trust Security end-to-end encryption uses standard track protocols to generate a shared meeting encryption key (Messaging Layer Security (MLS)) and to encrypt meeting content (Secure Frame (S-Frame). With MLS, the meeting encryption key is generated by each participant's device using a combination of the shared public key of every participant and the participant's private key (never shared). The meeting encryption key does not traverse the cloud and is rotated as participants join and leave the meeting. For more details on Zero Trust Security based end-to-end encryption see the Zero Trust Security for Webex white paper.

With end-to-end encryption, all meeting content (voice, video, chat, etc.) is encrypted using the locally derived meeting encryption key. This data cannot be deciphered by the Service.

Note that when end-to-end encryption is enabled, Webex services and endpoints that need access to meeting keys to decrypt content (e.g., devices using SRTP where encryption is performed hop by hop) are not supported. This restricts meeting participants to those using the Webex App or cloud registered Webex devices only, and excludes services such as network-based recording, speech recognition etc. The following features are also not supported:

- Join Before Host
- Video-device enabled meetings
- Linux clients
- Network-Based Recording (NBR)
- Webex Assistant
- Saving session data transcripts, Meeting notes
- PSTN Call-in/Call-back

10. Sub-processors

We may share data with service providers, contractors or authorized third parties to assist in providing and improving the Service. We do not rent or sell your information. 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. Below is a list of sub-processors for Webex Meetings. Data shared with these sub-processors follows Webex data residency, except for those sub-processors who may be implicated by one of the exceptions listed in that section.

All Cisco sub-processors undergo a rigorous security and privacy assessment to confirm their compliance with our requirements. They are further bound by a data processing agreement which incorporates the EU Standard Contractual Clauses and places strict limits on their use and processing of any data provided by us or our Webex customers and users.

Sub-processor	Personal Data	Service Type	Location of Data Center
Akamai	• IP Address • Browser and Geographic Region	Akamai is used as content delivery network (CDN) services provider for static content. Akamai does not store content but may store IP addresses in logs for a maximum of 3 years.	Location generally maps to Customer's Webex data center assignment. To the extent Akamai receives IP addresses of Webex Meetings Customers, those IP addresses may be transmitted to the United States with strict access control means and appropriate safeguards under the EU Standard

			Contractual Clauses (SCCs).
Amazon Web Services (AWS)	• Limited Host & Usage Information • Meeting Recording Files (if applicable)	AWS cloud infrastructure is used to host the Webex signaling service that processes meeting participant UUIDs, meetings start and end times. Data will be deleted within 15 days of the meeting. (Location maps to Customer's Webex data center assignment.) AWS cloud infrastructure is used to host Webex media nodes that may process real-time meeting data such as VoIP, video and high frame rate sharing data. This information is not retained in AWS once your meeting has ended. AWS cloud infrastructure is also used to store Meetings recording files, if meeting record is enabled by the Customer. (Location maps to Customer's Webex data center assignment).	United States Germany Netherlands United Kingdom Brazil Australia Japan Singapore
WalkMe[4]	• Unique User ID (UUID) and user region	Provides user with a step-by-step tour and guidance on how to use Webex Meetings on the online site.	Globally
Vbrick	• Name • UUID • Email Address	Vbrick provides users with extended capacity for Webex Meetings including over 3,000 participants. Vbrick requires the data for authentication and the data is encrypted in transit. Vbrick does not store Webex Customer personal data.	United States EU: Germany, Ireland Australia

If a Customer acquires the Service through a Cisco partner, we may share any or all of the information described in this Privacy Data Sheet with the partner. Customers have the option of disabling this information-sharing with Cisco partners. If you use a third-party account to sign-in to your Webex account, Cisco may share only the necessary information with such third party for authentication purposes.

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 Requirements

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, including the EU General Data

[4] Customers may turn this feature off at any time. Feature is currently enabled for non-enterprise Webex sites.

Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and Personal Health Information Protection Act (PHIPA), Health Insurance Portability and Accountability Act (HIPAA), and Family Educational Rights and Privacy Act (FERPA).

In addition to the Cross-Border Data Transfer Mechanisms/Certifications listed in Section 5, 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. The 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.
- ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27701:2019 Certification
- 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
- Italian AgID (Agency for Digital Italy) Certification
- Australian IRAP (Information Security Registered Assessors Program) Certification

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:

<table>
<tr><td colspan="3">Chief Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td></tr>
<tr><td>Americas Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td><td>APJC Privacy Officer
Cisco Systems, Inc.
Bldg 80, Lvl 25, Mapletree Biz City,
80 Pasir Panjang Road,
Singapore, 117372
SINGAPORE</td><td>EMEAR Privacy Officer
Cisco Systems, Inc.
Haarlerbergweg 13-19, 1101 CH
Amsterdam-Zuidoost NETHERLANDS</td></tr>
</table>

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.

To receive email notifications of updates to the Privacy Data Sheet, click the "Subscribe" link in the upper right corner of the Trust Portal.

Addendum One: People Insights for Webex

This Addendum describes the processing of personal data (or personal identifiable information) by People Insights for Webex Meetings and the Webex App.

People Insights for Webex Meetings and the Webex App is a cloud-based company directory solution made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from People Insights for Webex Meetings and the Webex App 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 Webex Meetings and the Webex App to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

2. Overview

The People Insights feature ("People Insights" or the "Feature") provides Webex Meetings and Webex App users with comprehensive, publicly available business and professional information for meeting participants giving users context and increased insight about the people with whom they collaborate. People Insights only displays publicly available information, similar to what can be found in search engine results for a person's name and profession. People Insights will also display internal company directory information to users in the same company. This internal directory information is not visible to users outside the company. The People Insights database does not look behind logins or paywalls, which means your profile will notbe populated with content from sites like Facebook.

