



Offer Disclosure

Webex App and Messaging

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 App and Messaging (the "Cisco Offer" or "Webex" or the "Webex App") is a cloud-based service made available by Cisco to companies or persons (each as "Customer" or "you" or "your") who acquire it for use by their authorized users (each, a "user"). Webex provides a complete collaboration suite for your team to create, meet, message, make calls, and share, regardless of whether they are together or apart—in one continuous workstream before, during, and after meetings.

For more information about Webex App, visit

<https://www.cisco.com/c/en/us/solutions/collaboration/webex-call-message-meet.html>.

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 Personal Data processed by the Cisco Offer. The information described in the tables 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. This may include access to the keys used to encrypt or decrypt your User-Generated Information (including Webex-Generated Content).

If you are an individual subscribed to the Cisco Offer for personal use, your employer's policies will not apply to the data that you share while using the Cisco Offer. However, if you subscribed to the Cisco Offer using your employer-issued email address and your employer later purchases the Cisco Offer from Cisco, you will be required to update the email address associated with your account to a personal email address. Cisco recommends that you use your personal email address to access the Cisco Offer for personal use. If you want to change your email address, you can do so by following these [instructions](#).

Users can communicate with users from other companies through the Webex App. If you are a user posting into spaces created by or including users from other companies, those companies' policies related to retention, monitoring, deletion and export may govern that data (as described in the applicable sections of this Offer Disclosure).

This Offer Disclosure covers Webex App and Messaging. For more information regarding optional features for Webex App and Messaging, please see the Addendums below. When you launch a meeting in Webex, Webex Meetings functionality will be used. Accordingly, please see the Webex Meetings Offer Disclosure (available on [The Cisco Trust Center](#)) for a description of how recordings are collected and processed. If you use Webex Calling functionality through the Webex App, please see the Webex Calling Offer Disclosure (available on [The Cisco Trust Center](#)). Similarly, if you use functionality of the Slido service or the Vidcast service from within the Webex App, you can find the descriptions

of the Personal Data that may be processed in connection with those services in the applicable Offer Disclosure(s) (available on [The Cisco Trust Center](#)).

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

The Webex App 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 the content within your space(s) on Webex App, or
- process or use any Customer Content described in this Offer Disclosure to train any Webex App AI models without your authorization. To "train" in this context includes to evaluate, improve, fine-tune, or develop any Webex App AI models.

Data Retention. Webex allows for the persistent retention of messages and files shared by users. Accordingly, Customer's User-Generated Information is stored on the Webex platform while the Customer has an active subscription (subject to data storage limitations). For Customers that wish to minimize the amount of data stored on the platform or customize the retention period, Pro Pack for Webex Control Hub includes retention settings that automatically delete User-Generated Information or Webex-Generated Content in accordance with the enterprise Customer's corporate data retention and deletion policies.

After a Customer's subscription terminates or expires, its Personal Data is maintained as outlined in the tables below. If Cisco retains certain categories of data, the reasons why we retain it and the retention periods are described in the tables below.

In a group space, the retention policy of the organization that created the space controls, and its administrator can delete all of the information posted in the group space. In a one-on-one space, each organization's administrator can delete only those messages and files posted by its own users in accordance with its retention policy.

Table 1: Customer Content

Data Category	Data Elements (Examples)	Purposes	Retention Period	Reason for retention
User Information	Personal Data: - Activation Codes - Display Name - Email Address - Name - Profile Picture or Avatar image (optional, only applicable if provided by you) - Password - Company Name - Billing Contact Name - Organization ID - Universal Unique Identifier (UUID) - User information included in your organization directory - Pronouns (optional, only applicable if enabled by your organization and you) - User settings	- Provide you with the Cisco Offer - Enroll you in Webex - Display your Profile Picture and other optional identifiers to other users - Notify you about features and updates - Understand how the Cisco Offer is used - Manage customer account and services - Provide you remote access support - Authenticate and authorize access to your account	When you are an active customer: - As long as the Customer maintains an active subscription (paid or free). Upon termination/expiration: - Name and UUID are retained for 13 months from termination	- Name and UUID are maintained as part of Cisco's business records and to comply with Cisco's financial and audit requirements. - Account information provided to Cisco during the provisioning of the service is maintained for billing purposes.
User Information – Webex App Hub (APIs)	Personal Data: - Activation Codes - Display Name - Email Address - Name - Password - Company Name - Billing Contact Name - Organization ID - PIN - SIP Identifier - Phone Number - Directory Extension - Voicemail Box Number	- Authenticate and authorize access to Webex App Hub - Notify you of features and updates - Understand how the Cisco Offer is used - Provide you remote access support - If you choose to use Webex App Hub to add a third-party integration or bot to a space, the third party may share information and content associated with your third-party service or application account with us. We do not receive or store your passwords for these third-party services or applications, although we do store	When you are an active customer: As long as the Customer maintains an active subscription (paid or free). Upon termination/expiration: Name and UUID are retained for 13 months from termination	- Name and UUID are maintained as part of Cisco's business records and to comply with Cisco's financial and audit requirements. - Account information provided to Cisco during the provisioning of the service is maintained for billing purposes.

