Cisco Webex Meetings

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

1. Overview of Cisco Webex Meetings Capabilities

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

Because the Service enables collaboration among its users, as described below, your personal data is required in order to use the Service. The following paragraphs describe Cisco's processing of personal data in connection with the delivery of the Service, the location and transfers of that data, and how it is secured in accordance with privacy principles, laws, and regulations. Cisco will use your personal data consistent with this Privacy Data Sheet to serve the legitimate interests and fulfill the contractual obligations of providing the Solution. Note that this Privacy Data Sheet is a supplement to the Cisco Privacy Statement.

2. Personal Data Processing

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

Similarly, if users participate in meetings hosted by users in other companies, the meeting host will control any meeting recordings or files shared during the meeting, which will be subject to the host's corporate policies regarding access, use, monitoring, deletion, preservation, and export of information. The meeting host has the option to record meetings, which may be shared with others or discoverable in a legal matter. The meeting host should inform all meeting attendees prior to recording and Webex 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.

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

The table below list the categories of personal data used by the Service and describe why we process such data. Cisco Webex Meetings ***does not***:

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

Personal Data Category	Types of Personal Data	Purpose of Processing / Legitimate Interest
User Information	• Name • Email Address • Password • IP Address • Browser • Phone Number (Optional) • Mailing Address (Optional) • Geographic region • Avatar (Optional) • User information included in the Your Directory (if synched) • Unique User ID (UUID)	We use User Information to: • Provide you with the Service • Enroll you in the Service • Display your user avatar and profile to other users • Make improvements to the Service and other Cisco products and services • Provide you support • Customer relationship management (e.g., transactional communication) • Authenticate and authorize access to your account • Bill you for the Service • Display directory information to other Webex users (Avatar may be cached locally on devices of other Webex users that attend meetings with you for a period of 2 weeks) • Provide step-by-step guidance on how to use Webex online via WalkMe (optional)

Host and Usage Information	• IP Address
	• User Agent Identifier
	• Hardware Type
	• Operating System Type and Version
	• Client Version
	• IP Addresses Along the Network Path
	• MAC Address of Your Client (As
	• Applicable)
	• Service Version
	• Actions Taken
	• Geographic Region
	• Meeting Session Information (e.g., date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity)
	• Number of Meetings
	• Number of Screen-Sharing and NonScreen-Sharing Sessions
	• Number of Participants
	• Screen Resolution
	• Join Method
	• Performance, Troubleshooting, and Diagnostics Information
	• Meeting Host Information*
	  • Host Name and ID
	  • Meeting Site URL
	  • Meeting Start/End Time
	• Meeting Title
	• Call attendee information, including email addresses, IP address, username, phone numbers, room device information
	
	* Used for billing purpose
		We use Host and Usage Information to:
		• Provide you with the Service
		• Understand how the Service is used
		• Diagnose technical issues
		Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service
		• Respond to Customer support requests
		• Make improvements to the Service and other Cisco products and services
		
		If you use the Webex app, Cisco may use metadata from Webex meetings (e.g., meeting participants, frequencies) to help organize, sort, and/or prioritize your Webex app messages or spaces in a way that is relevant to you and your work.

User-Generated Information	• Meeting Recordings • Transcriptions of Call Recordings (optional, only applicable if enabled by you) • Uploaded Files (for Webex Events and Training only)	We use User-Generated Information to: • Provide the Service,

