



## Offer Disclosure

# Webex Meetings

This Offer Disclosure provides detailed information about data handling practices, security controls, and AI features specific to this Cisco Offer. It complements the [General Disclosures](#), which outline Cisco's overarching approach to handling Customer Systems Information and Customer Content, and the [Cisco Online Privacy Statement](#), which offers a more in-depth explanation of how Cisco manages Personal Data. Together, these documents provide transparency by addressing data handling at both a high level and an Offer specific level, helping you understand how Cisco protects and processes information across its Offers.

Capitalized words not otherwise defined in this Offer Disclosure have the meanings set forth in the Cisco General Terms or General Disclosures. To the extent this document differs from the Cisco Online Privacy Statement or General Disclosures, this document will take precedence regarding Offer specific information. If there is a difference in the translated, non-English versions of this document, the US-English version will take precedence.

Cisco will review and update this disclosure on an annual basis, or as needed, to reflect material changes in the processing of Customer Systems Information or Customer Content. For updates, subscribe via the "subscribe" link in the upper right corner of the [Trust Portal](#).

## 1. Overview

Webex Meetings (the "Cisco Offer" or "Webex Meetings") is a cloud-based web and video conferencing solution made available by Cisco to companies or persons (each as "Customer," "you," or "your") who acquire it for use by their authorized users (each, a "user"). The Cisco Offer 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, and support services. For more information regarding optional features for Webex Meetings, please see the addenda below.

This Offer Disclosure covers Webex Meetings, Webex Webinars, and Webex Support. If you use the Cisco Offer together with the Webex App, see the Webex App Offer Disclosure (available on [The Cisco Trust Center](#)) for description of data that may be collected and processed in connection with those services.

For more information about Webex Meetings, visit the Cisco Web Conferencing [homepage](#).

## 2. Data Handling

### 2a. Collection, Purpose & Retention

Cisco believes in transparency when it comes to how Cisco handles Customer Content and Customer Systems Information. This disclosure provides details about the types of data Cisco collects, specific data elements involved, the purposes for which they are used, and how long Cisco retains them for this Cisco Offer.

**Personal Data Processing.** If you are a user and your employer is the Customer that acquired the Cisco Offer, your employer serves as the data controller of data processed by the Cisco Offer. The information described in the table below and in this Offer Disclosure 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 Cisco Offer.

Similarly, if users participate in meetings hosted by users in other companies, the meeting host and/or co-host will control any meeting recordings, files or other information 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 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.

Because the Cisco Offer enables collaboration among its users, your Personal Data is required to use the Cisco Offer.

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 your meeting traffic or content,
- monitor or track user geolocation, or
- process or use any Customer Content described in this Offer Disclosure to train any Webex Meetings AI models without your authorization. To "train" in this context includes to evaluate, improve, fine-tune, or develop any Webex Meetings AI models.

**Data Retention.** Subject to their employer’s corporate retention policies, users with an active subscription can delete User-Generated Information from their account through the Webex User Hub 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.

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

**Table 1: Customer Content**

Data Category	Data Elements (Examples)	Purposes	Retention Period	Reason for retention
User Information	<b>Personal Data:</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Email Address</li> <li>• Password</li> <li>• Browser</li> <li>• Phone Number (optional)</li> <li>• Mailing Address (optional)</li> <li>• Profile Picture or Avatar image (optional)</li> </ul>	<ul style="list-style-type: none"> <li>• Provide you with the Cisco Offer</li> <li>• Enroll you in the Cisco Offer</li> <li>• Respond to customer support requests</li> <li>• Authenticate and authorize access to your account</li> <li>• Display directory information to other Webex users</li> <li>• Display your Avatar image and profile to other users (Avatar</li> </ul>	<b>When you are an active customer:</b> <ul style="list-style-type: none"> <li>• As long as you maintain an active subscription (paid or free)</li> </ul> <b>Upon termination/expiration:</b> <ul style="list-style-type: none"> <li>• Name and UUID are retained for 13 months from termination</li> </ul>	<ul style="list-style-type: none"> <li>• Name and UUID are maintained as part of Cisco’s business records and to comply with Cisco’s financial and audit requirements.</li> <li>• Account information provided to Cisco during the provisioning of the service is maintained for billing purposes.</li> </ul>

	<ul style="list-style-type: none"> <li>• User Information Included in Your Directory (if synced)</li> <li>• Unique User ID (UUID) (a pseudonymized 128-bit number assigned to compute nodes on a network)</li> <li>• User settings</li> </ul>	<p>image may be cached locally on devices of other Webex users that attend meetings with you for a period of 2 weeks)</p> <ul style="list-style-type: none"> <li>• Customer relationship management (e.g., transactional communication)</li> <li>• Bill you for the Cisco Offer</li> </ul>		
<b>User-Generated Information</b>	<p><b>Personal Data (optional and only applicable if you enable the relevant capability):</b></p> <ul style="list-style-type: none"> <li>• Meeting Recordings</li> <li>• Transcriptions of Meeting Recordings</li> <li>• Uploaded Files</li> <li>• Whiteboard content</li> <li>• Chat Messages</li> <li>• Annotations</li> <li>• Information Submitted Through Attendee Registration Form</li> </ul> <p><b>Personal Data:</b></p> <ul style="list-style-type: none"> <li>• Meeting Host Information<sup>1</sup> (Host Name and Email Address, Meeting Site URL, Meeting Start/End Time)</li> <li>• Meeting Title</li> <li>• Call Attendee Information, including Email Addresses, IP Addresses, Usernames, Phone Numbers</li> </ul>	<ul style="list-style-type: none"> <li>• Provide you with the Cisco Offer</li> </ul>	<p><b>When you are an active customer:</b></p> <ul style="list-style-type: none"> <li>• At Customer’s discretion for up to 360 days (or up to 1095 days with the purchase of Pro Pack)</li> <li>• 6 months for free users</li> <li>• 30 days post-deletion for user-deleted recordings</li> </ul> <p><b>Upon termination/expiration:</b></p> <ul style="list-style-type: none"> <li>• 60 days after service termination or account deactivation</li> </ul>	<p><b>When you are an active customer:</b></p> <ul style="list-style-type: none"> <li>• Retained based on Customer’s discretion (Customer controls retention settings).</li> <li>• If a user deletes User-Generated Information, Cisco no longer retains that information on the Webex platform, except for recordings, which are retained for a short time to allow users to retrieve recordings inadvertently deleted, and for Customer compliance purposes.</li> </ul> <p><b>Upon termination/expiration:</b></p> <ul style="list-style-type: none"> <li>• Retained for a short time after service termination to allow users the opportunity to download it.</li> </ul>
<b>Webex-Generated Content</b>	<p><b>Personal Data (all optional and only applicable if you enable the relevant feature or functionality):</b></p> <ul style="list-style-type: none"> <li>• AI Assistant –Generated Content</li> <li>• Images from the user’s camera feed during a Meeting (assuming you have turned on your camera)</li> </ul>	<ul style="list-style-type: none"> <li>• Provide you with the Cisco Offer</li> </ul>	<p><b>When you are an active customer:</b></p> <ul style="list-style-type: none"> <li>• At Customer’s or user’s discretion</li> <li>• AI Assistant-generated content is retained for 7 days from generation</li> </ul>	<ul style="list-style-type: none"> <li>• Webex-Generated Content generally is not retained on the Webex Meetings platform if Customer or user deletes this data.</li> <li>• AI Assistant-Generated Content is retained to allow a Customer or user to download it.</li> <li>• In-Meeting AI Assistant-Generated</li> </ul>