		authentication tokens associated with them.		
User-Generated Information	Personal Data: • Spaces Activity (date, time, person engaged and the activity) • Messages (content, sender, recipients, date, time, and read receipts) • Content Shared (files, file names, sizes and types and whiteboard content) • Meetings and Calls Information (title, invitation content, participants, link, date, time, duration and quality ratings) • Recordings • Transcriptions of Webex Meetings recordings (optional, only applicable if enabled by you) • Presence (user status) • Admin-generated information, e.g., Contact Service contact list • Voice (optional, only applicable if provided by user) • Calendar and Contact Information including information in the meeting invite like date, time, duration and meeting participants (optional, only applicable if you opt to integrate your calendar and/or contact information with the Service mobile application)	• Provide the Cisco Offer Message metadata (e.g., sender, date, frequency) may be used for: • Tagging, sorting and organization of your spaces, messages, and interactions with other users; and • Collaboration Insights feature (including Personal Insights) (optional) Calendar and Contact Information is used: • to make it easier for you to connect with your contacts through the Cisco Offer mobile application; and • to allow you to create a space from a calendar event using the Cisco Offer	When you are an active customer: • At Customer's discretion for up to 360 days (or up to 1095 days with the purchase of Pro Pack) • 6 months for free users • User-deleted recordings - 30 days post-deletion Upon termination/expiration: • Meeting Recordings and transcripts, which are on the Webex Meetings platform, retained for 60 days after service termination or account deactivation.	When you are an active customer: • Retained based on Customer's discretion (Customers controls retention settings). • User-deleted Messages and Meetings recordings are retained as described to allow users to retrieve messages and recordings inadvertently deleted, and for Customer compliance purposes. Upon termination/expiration: • Meeting recordings and transcripts are retained as described to allow users the opportunity to download them. <u>Note:</u> When you launch a meeting in Webex, Webex Meetings functionality is used.
Webex-Generated Content	Personal Data: • AI Assistant-Generated Content (optional, only applicable if the AI Assistant feature is enabled by you)	Provide the Cisco Offer	When you are an active customer: • At Customer's or user's discretion • AI Assistant-generated content retained for 7 days from generation	• Webex-Generated Content generally is not retained on the Webex platform when Customer or user deletes this data. • AI Assistant-generated content is retained to allow a Customer or user to download it.

Tabs Functionality Information (Customer may Opt-out)	Personal Data: • URL shortcuts (only if saved in Webex by user) • Browser cookies (maintained locally on user's device) • Activity logs (e.g., URL shortcut additions, use of feature)	• Provide the Cisco Offer • Understand how the Cisco Offer is used • Diagnose technical issues • Conduct analytics and statistical analysis for Customer to provide Customer administrators visibility into usage • Respond to Customer support requests	URLs saved as shortcuts within the Webex App embedded browser functionality will be retained until the user administrator deletes the shortcut or the Customer account is terminated	• URL shortcuts maintained to provide the Cisco Offer.
--	---	--	--	--