People Insights was designed with data protection and privacy in mind, and is aligned to global privacy requirements, including GDPR. This Feature provides users with a convenient single view into their already existing public presence and digital footprint. As outlined below, People Insights includes functionality to honor data subject rights. Users fully own their People Insights profile and can change or hide the profile to keep information private.

People Insights is enabled by default for U.S. provisioned Customers. Customers provisioned in the EU must opt-in to this feature. Users at an enabled organization can opt out of People Insights by suppressing their profile in the Webex App. This is accomplished by signing into people.webex.com and clicking on "Hide Profile."

If you join a Webex Meeting, or a space in Webex App, hosted by a Cisco Customer that has People Insights enabled on their Site Admin Page or Webex Control Hub, all participants' People Insight profiles will be visible unless they have chosen to hide their profiles as described above.

3. Personal Data Processing

People Insights compiles business and professional profiles for Webex App users and Webex Meetings participants using publicly available and legitimately sourced information, published authored works, news articles, search engine results, via APIs and through content supplied by the profile owner.

The table below lists the personal data processed by People Insights to provide the Feature and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
Publicly Available Business and Professional Biographical Data	• Profile Photos • News • Tweets • Authored Works • Bios • Employment History	As a processor: • Provide you with the Feature • To source the People Insights profile and to enable search within the Feature No uses as a controller

	• Education History • Web Links for a specific person	
Account & Usage Information	User Level Account Details (including email, name, and web interactions and platform usage)	As a processor: • Provide you with the Feature • Product analytics (e.g., frequency of profile edits, number of successful profile loads in a meeting, etc.) As a controller: • Make improvements to the Feature and other Cisco products and services
Directory Data	• If the directory option is enabled by the site administrator, professional information including the following may be collected from the internal company directory (as selected by the administrator): • Title • Phone Number • Location • Organization • Department • Photo • Role • Reporting Structure • Pronouns (optional, only applicable if available in your organization)	As a processor: • Provide you with the Feature • To augment the user's People Insights profile by providing company specific context to Webex App users and Webex Meetings participants who belong to the same organization. This data will only be visible to participants within the user's organization. No uses as a controller
User-Generated Information	• Information that the user adds in their People Insights profile.	As a processor: • Provide you with the Feature • Augment the user's own People Insights profile (visible to People Insights users) No uses as a controller

3. Data Center Locations

People Insights data is stored on third party servers provided by Amazon Web Services ("AWS"). AWS servers are located in the United States.

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- 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 People Insights, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
Publicly Available Business and Professional Biographical Data	• Cisco	• To provide the Feature
	• Users of Customer Webex site with enabled People Insights	
Account & Usage Information	• Cisco	• Registration Support • Correlate users with correct profiles • Analytics to improve service
	• Customer	• Feature enablement/disablement
Directory Data	• Customer (Admin) • People Insight users within the Customer's organization	• Directory data is provided and maintained by Customer administrator to allow integration into People Insights profile
	• Cisco	• Directory data is imported and integrated with Customer profile data to support profile development
User-Generated Information	• User	• Users may access their own User-Generated Information to edit or delete content

6. Data Portability

Individuals can receive a copy of their own People Insights profile, including their self-generated information, through the Cisco Privacy Request form.

7. Data Deletion and Retention

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

Type of Personal Data	Retention Period	Reason for Retention
Publicly Available Business & Professional Data	Obtained from public websites: three (3) years Obtained through third-party APIs: In accordance with contractual requirements	Publicly Available Business & Professional Data is derived from public sources. It is retained for three (3) years. Upon request, publication and links to source data can be suppressed and restricted from view and publication. As publicly available data originates from outside of the Webex App and Webex Meetings, any permanent changes or deletions must be addressed and requested with the primary source. At the request of users, the data can be archived to not appear. This allows for the data to remain permanently hidden rather than re-appearing with a new search after being previously purged.
Account & Usage Information	Active Subscriptions: At Customer's or user's discretion Deactivated Accounts: Deleted within thirty (30) days	Users can request to remove their Account Information by opening a TAC service request. Cisco will respond to such requests within thirty (30) days.
Directory Data	Active Subscriptions: At Customer's or user's discretion Deactivated Accounts: Deleted within thirty (30) days	Administrators can disable the Active Directory feature while still enabling People Insights. Directory data will be hard deleted in this case of deactivation. Non-directory data will remain, with the exception of name and email for users who had only directory data in their profile before the deactivation.

User-Generated Information	Active Subscriptions: At Customer's or user's discretion Deactivated Accounts: Deleted within thirty (30) days	Users can delete User-Generated Information from their profile at any time.

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.

Personal Data Category	Security Controls and Measures
Publicly Available Business & Professional Data	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS
Host & Usage Information	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS
Directory Data	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS
User-Generated Information	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for the Feature is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	• Publicly Available Business & Professional Data • Host & Usage Information • Directory Data • User-Generated Information	Cloud Storage	United States
Diffbot	• Name, Email Address	Supplementing Publicly Available Business & Professional Data	United States

Addendum Two: Facial Recognition for Webex Meetings (Optional)

This Addendum describes the processing of personal data (or personal identifiable information) by the Facial Recognition feature for Webex Meetings. The Facial Recognition feature is only available when using Webex Meetings on certain Cisco Endpoint devices.