<sup>1</sup> Used for billing purposes.

				<p>Content is not retained after the meeting.</p> <ul style="list-style-type: none"> <li>Images from the user's camera feed during a Meeting, which are processed to provide the functionality of certain optional features that use the images (for example the Auto Step Away feature or the Virtual Background, Blur and Effects feature), are not retained on the Webex Meetings platform.</li> </ul>
--	--	--	--	---

**Calendar.** If you use a Webex plug-in with your Calendar service, 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.

**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 the Slido Offer Disclosure.

**Extended Security Pack.** If you purchase the extended security pack, please see the [Cloudlock Offer Disclosure](#) for Cloudlock data privacy information.

**Table 2: Customer Systems Information**

Data Category	Data Elements (Examples)	Purposes	Retention Period	Reason for retention
Host and Usage Information	<p><b>Personal Data:</b></p> <ul style="list-style-type: none"> <li>IP Address</li> <li>User Agent Identifier</li> <li>Hardware Type</li> <li>Operation System Type and Version</li> <li>Client Version</li> </ul>	<ul style="list-style-type: none"> <li>Provide you with the Cisco Offer</li> <li>Diagnose technical issues</li> <li>Conduct analytics and statistical analysis for Customer to provide Customer</li> </ul>	<p><b>When you are an active customer:</b></p> <ul style="list-style-type: none"> <li>13 months for paid users, except IP Addresses, which are retained for (i) 30 days, then (ii) 6 months in access logs archival storage</li> </ul>	<ul style="list-style-type: none"> <li>IP addresses are retained to support Customer reporting in Webex Control Hub, as well as for security purposes.</li> <li>Other Host and Usage Information used for purposes such as analytics and</li> </ul>

	<ul style="list-style-type: none"> <li>IP Addresses Along the Network Path MAC Address of Your Client (as applicable)</li> <li>Service Version</li> <li>Actions Taken</li> <li>Geographic Region (e.g., Country Code)</li> <li>Meeting Session Information (e.g., date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity)</li> <li>Number of Meetings</li> <li>Number of Screen-Sharing and Non Screen-Sharing Sessions</li> <li>Number of Participants</li> <li>Screen Resolution</li> <li>Join Method</li> <li>Performance, Troubleshooting, and Diagnostics Information</li> <li>Meeting Host Information<sup>2</sup> (Host Name and Email Address, Meeting Site URL, Meeting Start/End Time)</li> <li>Meeting Title</li> <li>Call Attendee Information, including Email Addresses, IP Addresses, Usernames, Phone Numbers, Room Device Information</li> <li>Information Submitted Through Attendee Registration Form (optional, only applicable if you provide)</li> </ul>	<p>administrators visibility into usage</p> <ul style="list-style-type: none"> <li>Respond to Customer support requests</li> <li>Help organize, sort, and/or prioritize your Webex App messages or spaces in a way that is relevant to you and your work</li> <li>Provide you the Collaboration Insights feature (including Personal Insights) (optional)</li> <li>Bill you for the Cisco Offer</li> <li>Diagnostic and troubleshooting purposes</li> </ul>	<ul style="list-style-type: none"> <li>30 days for free users</li> </ul>	<p>troubleshooting is kept to provide technical support when requested by Customer and to improve the experience for Webex users.</p>
<b>Configuration Data</b>	<p><b>Non-Personal Data:</b></p> <ul style="list-style-type: none"> <li>User preferences</li> <li>Device settings</li> <li>Software configurations</li> <li>Other customizable options</li> </ul>	<ul style="list-style-type: none"> <li>Tailor the functionality of a system to specific requirements or preferences</li> </ul>	<p><b>When you are an active customer:</b></p> <ul style="list-style-type: none"> <li>User information will be maintained as long as Customer maintains an active subscription (paid or free)</li> </ul> <p><b>Upon termination/expiration:</b></p>	<ul style="list-style-type: none"> <li>Provide you with the Cisco Offer.</li> </ul>

<sup>2</sup> Used for billing purposes.

			<ul style="list-style-type: none"> <li>Deleted once the Cisco Offer is terminated</li> <li>Name and UUID are maintained 7 years from termination</li> </ul>	
<b>Events Data</b>	<b>Non-Personal Data:</b> <ul style="list-style-type: none"> <li>Records or logs of specific occurrences, actions, or incidents (activity logs)</li> </ul>	<ul style="list-style-type: none"> <li>Troubleshooting, auditing, monitoring, analysis, and reporting purposes to understand the behavior and performance of systems and applications</li> </ul>	<ul style="list-style-type: none"> <li>13 months</li> </ul>	<ul style="list-style-type: none"> <li>Respond to customer support requests and diagnose technical issues.</li> <li>Provide Customer administrators visibility into usage.</li> </ul>
<b>Telemetry Data</b>	<b>Non-Personal Data:</b> <ul style="list-style-type: none"> <li>Status updates</li> <li>Performance metrics</li> </ul>	<ul style="list-style-type: none"> <li>Monitoring and analysis</li> </ul>	<ul style="list-style-type: none"> <li>13 months</li> </ul>	<ul style="list-style-type: none"> <li>Respond to customer support requests and diagnose technical issues.</li> <li>Provide Customer administrators visibility into usage.</li> </ul>

## 2b. Storage and Processing

**Data Centers.** Cisco uses its own data centers as well as third-party infrastructure providers to deliver this Cisco Offer’s capabilities globally. These data centers are currently located in the following countries (data center locations may change from time to time, and this Offer Disclosure will be updated to reflect those changes).