Table 2: Customer Systems Information

Data Category	Data Elements (Examples)	Purposes	Retention Period	Reason for retention
Host and Usage Information	Personal Data: • Device Name • Country Code • IP Address • User Agent Identifier • Operating System Type and Version • Client Version • IP Addresses Along the Network Path • MAC Address • Time Zone • Domain Name • Activity Logs • Hardware Type (if applicable)	• Understand how the Cisco Offer is used • Diagnose technical issues • Conduct analytics and statistical analysis for Customer to provide Customer administrators visibility into usage • Respond to Customer support requests	• 3 years	• Information generated by instrumentation and logging systems created through the use and Cisco Offer delivery are maintained as part of Cisco's business records. After the retention period, Usage Information used to conduct analytics and measure statistical performance is retained but pseudonymized, aggregated or anonymized.
Host and Usage Information – Webex App Hub (APIs)	Personal Data: • Device name • Geolocation • IP Address • Mobile Type • MAC Address • Time Zone • Universal Unique Identifier • Domain Name	We use Host and Usage Information to: • Provide the Cisco Offer • Diagnose technical issues • Conduct analytics and statistical analysis for Customer to provide Customer administrators visibility into usage • Respond to Customer support requests	• 3 years	• Information generated by instrumentation and logging systems created through the use and Cisco Offer delivery are maintained as part of Cisco's business records. After the retention period, Usage Information used to conduct analytics and measure statistical performance is retained but pseudonymized, aggregated or anonymized.

	• Activity Logs			
Configuration Data	Non-Personal Data: • User preferences • Device settings • Software configurations • Other customizable options	• Tailor the functionality of a system to specific requirements or preferences	When you are an active customer: • User information will be maintained as long as Customer maintains an active subscription (paid or free) Upon termination/expiration: • Deleted once the Cisco Offer is terminated • Name and UUID are maintained 7 years from termination	• Provide you with the Cisco Offer.
Events Data	Non-Personal Data: • Records or logs of specific occurrences, actions, or incidents (activity logs)	• Troubleshooting, auditing, monitoring, analysis, and reporting purposes to understand the behavior and performance of systems and applications	• 13 months	• Respond to customer support requests and diagnose technical issues. • Provide Customer administrators visibility into usage.
Telemetry Data	Non-Personal Data: • Status updates • Performance metrics	• Monitoring and analysis	• 13 months	• Respond to customer support requests and diagnose technical issues. • Provide Customer administrators visibility into usage.

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.

Cisco Webex Device Subscription. If a user administrator chooses to use the Cisco Webex Device Subscription to register a Cisco Webex device to the Cisco Webex cloud or to Cisco on-premises infrastructure, Cisco collects and processes the User Information listed in Table 1 and Host and Usage Information listed in Table 2 to deliver the device management service. This occurs regardless of whether such device uses any Webex services (i.e., this occurs even if such device is used solely with third-party services such as Microsoft Teams, Google Meet, or Zoom and not Webex).

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). For specific data center locations as related to Webex Meetings, Webex Calling, Slido or Vidcast, please refer to individual Offer Disclosures for these offers as available on [The Cisco Trust Center](#).

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. If you use Webex App bots, information shared with the bots may be processed or stored in the United States.

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.

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") and Customers in the US ("US Customers") for Personal Data processed by the Webex App and Messaging, including User Information, Host and Usage Information, User-Generated Information and AI Assistant-Generated Content (other than as noted below). EU Customers that became Webex App and Messaging Customers after July 2021, can choose to provision their data in the EU. For EU Customers who were provisioned before July 2021, Customer administrators will be offered the option to migrate their user Messaging data to the EU. 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 or www.cisco.com) or through any Cisco service to learn more about Cisco products or events; (b) a Customer provides ordering information (business contact information); (c) a user engages in collaboration with users outside of their region; (d) a user requests technical support, including through Cisco TAC (in which case the information that a user provides within the initial TAC request may be transferred outside the region); (e) a user enables certain optional functionalities; or (f) a user enables cell phone "push" notifications (in which case the cell phone provider associated with iOS or Android functionality may transfer data outside of the region).