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

Cisco will process personal data from Facial Recognition feature for Webex Meetings 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 Webex Meetings to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

Cisco introduced the facial recognition feature ("Facial Recognition" or the "Feature") to provide Webex Meetings users with the ability to identify and recognize registered Webex Meetings participants (i.e., associate participant names with their positions in a Webex Meetings video), giving users increased connection to meeting participants. The Feature recognizes a face by converting it to an abstracted facial vector. A facial vector is a list of numbers that characterizes salient facial features of a user that is then used to identify who is in the meeting. This level of abstraction allows the system to recognize the same face even when things like lighting and position change.

Facial Recognition is disabled by default, and requires affirmative action by both the Customer and the user to enable. First, the administrator for the Customer may enable Facial Recognition using Webex Control Hub. However, the feature will not be available on the user's account until the user opt-ins at https://settings.webex.com. Because the Feature is based on facial vectors derived from profile images, the user must have a picture taken at the time of enablement.

2. Personal Data Processing

If the user opts in to the Feature, the Service uses the camera of the user's device to take a profile picture. This picture is sent to the Webex cloud where the Feature algorithm generates a facial vector from the picture so that it can be used for matching as further described below. Both the picture and the facial vector are encrypted and stored securely. The picture may be used to generate a new facial vector in the event Cisco updates or modifies the Feature algorithm by which facial vectors are generated. In the event a Customer or user reaches out to Cisco for support with the Feature, Cisco may also use the picture during the troubleshooting process. During each Webex Meeting, a second facial vector is generated, which is then matched in the Webex cloud against the stored facial vector. This second facial vector is not retained.

The table below lists the personal data processed by Facial Recognition to provide the Feature and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
User Information	• Name (First, Last) • Email • User ID	As a processor: • Enroll you in the Feature and enable opt-in • To display name of recognized user No uses as a controller

Biometrics	• User facial image • Facial vector mapping	As a processor: • To create facial vector mapping and provide the Feature • To generate a new facial vector in case of a modification or update to the Feature algorithm No uses as a controller
Host & Usage Information	• Information regarding accuracy of product, including: ○ Successful and unsuccessful facial vector matching ○ User feedback	As a processor: • To provide support and product analytics As a controller: • Make improvements to the Feature and other Cisco products and services
Location	• Meeting Room Proximity data	As a processor: • Proximity data is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations No uses as a controller
Calendar	• Meeting Room Calendar Information	As a processor: • Calendar information is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations No uses as a controller

3. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

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

4. Access Control

The table below lists the personal data used by Facial Recognition to provide the Feature, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
User Information	Cisco	• To display name of recognized user • Enroll you in the Feature and enable opt-in
	Customer	• View user facial recognition registration status
	Users through https://settings.webex.com/	• View and modify facial recognition registration details
Biometrics	Cisco	• To provide the Feature • Algorithm improvement • To troubleshoot issues in the event Customer or users request support
Host & Usage Information	Cisco	• To provide support and product analytics
Location	Cisco	• Proximity data is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations

Calendar	Cisco	• Calendar information is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations

5. Data Portability

While Webex Meetings allows Customers and users to export data as described in Section 7 of the Webex Meetings Privacy Data Sheet, it does not support the automatic export of Facial Recognition data.

6. Data Deletion and Retention

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

Type of Personal Data	Retention Period	Reason for Retention
User Information	User ID is maintained for all active Webex Meetings users. Once a user is deleted from a Customer's account, the User ID is also deleted from the Feature. All other User Information is not stored or retained by the Feature as this information is already stored by Webex Meetings.	User ID is used to track your enrollment in the Feature. Names are displayed upon a match in the Feature.
Biometrics	Images: Users control their image retention. The image is retained as long as the Feature is enabled and the user leaves the image associated with their profile. The image can be deleted at any time by the user. Images for all users are deleted upon Customer's discontinuation of the Service.	The image is used to provide the Feature, update the facial vector in case of an update to the Facial Recognition algorithm, and to troubleshoot issues when requested by a Customer or user.
	Facial vectors are retained as long as the facial images, but are stored separately. Facial vectors are deleted upon discontinuation of the Service.	The facial vectors are used to provide the Feature.
Host & Usage Information	2 weeks	To provide support and product analytics.
Location	2 days	Proximity data is used to improve Facial Recognition to assure images are assigned to the correct users in the correct locations.
Calendar	Facial Recognition does not store or retain this information separately than already maintained by Webex Meetings.	

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 table below summarizes encryption architecture of data stored specifically for the Feature.

Personal Data Category	Security Controls and Measures
User Information	Encrypted in transit, AES 256 for storage
Images	Encrypted in transit, AES 256 for storage
Biometrics	Encrypted in transit, AES 256 for storage

Host & Usage Information	Encrypted in transit, AES 256 for storage
Location	Encrypted in transit, AES 256 for storage

Addendum Three: Closed Captioning for Webex Meetings (Optional)

This Addendum describes the processing of personal data (or personal identifiable information) by the Closed Captioning feature for Webex Meetings ("Closed Captioning" or the "Feature").

Cisco will process personal data from Closed Captioning 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 Meetings to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

To make your Webex Meetings and Webex Webinars more accessible, Webex provides automated closed captioning which you can turn on without needing to turn on Webex Assistant for Webex Meetings. As people speak, closed captioning will appear above the Webex Meetings or Webex Webinar controls. A closed captions panel is also available, which shows users the closed captions from the moment they joined the Webex Meeting, so they can easily catch up if they miss anything that's being said.