**Table 3: Data Centers**

Cisco Data Center Locations	Media Data Center Locations	Internet Point of Presence (iPOP) Locations
Dallas, TX, USA	Dallas, TX, USA	Amsterdam, Netherlands
San Jose, CA, USA	San Jose, CA, USA	Los Angeles, California, USA
Toronto, Canada	Amsterdam, Netherlands	Chicago, Illinois, USA
Amsterdam, Netherlands	Frankfurt, Germany	New York, New York, USA
Mumbai, India	London, UK	Sydney, Australia
London, UK	Sao Paulo, Brazil	Dallas, Texas, USA
Singapore, Singapore	Singapore, Singapore	Ashburn, VA, USA
Tokyo, Japan	Sydney, Australia	

Sydney, Australia	Tokyo, Japan	
Secaucus, New Jersey, USA	Mumbai, India	
Frankfurt, Germany	Secaucus, New Jersey, USA	
Jeddah, Saudi Arabia	Jeddah, Saudi Arabia	
Riyadh, Saudi Arabia	Riyadh, Saudi Arabia	
Montreal, Canada		
Portland, Oregon, USA		
Columbus, Ohio, USA		
Culpeper, Virginia, USA		

**Media Data Centers.** Media Data Centers represent infrastructure where real-time media stream traffic may be processed but not retained.

**Internet Point of Presence Locations.** 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 traffic through Cisco's infrastructure and improve performance. Data routed through iPOP Locations remains encrypted and is not stored in that location.

For this Cisco Offer, User-Generated Information and Webex-Generated Content are 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.

**Webex Personal Data Residency.** Webex Personal Data residency provides Customer administrators (or partner administrators on the Customer's behalf) the ability to choose where their organization's Personal Data is stored. Personal Data residency is currently available for Customers in the European Union (EU) ("EU Customers"), Customers in Canada ("Canadian Customers"), and Customers in the United States ("US Customers") for Personal Data processed by Webex Meetings, including User Information, Host & Usage Information, User-Generated Information, and AI Assistant-Generated Content (other than as noted below).<sup>3</sup> 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, Customer 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.

<sup>3</sup> For Canadian Customers, certain Usage Information, including Usage Information related to billing will continue to be stored in the US.

For Canadian Customers who were provisioned before July 2022, Customer administrators were offered the option to migrate their user data to Canada. US Customers who are provisioned in the US by their Customer administrators will have their Personal Data processed and stored in the US.

To facilitate certain operations and aspects of the Cisco Offer, certain exceptions to Webex Personal 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](http://www.webex.com) or [www.cisco.com](http://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, Personal Data defined in this Offer Disclosure may be stored in a Webex data center outside the account holder’s region, including for EU and Canadian Customers.

**Service Providers.** Cisco may share Customer Systems Information and Customer Content with a trusted ecosystem of suppliers. In each instance, each participant has agreed to confidentiality terms, compliance with applicable law, and adherence to information security, privacy, and other data processing requirements with Cisco that are consistent with Cisco’s commitments to you.

Subcontractors assist with broader data processing services, while subprocessors specifically process Personal Data on Cisco’s behalf to support the functionality of the Cisco Offer. Both are listed below. For updates, subscribe via the “subscribe” link in the upper right corner of the Trust Portal.

**Table 4: Subprocessors and Subcontractors**

Name	Personal Data	Service Type	Cisco Data Center Location
<b>Akamai</b>	<ul style="list-style-type: none"> <li>IP Address</li> <li>Browser and Geographic Region</li> </ul>	<p>Akamai is used as content delivery network (CDN) services provider for static content.</p> <p>Akamai does not store content but may store IP addresses in logs for a maximum of 3 years.</p>	<ul style="list-style-type: none"> <li>Location generally maps to Customer’s Webex data center assignment.</li> <li>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).</li> </ul>

<b>Amazon Web Services (AWS)</b>	<ul style="list-style-type: none"> <li>• Limited Host &amp; Usage Information</li> <li>• Meeting Recording Files (if applicable)</li> <li>• AI Assistant-Generated Content</li> </ul>	<p>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.)</p> <p>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.</p> <p>AWS cloud infrastructure is also used to store Meetings recording files, if meeting recording is enabled by the Customer. (Location maps to Customer's Webex data center assignment).</p> <p>AWS is leveraged to provide certain AI features.</p>	<ul style="list-style-type: none"> <li>• United States</li> <li>• Germany</li> <li>• Netherlands</li> <li>• United Kingdom</li> <li>• Brazil</li> <li>• Australia</li> <li>• Japan</li> <li>• Singapore</li> </ul>
<b>Microsoft</b>	<ul style="list-style-type: none"> <li>• Enrollment information</li> <li>• Host &amp; Usage Information</li> <li>• User-Generated Information</li> <li>• Webex-Generated Content</li> </ul>	<p>Microsoft is leveraged to provide certain AI features.</p>	<ul style="list-style-type: none"> <li>• European Union (and Switzerland)</li> <li>• United Kingdom</li> <li>• United States</li> <li>• Australia</li> <li>• Singapore</li> </ul>

**Note:** Data shared with sub-processors follows Webex data residency, except for those sub-processors who may be implicated by one of the listed exceptions to the Webex data residency.

### Technical Support and Operations

Customer support is provided by Cisco Technical Assistance Center (TAC); more information regarding the data centers and service providers can be found in the [TAC Offer Disclosure](#).

## 2c. Access and Sharing

Customers and their authorized third parties may directly access Customer Systems Information as well as Personal Data described in this Offer Disclosure by using service-standardized data interfaces, to the extent those are described in API documentation found [here](#), [Webex for Developers Terms of Service](#) and subject to the provisions of the written or electronic agreement between the Customer and Cisco for the provision of the Cisco Offer to the Customer or any other terms where the parties expressly agree to this document (e.g. the Cisco General Terms).

The categories, volume, and frequency of Customer Systems Information generated by this Cisco Offer are dependent on the Customer's configuration and use case(s).

Webex for Developers APIs support both structured and unstructured data sets. Depending on the standard implemented by the API, structured data sets may use JSON, XML, or other standardized data formats; while unstructured data sets may be in the form of text, PDF or other unstructured data file formats. For more details, please consult the API documentation referenced above.

Customers may send requests for expanded API or data interface capabilities through their usual Cisco support or account management channels. 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.

Some data made available in connection with this Cisco Offer is considered a Cisco Trade Secret, and is released pursuant to the confidentiality obligations set forth in [Cisco's General Terms](#). To the extent that any information comprising Cisco's algorithms, analysis, inferences, proprietary software, insights, derivations, or assigned values can be viewed, reverse engineered, reconstituted, or otherwise interpreted from the data, such information is a "Cisco Trade Secret," and subject to such confidentiality obligations.