For free user accounts, Personal Data defined in this Offer Disclosure may be stored in a Webex data center outside the account holder's region, including for EU 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: Subcontractors

Name	Service Type	Cisco Data Center Location
Amazon Web Services	AWS cloud infrastructure is used to host the Cisco Offer.	Germany Ohio, United States Oregon, United States Texas, United States
Microsoft	Microsoft is leveraged to provide certain AI features.	Australia Germany Ireland Netherlands California, United States Maryland, United States Oregon, United States
Snowflake	This service is used to produce customized reports when expressly requested by Customer.	Australia Ireland Germany Netherlands California, United States Maryland, United States Oregon, United States

Table 5: Subprocessors

Name	Personal Data	Service Type	Cisco Data Center Location
Amazon Web Services	Host and Usage Information, User-Generated Information	AWS cloud infrastructure is used to host the Cisco Offer.	Dallas, TX, USA Frankfurt, Germany Ohio, USA Portland, OR, USA United Arab Emirates
Microsoft	Enrollment information, Host and Usage Information, User-Generated Information, Webex-Generated Content	Microsoft is leveraged to provide certain AI features.	European Union (and Switzerland) United States Australia

Rackspace	Avatar image or Profile Picture	Cloud Infrastructure Use of avatar images or profile pictures is optional for Webex users. *Only applicable to data stored prior to October 2019.	Global; existing EU customer data is stored within the EU
Snowflake	Host and Usage Information (as requested by Customer)	This service is used to produce customized reports when expressly requested by Customer.	United States (AWS) Ireland (AWS) Frankfurt (AWS) Sydney (Australia) (AWS) Azure US -East Azure Europe West
Sparkpost Email Service	Name, Email address	Send communications to Customers.	Global

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.

Optional Third-Party Integrations

Webex integrations: Customers may incorporate third-party industry leading applications right into the Webex workflow. Such third-party applications have their own privacy policy applicable to the data shared by the Customer through the integration. To use such third-party applications, Customers must enable each integration. For more information, please visit the [Webex Integration Site](#). Unencrypted messages may be shared with third-party services and applications that you choose to integrate with the Cisco Offer, but not with any other third parties without your permission or unless required by law.

Device Push Notifications: Cisco may send user updates about the Webex App on iOS and Android devices by sending push notifications through Apple Push Notification service and Google Firebase Cloud Messaging respectively. Users may opt-out of receiving these notifications at any time by changing their device's notification settings.

GIPHY: Users can share animated GIFs by accessing GIPHY directly from the Webex App. While GIPHY appears within the user interface by default in latest versions of the Webex App, Customers may opt-out of the GIPHY feature at any time through the Control Hub portal. If GIPHY is available and users choose to utilize GIPHY's functionality to personalize their message, GIPHY may receive the user's IP address and GIF search terms. For more information, you may visit GIPHY's [terms of service](#) and [privacy policy](#).

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

Webex allows Customers to export up to 90 days of User-Generated Information (including Webex-Generated Content) using APIs provided with the Cisco Offer (except for Webex Meetings recordings, discussed below). Additionally, Customers that purchase Pro Pack for Webex Control Hub can use the APIs that come with that service to export User-Generated Information (including Webex-Generated Content) for any period that the Customer sets, in accordance with its corporate policies.

Customers with a free Webex account can request to export User-Generated Information (including Webex-Generated Content) by submitting a request using the [Privacy Request Form](#) or opening a TAC support request. The User-Generated Information and Webex-Generated Content posted by users who are using Cisco Webex purchased by their employer is treated as data of the employer (Cisco's Customer). Accordingly, the Customer's corporate policies will apply.

If users wish to export their User-Generated Information and Webex-Generated Content, the user must consult the Customer administrator or the person within their employer authorized to make determinations regarding the disposition of data belonging to the Customer. In a group space, the administrator of the organization that created the space can export all of the information posted in the group space; whereas the administrator of organizations that have participants in the space can export only those messages and files posted by their own users. In a one-on-one space, both organizations' administrators can export all of the information posted in the one-on-one space.

There are several ways Customers may export their Personal Data from the Webex platform. Customers may export limited categories of Personal Data via Webex Control Hub (as CSV exports) and all types of Personal Data (except authentication tokens) using APIs. When you launch a meeting in Webex, Webex Meetings functionality will be used. Webex Meetings allows Customers to export all Webex Meetings recordings stored on the Webex Meetings platform. A Customer's administrator may do so using APIs provided with the Webex Meetings service or through the Webex Meetings Site Admin Page, while individual users may do so through the Webex User Hub. Webex Meetings recordings are available in standard mp4 format.