Closed Captioning is a cloud-based feature that is enabled "ON" by default; user administrators can select enablement for specific users or, if a user administrator intends to disable for all users, he or she can request that Cisco disable at an organization level. Users can also disable Closed Captioning, so that captions do not appear for themselves; however, if other users in their Webex Meeting(s) have Closed Captioning ON, data belonging to users who have disabled the functionality will still be processed in accordance with the privacy disclosures below.

If a host turns on Webex Assistant for Webex Meetings in addition to Closed Captioning, then they will have additional capabilities to make voice commands and highlight captions to capture audio snippet notes, as detailed in Addendum Four. Additionally, hosts can record the Webex Meeting and receive a post-meeting transcript, which they can choose to share with other Webex Meetings users.

User administrators can also enable or disable the Captions & Highlights panel for their site.

2. Personal Data Processing

The table below lists the personal data processed by Closed Captioning to provide the Feature and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
Audio Information	• Audio captured during meeting	As a processor: • Provide Closed Captioning As a controller: • When you utilize the real-time translation and transcription feature in multiple languages, data may be used for product improvement. You may opt out of this use by submitting a request here.
Transcript Information	• Webex Meetings Transcript • Text of real-time speech for translations	As a processor: • Provide Closed Captioning As a controller:

		• When you utilize the real-time translation and transcription feature in multiple languages, data may be used for product improvement. You may opt out of this use by submitting a request here.
Host and Usage Information	• Usage of Closed Captioning, including number of Webex Meetings with Closed Captioning enabled, and troubleshooting events	As a processor: • Provide Closed Captioning • Provide Customer with usage information • Diagnose technical issues • Improve the technical performance of the Service As a controller: • Understand how Closed Captioning is used

3. Data Center Locations

Closed Captioning data center locations track the data center locations for Webex Assistant for Webex Meetings, which are outlined in Addendum Four below. Please refer to Addendum Four below.

4. Cross-Border Data Transfer Mechanisms

Closed Captioning cross-border data transfer mechanisms are the same as those listed for Webex Assistant for Webex Meetings, which are outlined in Addendum Four below. Please refer to Addendum Four below.

5. Access Control

The table below lists the personal data used by Closed Captioning, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
User Information	Cisco	Enroll users in Closed Captioning.
	Customer	Enable/disable Closed Captioning for specific Webex Meetings users or an entire site.
Audio Information	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer and will only access in accordance with Cisco's data access and security controls process.
	Customer	Customer will continue to have access to Meetings Recordings (if the meeting was recorded by host) in accordance with Customer's personal data policy and as described in the Webex Meetings Privacy Data Sheet.
	User	No highlights or meeting audio information is retained after the meeting when Close Captioning only is used during the live meeting
Transcript Information	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer and will only access in accordance with Cisco's data access and security controls.
	User	By default, no transcript is retained when Closed Captioning only is used during the live Webex Meeting unless recording was enabled. If recording was enabled, a transcript will be available in the recording page and review tab in the post meeting experience, a meeting host will be able to view, access and/or share transcript Information. A host may share and give certain edit permissions to other Webex Meetings users.
Host and Usage Information	Cisco	Support and improve the Service in accordance with Cisco's data access and security controls.

	Customer	View and analyze usage information.

6. Data Portability

- Webex Meetings hosts and users with edit privileges to a given meeting can download the meeting transcript in txt or vtt formats.
- Webex Meetings hosts and users with edit privileges to a given meeting can email highlights to a selected email account.
- Webex Meetings hosts and users with edit privileges to a given meeting can share a meeting in an existing or a newly created Webex space.

7. Data Deletion and Retention

Subject only to their employer's corporate retention policies, users with an active subscription have control over their Audio and Transcript Information and can delete such information from their account through the My Webex Page as described below. If you have any questions regarding deletion or deletion requests, please contact Cisco through the Cisco Privacy Request Form.

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

Type of Personal Data	Retention Period	Reason for Retention
User Information	User Information is not separately stored or retained as part of Closed Captioning, as this information is already stored by Webex Meetings.	
Audio Information	Active Subscriptions: Audio Information deleted at Customer's or user's discretion. Terminated Service: Deleted within 60 days	Audio Information is retained to provide you with the Service and will be deleted once it is no longer necessary to provide the Service. Audio Information retained after the Service is terminated is done to make it available to Customers for download. Audio Information related to real-time translation and transcription in multiple languages is retained for 2 years for product improvement. You may opt out of this use by submitting a request here.
Transcript Information	Active Subscriptions: Highlights may be deleted at Customer's or user's discretion. Terminated Service: Deleted within 60 days	Transcript Information is retained to provide you with the Service and will be deleted once it is no longer necessary to provide the Service. Transcript Information retained after the Service is terminated is done to make it available to Customers for download. Transcription Information related to real-time translation and transcription in multiple languages is retained for 2 years for product improvement. You may opt out of this use by submitting a request here.
Host and Usage	Deleted after 3 years.	Usage information used to conduct analytics and measure statistical performance is retained but pseudonymized.

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 table below summarizes the encryption architecture of data stored specifically for Closed Captioning.

Personal Data Category	Security Controls and Measures
User Information	Closed Captioning does not store or retain this information separately than the information already maintained by Webex Meetings.
Audio Information	Encrypted in transit. Closed Captioning is not stored at rest.
Transcript Information	Encrypted in transit. Closed Captioning is not stored at rest.
Host and Usage	Encrypted in transit and at rest.