Regardless of whether the data made available in connection with this Cisco Offer is a Cisco Trade Secret, such data is subject to the following use restrictions:

- Data shall not be analyzed for the purpose of deriving insights about Cisco's economic situation, assets or production methods.
- Data cannot be used to develop a product that competes with the product from which the data originates.

## **2d. Data Portability**

The Cisco Offer allows Customers and users to export all User-Generated Information and Webex-Generated Content. A Customer's administrator may do so using APIs provided with the Cisco Offer (recordings only) or through the Site Admin Page, while individual users may do so through the Webex User Hub. 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.

# 3. Security

## 3a. Access Control and Encryption

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

**Table 5: Access & Controls**

Data Category	Who Has Access	Purpose of Access	Security Controls
<b>User Information</b>	User through Webex User Hub	Modify, control, and delete User Information	Encrypted in transit and at rest.  Passwords (stored if Single Sign On is not configured) are encrypted and hashed in transit and at rest.
	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 Cisco Offer in accordance with Cisco's data access and security controls process	
<b>Host and Usage Information</b>	Host through the Webex User Hub	View meeting session information	Encrypted in transit and at rest
	Customer may view this information through the Site Admin Page, Webex Control Hub, or may be otherwise provided by Cisco	View usage, meeting session and configuration information	
	Cisco	Diagnostic and troubleshooting	
<b>User-Generated Information</b>	User through the Webex User Hub	Modify, control, and delete based on user's preference	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.
	Customer using APIs provided with the Cisco Offer 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 Cisco Offer, 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 Cisco Offer,	

		copies of that content may remain viewable elsewhere to the extent it has been shared with others	
<b>Webex-Generated Content</b>	Users through the Webex User Hub	Modify, control, and delete based on user's preference	Encrypted in transit and at rest.
	Customer using APIs (if any are provided with the Cisco Offer) 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 Cisco Offer, 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	

**Protecting Data at Rest.** The Cisco Offer encrypts User Information, Passwords, User-Generated Information, and Webex-Generated Content, 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 signaling. 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 behavior 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 signaling 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 Cisco Offer.

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

### **3b. Reports & Resources**

In addition to complying with internal standards, Cisco maintains third-party validations and certifications to demonstrate its commitment to robust information security and privacy. The General Disclosures describe Cisco’s enterprise-wide certifications. The following additional resources and certifications apply specifically to this Offer:

- 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
- ISO 22301 Certification (Business Continuity Management System)
- SOC 2 Type II Report

- BSI Cloud Computing Compliance Criteria Catalogue (German C5)
- CSA STAR Level 2 Certification)
- FedRAMP
- HIPAA Attestation
- Spanish Esquema Nacional de Seguridad Certification
- Australian IRAP (Information Security Registered Assessors Program) Certification
- Digital Trust Label (Switzerland)
- Electronic Transactions Development Agency Certification (Thailand)
- French Health Data Hosting (Hébergeurs de Données de Santé - HDS) Certification. The HDS certification (found on the Cisco Trust Portal) applies to the Webex service provisioned in the European Economic Area (EEA). Webex Meetings adheres to the HDS requirements by providing robust infrastructure and dedicated storage within the EEA. In order to comply with version 2.0 of the HDS referential data residency requirements, HDS customers must select a region within the EEA for data storage to meet the standard. Further evaluation of the customer's own requirements and manual configuration of the product is at the customer's discretion.

## 4. Artificial Intelligence

Cisco prioritizes trust and transparency, including when it comes to development and deployment of AI. Our AI Transparency Technical Notes provide a high-level understanding of how Webex leverages AI models to deliver AI-enabled features. Visit the Trust Portal and select 'AI Transparency' from the document type filter in the left-hand menu to see [all available AI Transparency Technical Notes](#).

# 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 Offer Disclosure. 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.

### 1. 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 not be 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.

## 2. 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
<b>Publicly Available Business and Professional Biographical Data</b>	<ul style="list-style-type: none"> <li>• Profile Photos</li> <li>• News</li> <li>• Tweets</li> <li>• Authored Works</li> <li>• Bios</li> <li>• Employment History</li> <li>• Education History</li> <li>• Web Links for a specific person</li> </ul>	<ul style="list-style-type: none"> <li>• Provide you with the Feature</li> <li>• To source the People Insights profile and to enable search within the Feature</li> </ul>
<b>Account and Usage Information</b>	<ul style="list-style-type: none"> <li>• User Level Account Details (including email, name, and web interactions and platform usage)</li> </ul>	<ul style="list-style-type: none"> <li>• Provide you with the Feature</li> <li>• Product analytics (e.g., frequency of profile edits, number of successful profile loads in a meeting, etc.)</li> </ul>
<b>Directory Data</b>	<ul style="list-style-type: none"> <li>• 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):</li> <li>• Title</li> <li>• Phone Number</li> <li>• Location</li> <li>• Organization</li> </ul>	<ul style="list-style-type: none"> <li>• Provide you with the Feature</li> <li>• 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.</li> </ul>

	<ul style="list-style-type: none"> <li>• Department</li> <li>• Photo</li> <li>• Role</li> <li>• Reporting Structure</li> <li>• Pronouns (optional, only applicable if available in your organization)</li> </ul>	
<b>User-Generated Information</b>	<ul style="list-style-type: none"> <li>• Information that the user adds in their People Insights profile.</li> </ul>	<ul style="list-style-type: none"> <li>• Provide you with the Feature</li> <li>• Augment the user's own People Insights profile (visible to People Insights users)</li> </ul>

### 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. 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
<b>Publicly Available Business and Professional Biographical Data</b>	<ul style="list-style-type: none"> <li>• Cisco</li> </ul>	<ul style="list-style-type: none"> <li>• To provide the Feature</li> </ul>
	<ul style="list-style-type: none"> <li>• Users of Customer Webex site with enabled People Insights</li> </ul>	
<b>Account and Usage Information</b>	<ul style="list-style-type: none"> <li>• Cisco</li> </ul>	<ul style="list-style-type: none"> <li>• Registration Support</li> <li>• Correlate users with correct profiles</li> <li>• Analytics to improve service</li> </ul>
	<ul style="list-style-type: none"> <li>• Customer</li> </ul>	<ul style="list-style-type: none"> <li>• Feature enablement/disablement</li> </ul>
<b>Directory Data</b>	<ul style="list-style-type: none"> <li>• Customer (Admin)</li> <li>• People Insight users within the Customer's organization</li> </ul>	<ul style="list-style-type: none"> <li>• Directory data is provided and maintained by Customer administrator to allow integration into People Insights profile</li> </ul>
	<ul style="list-style-type: none"> <li>• Cisco</li> </ul>	<ul style="list-style-type: none"> <li>• Directory data is imported and integrated with Customer profile data to support profile development</li> </ul>
<b>User-Generated Information</b>	<ul style="list-style-type: none"> <li>• User</li> </ul>	<ul style="list-style-type: none"> <li>• Users may access their own User-Generated Information to edit or delete content</li> </ul>