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

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

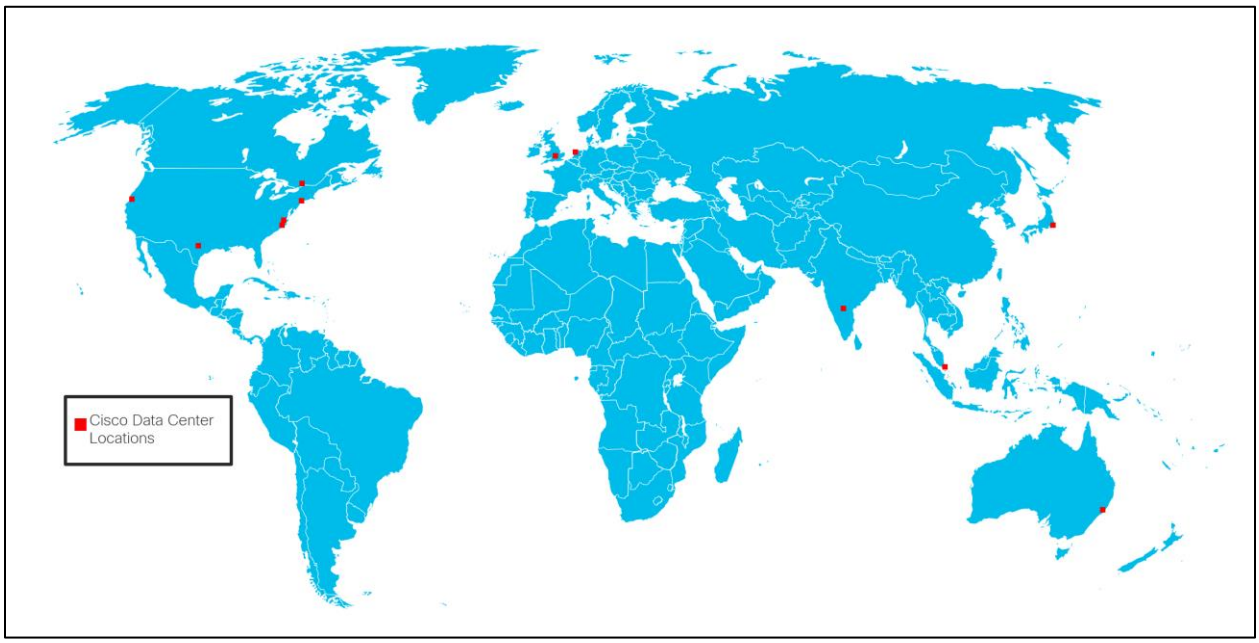
Control Hub
Cisco Webex Control Hub Analytics provides usage trends and valuable insights that can be used to help with strategies to promote and optimize adoption across teams. Cisco Webex Control Hub Analytics uses Host and Usage information to provide advanced analytics capabilities and reports.

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.

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

3. Cross-Border Transfers

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



Cisco Data Center Locations:	Internet Point of Presence (iPOP) Locations:
Amsterdam, Netherlands	Amsterdam, Netherlands
Bangalore, India	California, USA
California, USA	Hong Kong, China
London, UK	Illinois, USA
New York, USA	New Jersey, USA
North Carolina, USA	Sydney, Australia
Singapore, Singapore	Texas, USA
Sydney, Australia	
Texas, USA	
Tokyo, Japan	
Toronto, Canada	
Virginia, USA	

User-Generated Information is stored in the data center in Customer's region as provided during the ordering process. Data is replicated across data centers within the same region to ensure availability. Billing data is stored in the United States. Cisco Webex Analytics Platform data, which utilizes Host and Usage Information, is stored in the United States.

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

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 Meeting traffic through Cisco's infrastructure and improve performance. Data routed through iPOP Locations remains encrypted and is not stored in that location.

Please see the Webex Meetings Privacy Data Map for a visual representation of the data flows.

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

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

4. Access Control

Customers and Cisco can access personal data on the Service as described in the table below.