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.

Webex is ISO/IEC 27001:2013 certified and in accordance with those standards adopts technical and organizational security measures to protect your Personal Data from unauthorized access use or

disclosure as required by law. Additional information about our encryption architecture is summarized in the table and paragraphs below.

Customers and Cisco can access Personal Data stored on the Webex platform as described in the table below. In a group space, the administrator of the organization that created the space can monitor all of the information posted in the group space; whereas the administrator of organizations that have participants in the space can monitor only those messages and files posted by their own users. In a one-on-one space, both organizations' administrators can monitor all of the information posted in the one-on-one space. Participants in group spaces and one-on-one spaces can access all of the information posted in the space. The table below lists the Personal Data used by Webex to carry out the service, who can access that data, and why.

Table 6: Access & Controls

Data Category	Who Has Access	Purpose of Access	Security Controls
User Information	Customer through Webex Control Hub	Process in accordance with Customer's Personal Data policy.	Encrypted in transit and at rest. Passwords are encrypted in transit and at rest.
	Cisco	Support the Cisco Offer in accordance with Cisco's data access and security controls process.	
Host and Usage Information	Customer through Webex Control Hub	Process in accordance with Customer's Personal Data policy.	Encrypted in transit and at rest.
	Cisco	Support and improvement of the Cisco Offer by the Webex Support and Development Team.	
User-Generated Information (excluding Recordings and Transcripts, discussed below)	Customer through Webex Control Hub	Process in accordance with Customer's Personal Data policy.	Encrypted end to end (except as explained below) with Cisco holding keys on Customer's behalf unless Customer purchases the Pro Pack for Webex Control Hub and deploys Hybrid Data Security, which allows Customer to hold keys.
	Cisco	While Cisco operates the Cisco Offer, Cisco does not access or monitor this data unless it is shared with Cisco by Customer and will only do so in accordance with Cisco's data access and security controls process. Additionally, if users invite Cisco into a user-hosted space, or join a Cisco-owned space, users should be aware that as part of Cisco's security process, Cisco may scan (but does not retain) uploaded files. Calendar and contact information is accessed only by the application locally on your mobile device and is not shared with Cisco unless and until:	

		• you interact with a contact from your mobile device contact list using the Cisco Offer, in which case we collect information only about that user. The Cisco Offer mobile application uses this information to make it easier for you to connect with your contacts. • you create a space from a calendar event using the Cisco Offer, in which case, we collect the information in the meeting invitation, including the date, time, duration and meeting participants.	
	Other Customers (when users share with other Customers) Bots (when users add them to their spaces and communicate with the bot directly)	To the extent users post User-Generated Information in spaces that include users from other companies, those users and their administrators may be able to access the data posted. Users can see the other participants (including bots) in a space, and any user in a non-moderated space and the moderator in a moderated space can remove another user or bot at any time.	
Recordings and Transcripts (if Webex Meetings functionality is used)	User through the Webex User Hub	Modify, control, and delete Webex Meetings recordings based on user's preferences.	When you launch a meeting in the Webex App, Webex Meetings functionality will be used. Recordings and transcripts created after May 2018 are encrypted in transit and at rest by default.
	Customer using APIs provided with the Cisco Offer or through the Site Admin Page	Modify, control, and delete in accordance with Customer's Personal Data policy.	
	Cisco	While Cisco operates the Cisco Offer, Cisco does not access or monitor this data unless it is shared with Cisco by Customer, and will only do so 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 Webex Meeting may be accessed by users in the meeting, wherever they are located. Even after you remove information from Webex Meetings, copies of that content may remain viewable elsewhere to the extent it has been shared with others.	
Webex-Generated Content	User 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.	
Tabs Functionality Information (Customer may opt out)	Cisco	If a Customer does not opt out, Cisco's access is limited to support and improve the Cisco Offer, in accordance with Cisco's data access and security controls process.	Encrypted in transit and at rest.