## 5. Data Portability

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

## 6. Data 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
<b>Publicly Available Business &amp; Professional Data</b>	<p><b>Obtained from public websites:</b> three (3) years</p> <p><b>Obtained through third-party APIs:</b> In accordance with contractual requirements</p>	<p>Publicly Available Business &amp; 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.</p> <p>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.</p> <p>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.</p>
<b>Account and Usage Information</b>	<p><b>Active Subscriptions:</b> At Customer's or user's discretion</p> <p><b>Deactivated Accounts:</b> Deleted within thirty (30) days</p>	Users can request to remove their Account Information by opening a TAC service request. Cisco will respond to such requests within thirty (30) days.
<b>Directory Data</b>	<p><b>Active Subscriptions:</b> At Customer's or user's discretion</p> <p><b>Deactivated Accounts:</b> Deleted within thirty (30) days</p>	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.
<b>User-Generated Information</b>	<p><b>Active Subscriptions:</b> At Customer's or user's discretion</p> <p><b>Deactivated Accounts:</b> Deleted within thirty (30) days</p>	Users can delete User-Generated Information from their profile at any time.

## 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.

Personal Data Category	Security Controls and Measures
------------------------	--------------------------------

<b>Publicly Available Business &amp; Professional Data</b>	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS
<b>Account and Usage Information</b>	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS
<b>Directory Data</b>	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS
<b>User-Generated Information</b>	Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS

## 8. 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
<b>Amazon Web Services</b>	<ul style="list-style-type: none"> <li>• Publicly Available Business &amp; Professional Data</li> <li>• Host &amp; Usage Information</li> <li>• Directory Data</li> <li>• User-Generated Information</li> </ul>	Cloud Storage	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 Offer Disclosure. 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. 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 Cisco Offer 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
<b>User Information</b>	<ul style="list-style-type: none"><li>• Name (First, Last)</li><li>• Email</li><li>• User ID</li></ul>	<ul style="list-style-type: none"><li>• Enroll you in the Feature and enable opt-in</li><li>• To display name of recognized user</li></ul>
<b>Biometrics</b>	<ul style="list-style-type: none"><li>• User facial image</li><li>• Facial vector mapping</li></ul>	<ul style="list-style-type: none"><li>• To create facial vector mapping and provide the Feature</li><li>• To generate a new facial vector in case of a modification or update to the Feature algorithm</li></ul>
<b>Host and Usage Information</b>	Information regarding accuracy of product, including: <ul style="list-style-type: none"><li>• Successful and unsuccessful facial vector matching</li><li>• User feedback</li></ul>	<ul style="list-style-type: none"><li>• To provide support and product analytics</li><li>• Make improvements to the Feature</li><li>• Diagnostic and troubleshooting purposes</li></ul>
<b>Location</b>	<ul style="list-style-type: none"><li>• Meeting Room Proximity data</li></ul>	<ul style="list-style-type: none"><li>• Proximity data is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations</li></ul>
<b>Calendar</b>	<ul style="list-style-type: none"><li>• Meeting Room Calendar Information</li></ul>	<ul style="list-style-type: none"><li>• Calendar information is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations</li></ul>

## 3. 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	<ul style="list-style-type: none"> <li>To display name of recognized user</li> <li>Enroll you in the Feature and enable opt-in</li> </ul>
	Customer	<ul style="list-style-type: none"> <li>View user facial recognition registration status</li> </ul>
	Users through <a href="https://settings.webex.com/">https://settings.webex.com/</a>	<ul style="list-style-type: none"> <li>View and modify facial recognition registration details</li> </ul>
Biometrics	Cisco	<ul style="list-style-type: none"> <li>To provide the Feature</li> <li>Algorithm improvement</li> <li>To troubleshoot issues in the event Customer or users request support</li> </ul>
Host and Usage Information	Cisco	<ul style="list-style-type: none"> <li>To provide support and product analytics</li> </ul>
Location	Cisco	<ul style="list-style-type: none"> <li>Proximity data is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations</li> </ul>
Calendar	Cisco	<ul style="list-style-type: none"> <li>Calendar information is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations</li> </ul>

## 4. Data Portability

While Webex Meetings allows Customers and users to export data as described in Offer Disclosure, it does not support the automatic export of Facial Recognition data.

## 5. Data 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	<p>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.</p> <p>All other User Information is not stored or retained by the Feature as this information is already stored by Webex Meetings.</p>	<p>User ID is used to track your enrollment in the Feature.</p> <p>Names are displayed upon a match in the Feature.</p>

<b>Biometrics</b>	<p>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.</p> <p>Images for all users are deleted upon Customer's discontinuation of the Cisco Offer.</p>	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.
	<p>Facial vectors are retained as long as the facial images but are stored separately.</p> <p>Facial vectors are deleted upon discontinuation of the Cisco Offer.</p>	The facial vectors are used to provide the Feature.
<b>Host and Usage Information</b>	2 weeks	To provide support and product analytics.
<b>Location</b>	2 days	Proximity data is used to improve Facial Recognition to assure images are assigned to the correct users in the correct locations.
<b>Calendar</b>	Facial Recognition does not store or retain this information separately than already maintained by Webex Meetings.	

## 6. 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.

<b>Personal Data Category</b>	<b>Security Controls and Measures</b>
<b>User Information</b>	Encrypted in transit, AES 256 for storage
<b>Images</b>	Encrypted in transit, AES 256 for storage
<b>Biometrics</b>	Encrypted in transit, AES 256 for storage
<b>Host and Usage Information</b>	Encrypted in transit, AES 256 for storage
<b>Location</b>	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 Offer Disclosure. 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.

## 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; Customer administrators can select enablement for specific users or, if a Customer 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.