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for Closed Captioning is below:

Sub-processor	Personal Data	Service Type	Location of Dataf Center
Amazon Web Services	Audio Information	Cloud Infrastructure (transient storage only)	US, Singapore, France, Japan, Ireland, Sweden
Google	Audio and transcript of Voice Command only (e.g., "OK, Webex, create a note"). Please note that the core transcription technology that processes and stores all other Audio and Transcript Information is owned, managed and executed by Cisco.	• Speech-to-Text service (voice commands only) • Text-to-Speech service (voice command responses only)	US, Germany, Singapore, Netherlands, Belgium, Japan
Google*	Transcript Information	Provide translation and/or foreign language transcription using text of real-time speech. Google may process but not store transcript Information to provide speech-to-text services Transcript data is processed by Google at global endpoints, except when a Customer is provisioned in the European Union (EU). For EU Customers, transcript data processed by Google is processed within region as part of Webex Data Residency.	Globally For EU Customers, within the EU
	Audio Information (except if spoken language chosen is English)	When you add-on and use the real-time translation and transcription feature in multiple languages, Google may process but not store Audio Information to provide speech-to-text services. Audio data is processed by Google at global endpoints, except when a Customer is provisioned in the EU. For EU Customers, audio data processed by Google is processed within region as part of Webex Data Residency.	Globally For EU Customers, within the EU

* These sub-processors will only apply to You if You have purchased and are using real-time translation and transcription in multiple languages.

Addendum Four: Webex Assistant for Meetings (Optional)

This Addendum describes the processing of personal data (or personal identifiable information) by Webex Assistant for Webex Meetings ("Webex Assistant") feature for Webex Meetings.

Webex Assistant is a cloud-based feature made available by Cisco to companies or persons who acquire it for use by their authorized users. Webex Assistant provides additional functionality to Closed Captioning, for example, allowing users to use voice commands, highlight closed captions during the meeting, and edit or share highlights after a meeting.

Cisco will process personal data from Webex Assistant 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 Webex Meetings in order to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

Webex Assistant is an intelligent, interactive virtual meeting assistant that makes meetings searchable, actionable, and more productive. When Webex Assistant is turned on, the meeting host and participants can capture meeting highlights with one click or through a voice command. Even when Webex Assistant joins a Webex Meeting, it will only be activated by the wake word, "OK Webex." Once the wake word is detected, the voice command is streamed to the cloud for speech-to-text transcription and processing. Any participant can use one of many voice commands and create a meeting highlight. Meeting highlights can include meeting key points, notes, summaries, agendas, action items or decisions.

Webex user administrators can enable or disable Webex Assistant for a Webex site and can restrict use of Webex Assistant to certain users or groups of users at any time.

Cisco has put several controls in place to ensure user transparency. When Webex Assistant is enabled, the Webex Assistant icon appears in the lower left of the host and participant's screen. On Webex endpoint devices, there will be a visual cue similar to the existing one you see when a Webex Meeting is recorded. Additionally, when the host turns on Webex Assistant in a Webex Meeting, there will be an audio announcement made to all participants on the call, even if they join late (unless the Webex user administrator has disabled the announcement). As further described below, the host can choose to share the transcript and meeting highlights with other Webex Meetings users.

2. Personal Data Processing

The table below lists the personal data processed by Webex Assistant to provide its services and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
User Information	• Name (First, Last) • Email • Username • Unique User Identifier (UUID)	As a processor: • Enable Webex Assistant for specific Webex Meetings users or for an entire site • Provide Webex Assistant No uses as a controller

Audio Information	• Webex Meetings Recordings • Audio Commands to Webex Assistant • Audio captured during meeting	As a processor: • Provide Webex Assistant As a controller: • When you utilize the real-time translation and transcription feature in multiple languages, data may be used for product improvement. You may opt out of this use by submitting a request here.
Transcript Information	• Webex Meetings Transcript • Text of meeting Highlight • Text of real-time speech for translations	As a processor: • Provide Webex Assistant As a controller: • When you utilize the real-time translation and transcription feature in multiple languages, data may be used for product improvement. You may opt out of this use by submitting a request here.
Host and Usage Information	• Usage of the Webex Assistant features, including number of meetings with Webex Assistant enabled, number/type of Highlight views/edits/downloads, troubleshooting events	As a processor: • Provide Webex Assistant • Provide Customer with usage information • Improve the technical performance of the Service • Diagnose technical issues As a controller: • Understand how Webex Assistant is used

3. Data Center Locations

Cisco leverages its own data centers as well as third-party hosting providers and business partners to deliver the Service, including Webex Assistant, globally.

Webex Assistant Audio and Transcript Information will be stored in the same location in which the Customer is provisioned for Webex Meetings recordings. Although Webex Assistant may process data in AWS as listed in Section 9 below, no data will be stored there.

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- 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 Webex Assistant, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
User Information	Cisco	Enroll users with Webex Assistant.
	Customer	Enable Webex Assistant for specific Webex Meetings users or for an entire site.
Audio Information	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer and will only access in accordance with Cisco's data access and security controls process.

	Customer	Customer will continue to have access to Meetings Recordings in accordance with Customer's personal data policy and as described in the Webex Meetings Privacy Data Sheet.
	User	A meeting host will be able to view, access and/or delete highlights. A host may share and give certain edit permissions to other Webex Meetings users.
Transcript Information	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer and will only access in accordance with Cisco's data access and security controls.
	User	A meeting host will be able to view, access and/or share transcript information. A host may share and give certain edit permissions to other Webex Meetings users.
Host and Usage Information	Cisco	Support and improve the Service in accordance with Cisco's data access and security controls.
	Customer	View and analyze usage information.