Personal Data Category	Who has access	Purpose of the access
User Information	User through the My Webex Page	Modify, control, and delete User Information
	Customer through the Site Admin Page or Webex Control Hub	Modify, control, and delete in accordance with Customer's personal data policy
	Cisco	Support the Service in accordance with Cisco's data access and security controls process
Host and Usage Information	Host through the My Webex Page	View meeting session Information
	Customer may view this information through the Site Admin Page, Webex Control Hub, or may be otherwise provided by Cisco	View usage, meeting session and configuration information
	Cisco	Support and improvement of the Service by the Cisco Webex Meetings support and development team
User Generated Information	User through the My Webex Page	Modify, control, and delete based on user's preference
	Customer using APIs provided with the Service or through the Site Admin Page or Webex Control Hub	Modify, control, and delete in accordance with Customer's personal data policy
	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer, and will only access in accordance with Cisco's data access and security controls process.
	Other Customers and users (when shared during a meeting)	Content you choose to share during a meeting may be accessed by users in the meeting, wherever they are located. Even after you remove information from the Service, copies of that content may remain viewable elsewhere to the extent it has been shared with others.

5. Data Portability

The Service allows Customers and users to export all User-Generated Information. A Customer's administrator may do so using APIs provided with the Service (recordings only) or through the Site Admin Page; while individual users may do so through the My Webex Page. Meeting recordings are available in proprietary ARF and standard mp4 formats depending on the account type. Cisco offers a free ARF player to convert ARF files to 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.

6. Data Deletion & Retention

Subject to their employer's corporate retention policies, users with an active subscription can delete User-Generated Information from their account through the My Webex Page at any time during the term of their subscription. Enterprise Customers have the ability to set organization-wide retention periods for recordings using APIs. Cisco provides free account users up to 6 months of free storage.

The table below describes the retention period and the business reasons that Cisco retains the personal data. Users seeking deletion of personal data retained on their employer's Webex Meetings site must request deletion from their employer's site administrator.

Personal Data Category	Retention period	Reason and Criteria for Retention
User Information	Active Subscriptions: • User Information will be maintained as long as Customer maintains active subscription (paid or free). Terminated Service: • Deleted once the Service is terminated • Name and UUID are maintained 7 years from termination	Name and UUID are maintained 7 years from termination as part of Cisco's business records and are maintained to comply with Cisco's financial and audit requirements. Any billing information is also subject to this retention period.
User Generated Information	Active Subscriptions: • At Customer's or user's discretion Terminated Service: • Deleted within 60 days	User-Generated Information is not retained on the Webex Meetings platform when Customer or user deletes this data. User Generated Information is retained for 60 days after services are terminated to give Customers opportunity to download.
Host and Usage Information	3 years	Host and Usage is kept as part of Cisco's record of Service delivery. Host and Usage information used to conduct analytics and measure statistical performance is retained but pseudonymized. * Any billing information is retained for 7 years as part of Cisco's business records and are maintained to comply with Cisco's financial and audit requirements. Once the specified retention period has expired, data will be deleted or anonymized.

7. Personal Data Security

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

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

Protecting Data at Rest
The Service encrypts Passwords and User Generated Information, as described above, at rest. Any data not encrypted at rest is protected by highly-secure data center protection mechanisms and operational procedures. Webex Meetings data centers feature communication infrastructure with industry-leading performance, integration, flexibility, scalability, and availability.

Encryption at Run Time
All communications on the Webex Meetings platform occur over encrypted channels. Cisco Webex uses TLS 1.2 protocol with high strength cipher suites.

Encrypted media can be transported over UDP, TCP or TLS; User Datagram Protocol (UDP) is the preferred transport protocol for media. Media packets are encrypted using either AES 128 or AES 256 based ciphers. Webex Video devices and 3rd party video devices supporting media encryption with SRTP use AES-CM-128-HMAC-SHA1. The key exchange happens over a TLS-secured channel.

After a session is established, all media streams (audio, VOIP, video, screen share, and document share) are encrypted. The Service then re-encrypts the media stream before sending it to other users. Note that if a Customer allows attendees to join its meetings using third-party video end points, those attendees may be sending your meeting data unencrypted on the Internet. Media streams flowing from a user to Cisco Webex Meetings servers are decrypted after they cross the Cisco firewalls. This enables Cisco to provide network-based recording and SIP-based call support for video end points.