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

Webex encrypts user-content (messages, files, boards, calendar events) end-to-end between communicating parties. End-to-end keys are accessible to only those parties and processing endpoints authorized by the customer (e.g., transcoders, DLP engines, virus-scanners). Customers that require full control over their end-to-end encryption keys may also deploy a Hybrid Data Security (HDS) server within their datacenters. If you have opted to share your location information, that information is also encrypted. Messages remain encrypted until they are received by other users, where they are decrypted on those user's devices. The same process is used for each whiteboard stroke, whiteboard background images, and whiteboard snapshots (with one exception listed below under media encryption). The same process is also used for content that you share, except as noted below. Push notifications are likewise end-to-end encrypted.

There are a few circumstances under which User-Generated Information is decrypted:

- For certain types of files (PDFs, Microsoft Word documents, and PowerPoint presentations), we decrypt the file to be “transcoded” for display in a space. For example, if you upload a slide presentation into a space, it will first be encrypted on your device. When we receive the presentation on our server, we will decrypt it to generate an individual thumbnail images of each slide. We will then encrypt the thumbnails and presentation and send them to the other users in the space. The decrypted file and images are not stored; only the encrypted forms of these objects are stored.
- For bots and integrations that have not integrated with our end-to-end encryption scheme, we decrypt messages and content associated with the bot or integration before sending it to the third party supporting the bot or integration. We do not store the decrypted messages and content.

- Messages and content may be decrypted by your employer or the employers of those you communicate with using the Cisco Offer. If you communicate with Cisco employees, then those messages can be decrypted by Cisco.

Media encryption is used to protect the audio, video, screen sharing data, and voicemails that you transmit during a call. When you make a call, media is encrypted from your device to our servers. It may be decrypted on our servers so that we can manage the call. It is re-encrypted before being sent to the other participants on the call unless they are connected via the public telephone network or do not support encryption. If you dial into a meeting using SIP and there is whiteboarding taking place in the meeting, we will decrypt the end-to-end encrypted whiteboard content, transcode it, and send it to you using media encryption. We do not store any call audio, video, or screen sharing data on our servers. Voicemails are encrypted from your device to our servers, decrypted to be prepared for storage, and re-encrypted in storage on our servers. Voicemails transmitted via email are not encrypted. Therefore, Webex Control Hub provides the option to transmit voicemails via Webex instead of email. Faxes are not encrypted.

Transport encryption (also known as HTTPS) is used to protect all connections to and from the Cisco Offer other than voice and video calls. When you register for the Cisco Offer, send messages, share content, write on a whiteboard, connect with third-party services or applications via integrations, or screen shots to provide us with feedback, or otherwise connect to the Cisco Offer, we always use transport encryption.

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 [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
- HIPAA Attestation
- Spanish ENS (Esquema Nacional de Seguridad) Certification
- Australian IRAP (Information Security Registered Assessors Program) Certification

- Japanese ISMAP (Information System Security Management and Assessment) Certification
- 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 App and Messaging adhere 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:

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 describes the processing of Personal Data (or personal identifiable information) by the Service when used together with Webex App and Messaging. If you use the Service together with Webex Meetings, see the Webex Meetings 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
User Information	• Name • Email Address • Course Enrollment • Course Role • Browser • Unique User ID (UUID) • Webex Team and Space membership	• Provide you with the Service • Enroll you in the Service • Respond to Customer support requests • Authenticate and authorize access to your account • Display directory information to other Webex users • Customer relationship management (e.g., transactional communication)

Host and Usage Information	• IP Address • User Agent Identifier • Hardware Type • Operating System Type and Version • Client Version • Unique User ID (UUID) • IP Addresses Along the Network Path • MAC Address of Your Client (as applicable) • Service Version • Actions Taken • Geographic Region (i.e., Country Code) • Meeting Session Information (e.g., date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity) • Number of Meetings • Number of Participants • Meeting Host Information • Host Name and Email Address • Meeting Site URL • Meeting Start/End Time • Meeting Title • Meeting Attendee Information, including Email Addresses • Information Submitted Through Attendee Registration Form (optional, only applicable if provided by you)	• Provide you with the Service • Diagnose technical issues • Respond to Customer support requests • Make improvements to the Service and other Cisco products and services • Understand how the Service is used • Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service
-----------------------------------	---	---

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
AWS (Amazon Web Services) *	• User Information • Host & Usage Information	• AWS cloud infrastructure is used to host Webex LTI and Webex LTI Legacy	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.