6. Data Portability

Users have the option to email any transcript or highlight to a selected email account.

7. Data Deletion and Retention

Subject only to their employer's corporate retention policies, users with an active subscription have control over their Audio and Transcript Information and can delete such information from their account through the My Webex Page as described below. If you have any questions regarding deletion or deletion requests, please contact Cisco through the Cisco Privacy Request Form.

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

Type of Personal Data	Retention Period	Reason for Retention
User Information	User Information is not separately stored or retained by Webex Assistant as this information is already stored by Webex Meetings.	
Audio Information	Active Subscriptions: Audio Information deleted at Customer's or user's discretion. Terminated Service: Deleted within 60 days	Audio Information is retained in order to provide you with the Service and will be deleted once it is no longer necessary to provide the Service. Audio Information retained after the Service is terminated is done in order to make it available to Customers for download. Audio Information related to real-time translation and transcription in multiple languages is retained for 2 years for product improvement. You may opt out of this use by submitting a request here.
Transcript Information	Active Subscriptions: Highlights may be deleted at Customer's or user's discretion. Terminated Service: Deleted within 60 days	Transcript Information is retained in order to provide you with the Service and will be deleted once it is no longer necessary to provide the Service. Transcript Information retained after the Service is terminated is done in order to make it available to Customers for download.

		Transcription Information related to real-time translation and transcription in multiple languages is retained for 2 years for product improvement. You may opt out of this use by submitting a request here.
Host and Usage	Deleted after 3 years.	Usage information is used to conduct analytics and measure statistical performance.

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 table below summarizes encryption architecture of data stored specifically for Webex Assistant.

Personal Data Category	Security Controls and Measures
User Information	Webex Assistant does not store or retain this information separately than the information already maintained by Webex Meetings.
Audio Information	Encrypted in transit and at rest.
Transcript Information	Encrypted in transit and at rest.
Host and Usage	Encrypted in transit and at rest.

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for Webex Assistant is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	Audio Information	Cloud Infrastructure (transient storage only)	US, Singapore, France, Japan, Ireland, Sweden
Google	Audio and transcript of Voice Command only (e.g., "OK, Webex, create a note"). Please note that the core transcription technology that processes and stores all other Audio and Transcript Information is owned, managed and executed by Cisco.	• Speech to Text service (voice commands only) • Text to Speech service (voice command responses only)	US, Germany, Singapore, Netherlands, Belgium, Japan
Google*	Transcript Information	Provide translation using text of real-time speech. Transcript data is processed by Google at global endpoints, except when a Customer is provisioned in the European Union (EU). For EU Customers, transcript data processed by Google is processed within region as part of Webex Data Residency.	Globally For EU Customers, within the EU

	Audio Information (except if spoken language chosen is English)	When you add-on and use the real-time translation and transcription feature in multiple languages, Google may process but not store Audio Information to provide speech-to-text services Audio data is processed by Google at global endpoints, except when a Customer is provisioned in the EU. For EU Customers, audio data processed by Google is processed within region as part of Webex Data Residency.	Globally For EU Customers, within the EU

* These sub-processors will only apply to you if you have purchased and are using real-time translation and transcription in multiple languages.

Addendum Five: Webex Assistant for Devices

This Addendum describes the processing of personal data (or personal identifiable information) by Webex Assistant for Devices.

Webex Assistant for Devices is a cloud-based feature made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from Webex Assistant for Devices 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 Meetings in order to provide its functionality.

1. Overview

Webex Assistant for Devices gives you a new way to control your devices by using voice commands. Through voice commands, a user is able to join meetings, control meeting settings and more. Webex Assistant for Devices is disabled by default and can be enabled by the Organization's administrator in Webex Control Hub.

Webex Assistant for Devices is activated by the wake word, "OK Webex." Once the wake word is detected, speech is streamed to the cloud for speech-to-text transcription. As wake word processing is local on the device, no audio data is stored, processed or streamed to the cloud until the wake word is detected. After the wake word and command are processed, the resulting text from the speech engine is returned to the Webex Assistant client on the endpoint device and displayed to the user. Although Webex Assistant for Devices securely manages functional interactions with Google Speech Services to enable the service, data is not stored or further processed by Google for any other purpose than to provide you with the service.

2. Personal Data Processing

The table below lists the personal data processed by Webex Assistant for Devices to provide its services and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing

User Information	• Synched Corporate Directory information (e.g., name, email, title)
	• For users who pair with Cisco endpoint device:
	  ○ Unique User Identifier
	  ○ First Name
	  ○ Display name
		As a processor:
		• Provide Webex Assistant
		• Improve Webex Assistant's accuracy to user's command
		
		No uses as a controller

Audio	• User audio commands	As a processor: • Provide Webex Assistant No uses as a controller
Transcripts	• Text of command	As a processor: • Provide Webex Assistant As a controller: • Train and/or improve Cisco language services
Usage	• Webex Assistant usage information (e.g., number of queries from endpoint devices, dates) • Endpoint devices used	As a processor: • Diagnose technical issues • Improve the technical performance of Webex Assistant As a controller:

		• Understand how Webex Assistant is used

3. Data Center Locations

Cisco leverages its own data centers as well as third-party hosting providers and business partners to deliver Webex Assistant for Devices 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
Germany
United States
Singapore

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- 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 Webex Assistant for Devices, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
User Information	Cisco	Enable, support and improve Webex Assistant in accordance with Cisco's data access and security controls process.
Audio	Cisco	Provide Webex Assistant.
Transcripts	Cisco	Support, train and improve Webex Assistant. Understand how the product is being used.
Usage Information	Cisco	Support and improve the Service in accordance with Cisco's data access and security controls process. Understand how the product is being used.
	Customer	View and analyze some usage information on Control Hub.