End-to-End Encryption (Optional)
For standard meetings, Webex media servers may need to decrypt media for PSTN, transcoding and recording. However, for businesses requiring a higher level of security, the Service also provides end-to-end encryption.

To achieve this, each participant's Cisco Webex client generates 2048-bit RSA public and private key pair and sends the public key to the host's client. The host's client encrypts the meeting key using the participant's public key and returns the encrypted meeting encryption key back to the participant's client. The client can then decrypt the meeting key using its RSA private key.

All meeting data (voice, video, chat etc.) generated by Cisco Webex clients is encrypted using the shared meeting encryption key. Using Webex End to End Encryption meeting data cannot be deciphered by Cisco Webex service. This end-to-end encryption option is available for Cisco Webex Meetings and Cisco Webex Support. Note that when end-to-end encryption is enabled, the following features are not supported:

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

8. Third Party Service Providers (Sub-processors)

We may share data with service providers, contractors or authorized third parties to assist in providing and improving the Service. We do not rent or sell your information. All sharing of information is carried out consistent with the Cisco Privacy Statement and we contract with third-party service providers that can provide the same level of data protection and information security that you can expect from Cisco. Below is a list of sub-processors for WebEx Meetings.

Sub-processor	Personal Data	Service Type	Location
Akamai	**IP address**	Akamai provides a platform from which Customer can download Webex clients	

Sub-processor	Personal Data	Service Type	Location
Amazon Web Services (AWS)	Limited Host & Usage Information	AWS cloud infrastructure is used to host the Webex signaling service that processes meeting participant UUIDs, meetings start and end times. Data will be deleted within 15 days of the meeting. (Location maps to Customer's Webex data center assignment) AWS cloud infrastructure is used to host Webex media nodes that may process real-time meeting data such as VoIP, video and high frame rate sharing data. This information is not retained in AWS once your meeting has ended.	United States Germany Netherlands United Kingdom Brazil Australia Japan Singapore
WalkMe* * Customers may turn this feature off at any time. Feature is currently enabled for non-enterprise Webex sites.	Unique User ID (UUID) and user region	Provides user with a step-by-step tour and guidance on how to use Webex Meetings online site.	Globally

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

9. Information Security Incident Management

Breach and Incident Notification Processes

Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The Cisco Security Center details the process for reporting security incidents.

The Cisco Notification Service allows Customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows Customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber's relationship with Cisco. If you have questions or concerns about any product or security notifications, contact your Cisco sales representative.

10. Certifications and Compliance with Privacy Laws

The Security & Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements, including the EU General Data Protection Regulation, California Consumer Privacy Act, Canada's Personal Information Protection and Electronic Documents Act and Personal Health Information Protection Act.

Cisco leverages the following privacy certifications to demonstrate alignment with global privacy frameworks and transfer mechanisms related to the lawful use of data across jurisdictions:

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

In addition to complying with our stringent internal standards, Cisco also continually maintains third-party validations to demonstrate our commitment to information security. The Service has received the following certifications:

- ISO 27001, 27017, 27018, 27701
- SOC 2 Type II Attestation, SOC 3, + C5
- FedRAMP

11. How to Exercise Your Data Subject Rights

You have the right to request access, rectification, suspension of processing, or deletion of your personal data processed by the Service.

We will ask you to confirm your identification (typically with the email address associated with your Cisco account) before responding to your request. If we cannot comply with your request, we will provide you with an explanation. Please note, if you are a user and your employer is the Customer/Controller, we may redirect you to your employer for a response. Requests can be made by the following means:

1) submitting a request using the Privacy Request Form
2) by postal mail:

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

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

12. General Information and GDPR FAQ

For more information related to technical and operational security features of the Service, please see the Webex Meetings Security White Paper and the Cisco Webex Trusted Platform site.

For more general information and FAQs related to Cisco's Security Compliance Program and Cisco's GDPR readiness please visit The Cisco Trust Center.