Customer 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
<b>Host and Usage Information</b>	<ul style="list-style-type: none"> <li>Usage of Closed Captioning, including number of Webex Meetings with Closed Captioning enabled, and troubleshooting events</li> </ul>	<ul style="list-style-type: none"> <li>Provide Closed Captioning</li> <li>Provide Customer with usage information</li> <li>Diagnose technical issues</li> <li>Improve the technical performance of the Cisco Offer</li> <li>Understand how Closed Captioning is used</li> </ul>
<b>User-Generated Information</b>	<ul style="list-style-type: none"> <li>Audio captured during meeting (Audio Information)</li> <li>Webex Meetings Transcript (Transcript Information)</li> <li>Text of real-time speech for translations (Transcript Information)</li> </ul>	<ul style="list-style-type: none"> <li>Provide Closed Captioning</li> <li>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.</li> </ul>

## 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. 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
<b>User Information</b>	Cisco	Enroll users in Closed Captioning.
	Customer	Enable/disable Closed Captioning for specific Webex Meetings users or an entire site.
<b>Host and Usage Information</b>	Cisco	Support and improve the Cisco Offer in accordance with Cisco's data access and security controls.
	Customer	View and analyze usage information.
	Cisco	While Cisco operates the Cisco Offer, Cisco will not access this data unless it is shared with Cisco by Customer and will only

<b>User-Generated Information (Audio Information)</b>		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 Offer Disclosure.
	User	No highlights or meeting audio information is retained after the meeting when Close Captioning only is used during the live meeting
<b>User-Generated Information (Transcript Information)</b>	Cisco	While Cisco operates the Cisco Offer, 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.

## 5. 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.

## 6. Data 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 Webex User Hub 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
-----------------------	------------------	----------------------

<b>User Information</b>	User Information is not separately stored or retained as part of Closed Captioning, as this information is already stored by Webex Meetings.	
<b>Host and Usage Information</b>	Deleted after 3 years	Usage information used to conduct analytics and measure statistical performance is retained but pseudonymized.
<b>User-Generated Information</b>	<p><b>Active Subscriptions:</b> Audio Information and Transcript highlights may be deleted at Customer's or user's discretion.</p> <p><b>Terminated Service:</b> Deleted within 60 days</p>	<p>User-Generated Information is retained to provide you with the Cisco Offer and will be deleted once it is no longer necessary to provide the Cisco Offer. Any User-Generated Information retained after the Cisco Offer is terminated is retained solely to make it available to Customers for download.</p> <p>User-Generated 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 <a href="#">here</a>.</p>

## 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 the encryption architecture of data stored specifically for Closed Captioning.

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

## 8. 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:

<b>Sub-processor</b>	<b>Personal Data</b>	<b>Service Type</b>	<b>Location of Data Center</b>
----------------------	----------------------	---------------------	--------------------------------

<b>Amazon Web Services</b>	Audio Information	Cloud Infrastructure (transient storage only)	US, Singapore, France, Japan, Ireland, Sweden
<b>Google</b>	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.	<ul style="list-style-type: none"> <li>• Speech-to-Text service (voice commands only)</li> <li>• Text-to-Speech service (voice command responses only)</li> </ul>	US, Germany, Singapore, Netherlands, Belgium, Japan
<b>Google*</b>	Transcript Information	<p>Provide translation and/or foreign language transcription using text of real-time speech.</p> <p>Google may process but not store transcript Information to provide speech-to-text services</p> <p>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.</p>	<p>Globally</p> <p>For EU Customers, within the EU</p>
	Audio Information (except if spoken language chosen is English, French, German, Italian, Spanish)	<p>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.</p> <p>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.</p>	<p>Globally</p> <p>For EU Customers, within the EU</p>
<b>Azure*</b>	Transcript Information	<p>Provide translation and/or foreign language transcription using text of real-time speech.</p> <p>Azure may process but not store transcript Information to provide speech-to-text services</p> <p>Transcript data is processed by Azure at global endpoints, except when a Customer is provisioned in the European Union (EU). For EU Customers, transcript data processed by Azure is processed within region as part of Webex Data Residency.</p>	<p>Globally</p> <p>For EU Customers, within the EU</p>
	Audio Information (except if spoken language chosen is English, French, German, Italian, Spanish)	<p>When you add-on and use the real-time translation and transcription feature in multiple languages, Azure may process but not store Audio Information to provide speech-to-text services.</p> <p>Audio data is processed by Azure at global endpoints, except when a Customer is provisioned in the EU. For EU Customers, audio data processed by Azure is processed within region as part of Webex Data Residency.</p>	<p>Globally</p> <p>For EU Customers, within the EU</p>

\* 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 Offer Disclosure. 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.

## 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 Customer 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 Customer 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
<b>User Information</b>	<ul style="list-style-type: none"> <li>• Name (First, Last)</li> <li>• Email</li> <li>• Username</li> <li>• Unique User Identifier (UUID)</li> </ul>	<ul style="list-style-type: none"> <li>• Enable Webex Assistant for specific Webex Meetings users or for an entire site</li> <li>• Provide Webex Assistant</li> </ul>
<b>Host and Usage Information</b>	<ul style="list-style-type: none"> <li>• Usage of the Webex Assistant features, including number of meetings with Webex Assistant enabled, number/type of Highlight views/edits/downloads, troubleshooting events</li> </ul>	<ul style="list-style-type: none"> <li>• Provide Webex Assistant</li> <li>• Provide Customer with usage information</li> <li>• Improve the technical performance of the Cisco Offer</li> <li>• Diagnose technical issues</li> <li>• Understand how Webex Assistant is used</li> </ul>
<b>User-Generated Information</b>	<ul style="list-style-type: none"> <li>• Webex Meetings Recordings</li> <li>• Audio Commands to Webex Assistant</li> <li>• Audio captured during meeting</li> <li>• Webex Meetings Transcript</li> <li>• Text of meeting Highlight</li> <li>• Text of real-time speech for translations</li> </ul>	<ul style="list-style-type: none"> <li>• Provide Webex Assistant</li> <li>• 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 <a href="#">here</a>.</li> </ul>

## 3. Data Center Locations

Cisco leverages its own data centers as well as third-party hosting providers and business partners to deliver the Cisco Offer, 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. 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
<b>User Information</b>	Cisco	Enroll users with Webex Assistant.
	Customer	Enable Webex Assistant for specific Webex Meetings users or for an entire site.
<b>Host and Usage Information</b>	Cisco	Support and improve the Cisco Offer in accordance with Cisco's data access and security controls.
	Customer	View and analyze usage information.
<b>User-Generated Information (Audio Information)</b>	Cisco	While Cisco operates the Cisco Offer, 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 Offer Disclosure.
	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.
<b>User-Generated Information (Transcript Information)</b>	Cisco	While Cisco operates the Cisco Offer, 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.