6. Data Portability

While Webex Meetings allows Customers and users to export data as described in Section 7 of the Webex Meetings Privacy Data Sheet, it does not support the export of Webex Assistant for Devices data.

7. Data Deletion and Retention

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

Type of Personal Data	Retention Period	Reason for Retention

User Information	Stored while Customer is enrolled in Webex Assistant for Devices. After Customer disables Webex Assistant, User Information is deleted within a week. If you have paired with a device, the relevant data is retained for 1 year.	User Information is retained in order to provide you with the Service and will be deleted once it is no longer necessary to provide the Service.
Audio	Not retained	N/A
Transcript	1 year	Transcripts are retained to evaluate and improve Webex Assistant and understand how the product is being used. Text transcripts (e.g., "OK Webex, Start a Meeting") will be de-identified and may be stored indefinitely.
Usage	Deleted within 2 years	Usage is retained to evaluate the service and understand how Webex Assistant is being used.

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 table below summarizes encryption architecture of data stored specifically for the Webex Assistant for Devices.

Personal Data Category	Security Controls and Measures
User Information	Encrypted in transit, encrypted at rest
Audio	Encrypted in transit, encryption at rest is not applicable[5]
Transcript	Encrypted in transit, encrypted at rest
Usage	Encrypted in transit, encrypted at rest

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for Assistant for Devices is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	Transcript	AWS cloud infrastructure is used to host Webex Assistant for Devices applications in Germany, Singapore, and the US. Transcripts routed to and processed in the EU (Frankfurt data center) are not stored. All other transcripts generated are stored in their closest region of storage (Singapore or the US).	United States Singapore Germany
Google Cloud	Audio	Speech to text service	Worldwide
Google Cloud	• Transcript	Cloud storage region	United States

[5] The Webex platform and Google Cloud do not store audio; therefore, encryption at rest is not available for audio.

	• Usage		
Splunk	• Transcript • Usage	Data analysis platform	United States

Addendum Six: Slido in Webex (Optional)

This Addendum to the Webex Meetings Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by the Slido feature in Webex Meetings ("Slido" "Slido in Webex," or the "Service").

1. Overview of Slido in Webex Meetings Capabilities

Slido in Webex is a cloud-based polling and Q&A solution aimed at B2B customers. Users stay engaged during meetings by voting in live polls and asking questions. Slido is an integrated part of Webex Meetings or available to hosts and meeting participants as a web application. For a detailed overview of the Service, please visit the Slido in Webex website.

2. Personal Data Processing

Because of the nature of the Service, we do not expect any sensitive data to be sent through Slido.

The table below lists the personal data processed by Slido in Webex to provide the Service and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
Host Information	• Name, email address, organization ID	As a processor: • Provide you with the Service • Respond to Customer support requests As a controller: • Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service
Participant Information	• Name, email address, organization ID	As a processor: • Provide you with the Service No uses as a controller
User-Generated Information	• Questions, answers, ideas, chats - any content shared or created by participants	As a processor: • Provide you with the Service No uses as a controller
User Technical Information	• Device data (e.g. hardware model, operating system version, unique device identifiers), • Log data (e.g., your search queries, details about your connection such as IP address, date, time, edge-location, ssl-protocol, ssl-cipher or time-taken to serve you requested site, device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL) • Location information (IP address) • Unique users IDs • Browser local storage and application data caches	As a processor: • Provide you with the Service As a controller: • Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service

Cookies	• Essential cookies collected through embedded browser utilized in the Webex-Slido interface	As a processor: • Provide you with the Service As a controller: • Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service
Support Information	We collect contact data of people reaching out through Slido.com for support: • Usually name, email, company	As a processor: • Provide you with the Service • Respond to Customer support requests As a controller: • Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service

Technical Support Assistance

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

3. Data Center Locations

Cisco uses third-party infrastructure providers to deliver the service globally. Please see Section 9 for a list of sub-processors, including infrastructure providers.

Data Center Locations - default
Ireland
Germany

Data Center Locations - optional
Virginia, USA
Oregon, USA

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- 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 Slido to carry out the service, who can access that data, and why. Content you choose to share during an event may be accessed by users in the event, wherever they are located. Even after you remove information from the Service, copies of that content may remain viewable elsewhere to the extent it has been shared with others.

Personal Data Category	Who has Access	Purpose of the Access
Host Information	Host	View host profile data through slido.com
	Customer	Manage, delete user's slido profiles through slido.com
	Cisco	Provide the Service
Participant Information	Host	View joined participants through slido.com
	Cisco	Support the Service in accordance with Cisco's data access and security controls
User-Generated Information	Customer	Delete participant content data by submitting privacy request form
	Host	View submitted User-Generated Information through slido.com
	Cisco	Support the Service in accordance with Cisco's data access and security controls. Cisco will not access this data unless authorization is granted by the Customer, and will only access it in accordance with Cisco's data access and security controls.
User Technical Information	Cisco	Provide, tailor and improve the Service
Cookies	Cisco	Provide, tailor and improve the Service
Support Information	Cisco	Support Information is kept as part of record of service delivery

6. Data Portability

Slido allows Customers and hosts to export event content data through slido.com.