Addendum One: People Insights feature for Cisco Webex

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by the People Insights feature for Cisco Webex Meetings and Cisco Webex.

1. Overview of People Insights Capabilities

The People Insights feature ("People Insights" or the "Feature") provides Cisco Webex 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 doesn't look behind logins or paywalls, which means your profile won't 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.

Users at an enabled organization can opt-out of People Insights by suppressing their profile from other meeting participants' view. This is accomplished in two ways:

1. Entering a meeting and selecting the "Hide Profile" link,
2. Signing into people.webex.com and clicking on "Hide Profile"

If you join a meeting, or a teamspace, hosted by a Cisco Customer that has People Insights enabled on their site, 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 meeting 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 tables below list the personal data used by People Insights and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
Publicly Available Business and Professional Biographical Data	• Profile Photos • News • Tweets • Authored Works • Bios • Employment History • Education History • Web Links for a specific person	• To source the People Insights profile and to enable search within the feature.
Account & Usage Information	• User Level Account Details (including email, name, and web interactions and platform usage)	• To provide support and improvement of the Feature • Product analytics (e.g. frequency of profile edits, # of successful profile loads in a meeting, etc.)

Personal Data Category	Types of Personal Data	Purpose of Processing
Directory Data	• If the directory option is enabled by the site administrator, professional information including the following may be collected from the internal company directory (as selected by the administrator): • Title • Phone Number • Location • Organization • Department • Photo • Role • Reporting Structure	• To augment the user's People Insights profile by providing company specific context to meeting participants who belong to the same organization. This data will only be visible to participants within the user's organization.
User Generated Information	• Information that the user adds in their People Insights profile.	• Augment the user's own People Insights profile (visible to Insights users)

3. Cross-Border Transfers

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

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions, as fully described in the Cisco Webex Meetings Privacy Data Sheets.

4. Access Control

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

5. Data Portability

Individuals can receive a copy of their own People Insights profile, including their self-generated information, by contacting privacy@cisco.com

6. Data Deletion & Retention

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

7. Personal Data Security

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

8. Third Party Service Providers (Sub-processors)

Cisco partners with service providers who 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 People Insights is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	• Publicly Available Business & Professional Data • Host & Usage Information • Directory Data • User-Generated Information	Cloud Storage	United States
Amplitude	• Host & Usage Information	User Analytics	United States

Addendum Two: Facial Recognition feature for Cisco Webex Meetings (Optional)

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

1. Overview of Facial Recognition Capabilities

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 meeting participants (i.e., associate participant names with their positions in a Webex meeting 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 characterize 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 Facial Recognition feature, the service uses the camera of the user's device to take a profile picture. This picture is sent to the Webex cloud where the Feature algorithm generates a facial vector from the picture so that it can be used for matching as further described below. Both the picture and the facial vector are encrypted and stored securely. The picture may be used to generate a new facial vector in the event Cisco updates or modifies the 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 meeting, a second facial vector is generated, then matched in the Webex cloud against the stored facial vector. This second facial vector is not retained.

The tables below list the personal data used by the Feature and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
User Information	• Name (First, Last) • Email • User ID	• To display name of recognized user • Enroll you in the Feature and enable opt-in
Biometrics	• User facial image • Facial vector mapping	• To create facial vector mapping and provide the facial recognition feature • To generate a new facial vector in case of a modification or update to the Feature algorithm • To provide the Facial Recognition feature

Host & Usage Information	• Information regarding accuracy of product, including:
	  ○ Successful and unsuccessful facial vector matching
	  ○ User feedback
		• To provide support and product analytics

Location	• Meeting Room Proximity data	• Proximity data is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations
Calendar	• Meeting Room Calendar Information	• Calendar information is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations

3. Access Control

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

4. Data Portability

While Webex Meetings allows Customers and users to export data as described in Section 5 of the Webex Meetings Data Privacy Sheet, it does not support the automatic export of Facial Recognition data.