## 5. Data Portability

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

## 6. Data 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 Webex User Hub 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
<b>User Information</b>	User Information is not separately stored or retained by Webex Assistant as this information is already stored by Webex Meetings.	
<b>Host and Usage Information</b>	Deleted after 3 years.	Usage information is used to conduct analytics and measure statistical performance.
<b>User-Generated Information</b>	<p><b>Active Subscriptions:</b> Audio Information and Highlights may be deleted at Customer's or user's discretion.</p> <p><b>Terminated Service:</b> Deleted within 60 days</p>	<p>Audio Information and Transcript Information is retained in order to provide you with the Cisco Offer and will be deleted once it is no longer necessary to provide the Cisco Offer.</p> <p>Any Audio Information or Transcript Information retained after the Cisco Offer is terminated is retained solely to make it available to Customers for download.</p> <p>Audio Information and Transcript 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.</p>
<b>Host and Usage</b>	Deleted after 3 years.	Usage information is used to conduct analytics and measure statistical performance.

## 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 Webex Assistant.

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

## 8. 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
<b>Amazon Web Services</b>	Audio Information	Cloud Infrastructure (transient storage only)	US, Singapore, France, Japan, Ireland, Sweden
<b>Google</b>	<p>Audio and transcript of Voice Command only (e.g., “OK, Webex, create a note”).</p> <p>Please note that the core transcription technology that processes and stores all other Audio and Transcript Information is owned, managed and executed by Cisco.</p>	<ul style="list-style-type: none"> <li>Speech to Text service (voice commands only)</li> <li>Text to Speech service (voice command responses only)</li> </ul>	US, Germany, Singapore, Netherlands, Belgium, Japan
<b>Google*</b>	Transcript Information	<p>Provide translation using text of real-time speech.</p> <p>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.</p>	<p>Globally</p> <p>For EU Customers, within the EU</p>
	Audio Information (except if spoken language chosen is English, French, German, Italian, Spanish)	<p>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</p> <p>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.</p>	<p>Globally</p> <p>For EU Customers, within the EU</p>
<b>Azure*</b>	Transcript Information	<p>Provide translation using text of real-time speech.</p> <p>Transcript data is processed by Azure at global endpoints, except when a Customer is provisioned in the European Union (EU). For EU Customers, transcript data processed by Azure is processed within region as part of Webex Data Residency.</p>	<p>Globally</p> <p>For EU Customers, within the EU</p>
	Audio Information (except if spoken language chosen is English, French, German, Italian, Spanish)	<p>When you add-on and use the real-time translation and transcription feature in multiple languages, Azure may process but not store Audio Information to provide speech-to-text services.</p>	Globally

		Audio data is processed by Azure at global endpoints, except when a Customer is provisioned in the EU. For EU Customers, audio data processed by Azure is processed within region as part of Webex Data Residency.	For EU Customers, with 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 Offer Disclosure. 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 Customer'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
<b>User Information</b>	<ul style="list-style-type: none"> <li>• Synched Corporate Directory information (e.g., name, email, title)</li> </ul> For users who pair with Cisco endpoint device: <ul style="list-style-type: none"> <li>• Unique User Identifier</li> <li>• First Name</li> <li>• Display name</li> </ul>	<ul style="list-style-type: none"> <li>• Provide Webex Assistant</li> <li>• Improve Webex Assistant's accuracy to user's command</li> </ul>
<b>Host and Usage Information</b>	<ul style="list-style-type: none"> <li>• Webex Assistant usage information (e.g., number of queries from endpoint devices, dates)</li> <li>• Endpoint devices used</li> </ul>	<ul style="list-style-type: none"> <li>• Diagnose technical issues</li> <li>• Improve the technical performance of Webex Assistant</li> <li>• Understand how Webex Assistant is used</li> </ul>
<b>User-Generated Information (Audio Information)</b>	<ul style="list-style-type: none"> <li>• User audio commands</li> </ul>	<ul style="list-style-type: none"> <li>• Provide Webex Assistant</li> </ul>
<b>User-Generated Information (Transcript Information)</b>	<ul style="list-style-type: none"> <li>• Text of commands</li> </ul>	<ul style="list-style-type: none"> <li>• Provide Webex Assistant</li> <li>• Train and/or improve Cisco language services</li> </ul>

### 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 Offer Disclosure will be updated to reflect those changes):

Data Center Locations
Germany
United States
Singapore

### 4. 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
------------------------	----------------	-----------------------

<b>User Information</b>	Cisco	Enable, support and improve Webex Assistant in accordance with Cisco's data access and security controls process.
<b>Host and Usage Information</b>	Cisco	Support and improve the Cisco Offer 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.
<b>User-Generated Information (Audio Information)</b>	Cisco	Provide Webex Assistant.
<b>User-Generated Information (Transcript Information)</b>	Cisco	Support, train and improve Webex Assistant. Understand how the product is being used.

## 5. Data Portability

While Webex Meetings allows Customers and users to export data as described in the Webex Meetings Offer Disclosure, it does not support the export of Webex Assistant for Devices data.

## 6. Data 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
<b>User Information</b>	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 Cisco Offer and will be deleted once it is no longer necessary to provide the Cisco Offer.
<b>Host and Usage Information</b>	Deleted within 2 years	Usage is retained to evaluate the service and understand how Webex Assistant is being used.
<b>User-Generated Information (Audio Information)</b>	Not retained	N/A
<b>User-Generated Information (Transcript Information)</b>	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.

## 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 Webex Assistant for Devices.

Personal Data Category	Security Controls and Measures
User Information	Encrypted in transit, encrypted at rest
Host and Usage Information	Encrypted in transit, encrypted at rest
User-Generated Information (Audio Information)	Encrypted in transit, encryption at rest is not applicable <sup>4</sup>
User-Generated Information (Transcript Information)	Encrypted in transit, encrypted at rest

## 8. 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 • Usage	Cloud storage region	United States
Splunk	• Transcript • Usage	Data analysis platform	United States

<sup>4</sup> The Webex platform and Google Cloud do not store audio; therefore, encryption at rest is not available for audio.



# Addendum Six:

## Cisco-Developed Embedded Apps (Optional)

This Addendum to the Webex Meetings Offer Disclosure 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 Offer Disclosure, 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 Webex Meetings; for that, please refer to the Webex Meetings Offer Disclosure above.