7. Data Deletion and Retention

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

Type of Personal Data	Retention Period	Reason for Retention

Host Information	Host Information is retained until account termination.	• Provide the Service
Participant Information	Participant Information associated with a specific meeting is retained until account termination. Participant Information associated with a specific meeting can be deleted by deleting all Slido data associated with that meeting. As request must be submitted through a privacy request.	• Provide the Service
User-Generated Information	User-Generated Information associated with a specific meeting is retained until account termination. User-Generated Information associated with a specific meeting can be deleted by deleting all Slido data associated with that meeting. As request must be submitted through a privacy request.	• Provide the Service
Technical Information	Deleted 1 year after collection	• Technical Information is kept as part of Cisco's record of service delivery, conduct analytics and measure statistical performance.
Cookies	Maximum of one year	• To provide, tailor and improve the Service
Support Information	Not deleted	• Support Information is kept as part of record of service delivery.

8. Personal Data Security

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

Personal Data Category	Security Controls and Measures
Host Information	Encrypted in transit and at rest
Participant Information	Encrypted in transit and at rest
User-Generated Information	Encrypted in transit and at rest
User Technical Information	Encrypted in transit and at rest
Cookies	Encrypted in transit and at rest
Support Form Information	Encrypted in transit

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for the service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	• Host Information • Participant Information • User-Generated Information • User Technical Information • Cookies • Support Information	Infrastructure as a Service	Dublin, Ireland Frankfurt, Germany

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 Requirements

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.

Slido currently holds the following privacy certifications:

- ISO/IEC 27001:2013

As part of its integration, Slido intends to pursue other privacy certifications, including those associated with Webex.

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 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:

<table>
<tr><td colspan="3">Chief Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td></tr>
<tr><td>Americas Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td><td>APJC Privacy Officer
Cisco Systems (USA) Pte Ltd
Bldg 80, Lvl 25, Mapletree Biz City,
80 Pasir Panjang Road,
Singapore, 117372
SINGAPORE</td><td>EMEAR Privacy Officer
Cisco Systems, Inc.
Haarlerbergweg 13-19, 1101 CH
Amsterdam-Zuidoost NETHERLANDS</td></tr>
</table>

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.

Addendum Seven: Cisco-Developed Embedded Apps (Optional)

This Addendum to the Webex Meetings Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco-developed embedded apps in Webex Meetings. Embedded apps developed by third parties, as stated in the Webex Meetings Privacy Data Sheet, are governed by the respective third party's privacy policies.

Shared Timer

1. Overview

Shared Timer (the "Service") is a cloud-based application that allows meeting hosts and participants to set a timer, using preset intervals, during a particular meeting. The countdown timer is displayed with other meeting participants.

Personal data processing for Shared Timer is largely covered by the disclosed personal data processing associated with the Webex Meetings Service; for that, please refer to the Webex Meetings Privacy Data Sheet above.

A Customer user administrator controls whether user-level personal data can be shared with Shared Timer. In Webex Control Hub, the Customer user administrator can set enable or disable personally identifiable information ("PII") sharing through "PII Restrictions." "PII Restrictions" are disabled by default (i.e., without any action by the Customer user administrator) and the only pseudonymized user-level personal data will be processed by Shared Timer, as described below.

The following information is supplementary privacy data information associated specifically with Shared Timer.

2. Personal Data Processing

The table below lists the personal data processed by Shared Timer to provide the Service and describes why the data is processed.

If PII Restrictions are enabled, PII sharing mode is on, and the following applies:

Personal Data Category	Type of Personal Data	Purpose of Processing
User Information	• UUID • Display Name	As a processor: • UUID is used to identify which user within the meeting performed specific activities (e.g., who paused the timer); • Display Name is used to identify the user-specific activities (to display that a certain individual set or reset the timer) No uses as a controller
Host and Usage Information*	• IP Address • User Agent • Browser • Operating System • Device Type	As a processor: • Provide you with the Service • Diagnose technical issues • Respond to Customer support requests As a controller: • Make improvements to the Service and other Cisco products and services • Understand how the Service is used • Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the

		Service

To the extent personal data is shared with sub-processors, it is encrypted at transit. Sub-processors do not have access to the data in the raw.

If the PII Restrictions are disabled, PII sharing is off, and the following applies:

Personal Data Category	Type of Personal Data	Purpose of Processing
User Level	• Personal data that is collected (e.g., UUID and Display Name) is pseudonymized	As a processor: • UUID used to identify which user within the meeting performed specific activities (e.g., who paused the timer); • Name is processed to identify the user-specific activities (to display that a certain individual set or reset the timer) No uses as a controller
Host and Usage Information*	• IP Address • User Agent • Browser • Operating System • Device Type	As a processor: • Provide you with the Service • Diagnose technical issues • Respond to Customer support requests As a controller: • Make improvements to the Service and other Cisco products and services • Understand how the Service is used • Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service

2. Sub-processors

Shared Timer does not use the sub-processors listed in the Webex Meetings Privacy Data Sheet. Shared Timer uses only the following third-party sub-processor.

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	• UUID** • Display Name**	• Used to provide Shared Timer functionality	USA

* Collected through use of Webex Meetings processed in connection with Shared Timer.
** When PII sharing mode is ON. When PII sharing mode if OFF, data is pseudonymized.