A Customer administrator controls whether user-level Personal Data can be shared with Shared Timer. In Webex Control Hub, the Customer administrator can 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 administrator). If the Customer administrator enables "PII Restrictions", 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 disabled, PII sharing mode is on, and the following applies:

Personal Data Category	Type of Personal Data	Purpose of Processing
<b>User Information</b>	<ul style="list-style-type: none"> <li>• UUID</li> <li>• Display Name</li> </ul>	<ul style="list-style-type: none"> <li>• UUID is used to identify which user within the meeting performed specific activities (e.g., who paused the timer)</li> <li>• Display Name is used to identify the user-specific activities (to display that a certain individual set or reset the timer)</li> </ul>
<b>Host and Usage Information*</b>	<ul style="list-style-type: none"> <li>• IP Address</li> <li>• User Agent</li> <li>• Browser</li> <li>• Operating System</li> <li>• Device Type</li> </ul>	<ul style="list-style-type: none"> <li>• Provide you with the Service</li> <li>• Diagnose technical issues</li> <li>• Respond to Customer support requests</li> <li>• Make improvements to the Service and other Cisco products and services</li> <li>• Understand how the Service is used</li> <li>• Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service</li> </ul>

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 enabled, PII sharing is off, and the following applies:

Personal Data Category	Type of Personal Data	Purpose of Processing
<b>User Level</b>	<ul style="list-style-type: none"> <li>• Personal Data that is collected (e.g., UUID and Display Name) is pseudonymized</li> </ul>	<ul style="list-style-type: none"> <li>• UUID used to identify which user within the meeting performed specific activities (e.g., who paused the timer);</li> <li>• Name is processed to identify the user-specific activities (to display that a certain individual set or reset the timer)</li> </ul>

<b>Host and Usage Information*</b>	<ul style="list-style-type: none"> <li>• IP Address</li> <li>• User Agent</li> <li>• Browser</li> <li>• Operating System</li> <li>• Device Type</li> </ul>	<ul style="list-style-type: none"> <li>• Provide you with the Service</li> <li>• Diagnose technical issues</li> <li>• Respond to Customer support requests</li> <li>• Make improvements to the Service and other Cisco products and services</li> <li>• Understand how the Service is used</li> <li>• Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service</li> </ul>
------------------------------------	--	---

### 3. Sub-processors

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

Sub-processor	Personal Data	Service Type	Location of Data Center
<b>Amazon Web Services</b>	<ul style="list-style-type: none"> <li>• UUID**</li> <li>• Display Name**</li> </ul>	<ul style="list-style-type: none"> <li>• Used to provide Shared Timer functionality</li> </ul>	<ul style="list-style-type: none"> <li>• United States</li> </ul>

\* 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.

# Addendum Seven: Webex LTI and Webex LTI Legacy (Optional)

## 1. Overview

Webex Meetings and Webex App and Messaging can be used with certain learning management systems (“LMSs”) that support the learning tools interoperability standard (“LTI”). Webex LTI and Webex LTI Legacy (collectively the “Service”) are cloud-based applications that utilize the LTI standard to integrate Webex Meetings and/or the Webex App and Messaging with LMSs. Webex LTI utilizes LTI 1.3 and LTI Advantage to integrate with LMSs. Webex LTI Legacy utilizes LTI 1.1 and certain LMS-specific APIs to integrate with LMSs. Previous installations of Webex Education Connector have been migrated to Webex LTI Legacy.

This Addendum to the Webex Meetings Offer Disclosure describes the processing of Personal Data (or personal identifiable information) by the Service when used together with Webex Meetings. If you use the Service together with Webex App and Messaging, see the Webex App Offer Disclosure (available on The Cisco Trust Center) for descriptions of the data that may be collected and processed in connection with those services.

## 2. Personal Data Processing

The table below lists the Personal Data processed by Webex LTI and Webex LTI Legacy to provide the Service and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
<b>User Information</b>	<ul style="list-style-type: none"><li>• Name</li><li>• Email Address</li><li>• Course Enrollment</li><li>• Course Role</li><li>• Browser</li><li>• Unique User ID (UUID)</li><li>• Webex Team and Space membership</li></ul>	<ul style="list-style-type: none"><li>• Provide you with the Service</li><li>• Enroll you in the Service</li><li>• Respond to Customer support requests</li><li>• Authenticate and authorize access to your account</li><li>• Display directory information to other Webex users</li><li>• Customer relationship management (e.g., transactional communication)</li></ul>

<b>Host and Usage Information</b>	<ul style="list-style-type: none"> <li>• IP Address</li> <li>• User Agent Identifier</li> <li>• Hardware Type</li> <li>• Operating System Type and Version</li> <li>• Client Version</li> <li>• Unique User ID (UUID)</li> <li>• IP Addresses Along the Network Path MAC Address of Your Client (as applicable)</li> <li>• Service Version</li> <li>• Actions Taken</li> <li>• Geographic Region (i.e., Country Code)</li> <li>• Meeting Session Information (e.g., date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity)</li> <li>• Number of Meetings</li> <li>• Number of Participants</li> <li>• Meeting Host Information</li> <li>• Host Name and Email Address</li> <li>• Meeting Site URL</li> <li>• Meeting Start/End Time</li> <li>• Meeting Title</li> <li>• Meeting Attendee Information, including Email Addresses</li> <li>• Information Submitted Through Attendee Registration Form (optional, only applicable if provided by you)</li> </ul>	<ul style="list-style-type: none"> <li>• Provide you with the Service</li> <li>• Diagnose technical issues</li> <li>• Respond to Customer support requests</li> <li>• Make improvements to the Service and other Cisco products and services</li> <li>• Understand how the Service is used</li> <li>• Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service</li> </ul>
-----------------------------------	--	---

### 3. 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. These technical and organizational measures include the following:

Personal Data Category	Security Controls and Measures
User Information	Encrypted in transit and at rest
Host and Usage Information	Encrypted in transit and at rest

## 4. Data Center Locations

Cisco uses third-party infrastructure providers to deliver the Service globally. Webex LTI and Webex LTI Legacy are hosted only in US data centers. The hosting of Webex LTI and Webex LTI Legacy is separate from the hosting of other Webex services.

Data Center Location
Virginia, USA

## 5. Sub-processors

Cisco partners with service providers that act as sub-processors of Personal Data and contract to provide the same level of data protection and information security provided to you by Cisco. The current list of sub-processors for Webex LTI and Webex LTI Legacy is set out below.

Sub-processor	Personal Data	Service Type	Location of Data Center
<b>AWS (Amazon Web Services) *</b>	<ul style="list-style-type: none"><li>• User Information</li><li>• Host &amp; Usage Information</li></ul>	<ul style="list-style-type: none"><li>• AWS cloud infrastructure is used to host Webex LTI and Webex LTI Legacy</li></ul>	Virginia, USA

\*Webex LTI and Webex LTI Legacy are hosted in their own AWS tenant in Virginia, USA, separate from infrastructure used by other Webex services.