5. Data Deletion & Retention

Type of Personal Data	Retention Period	Reason and Criteria for Retention
User Information	User ID is maintained for all active Webex Meetings users. Once a user is deleted from a Customer's account, the User ID is also deleted from the Facial Recognition service. All other User Information is not stored or retained by the Facial Recognition service as this information is already stored by Webex Meetings.	UserID is used to track your enrollment in the Feature Names are displayed upon a match in the facial recognition feature.
Biometrics	Images: Users control their image retention. The image is retained as long as the feature is enabled and the user leaves the image associated with their profile. The image can be deleted at any time by user. Images for all users are deleted upon customer's discontinuation of the service.	The image is used to provide the Facial Recognition feature, update the facial vector in case of an update to the algorithm, and to troubleshoot issues when requested by a customer or user.

Type of Personal Data	Retention Period	Reason and Criteria for Retention
	Facial vectors are retained as long as the facial images, but are stored separately. Facial vectors are deleted upon discontinuation of the service.	The facial vectors are used to provide the facial recognition feature.
Host & Usage Information	2 Weeks	To provide support and product analytics
Location	2 days	Proximity data is used to improve facial recognition to assure images are assigned to the correct users in the correct locations.
Calendar	Facial Recognition does not store or retain this information separately than already maintained by Webex Meetings.	Calendar data is used to improve facial recognition to assure images are assigned to the correct users in the correct locations.

6. Personal Data Security

The table below summarizes encryption architecture of data stored specifically for the Facial Recognition feature.

Personal Data Category	Type of Encryption
User Information	Encrypted in transit, AES 256 for storage
Images	Encrypted in transit, AES 256 for storage
Biometrics	Encrypted in transit, AES 256 for storage
Host & Usage Information	Encrypted in transit, AES 256 for storage
Location	Encrypted in transit, AES 256 for storage

Addendum Three: Webex Assistant for Meetings (Optional)

This addendum to the Webex Meetings Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by the Webex Assistant for Meetings ("Webex Assistant" or "Assistant") feature for Cisco Webex Meetings.

1. Overview of Webex Assistant Capabilities

Webex Assistant for Meetings 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 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 Assistant can also show captions so that no one misses a word of what's being said. Additionally, a meeting host can record the meeting to get a post-meeting transcript.

Webex administrators can provision Webex Assistant for Meetings for an organization, an entire Webex site, or for specific users through license assignment. A Customer's administrator can enable and disable Webex Assistant at any time. The administrator may also set the Assistant default to be either ON or OFF at meeting start times. If the Assistant is set to default ON by an administrator, the Assistant will be on when the meeting begins but can be disabled. If Assistant setting is set to OFF, the meeting host will have to explicitly turn on the Assistant in the meeting in order to use it.

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 meeting is recorded. Additionally, when the host turns on Webex Assistant in a meeting, there will be an audio announcement made to all participants on the call, even if they join late. As further described below, the host can choose to share the transcript and meeting highlights with other Webex Meeting users.

2. Personal Data Processing

The tables below list the personal data used by the Feature and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
User Information	• Name (First, Last) • Email • Username • Unique User Identifier (UUID)	• Provision Webex Assistant licenses to specific Webex Meeting users or to an entire organization or site • Provide the Webex Assistant service
Audio Information	• Meetings Recordings • Audio Commands to Webex Assistant • Audio associated with meeting Highlight	• Provide the Webex Assistant Service
Transcript Information	• Meeting Transcript • Text of meeting Highlight	• Provide the Webex Assistant service

Personal Data Category	Types of Personal Data	Purpose of Processing
Host and Usage Information	• Usage of the Webex Assistant features, including number of meetings with Assistant enabled, number/type of Highlight views/edits/downloads, troubleshooting events	• Provide the Webex Assistant service • Understand how the service is used • Provide Customer with usage information • Diagnose technical issues • Improve the technical performance of the service

3. Access Control

Personal Data Category	Who has access	Purpose of the access
User Information	Cisco	Enroll the to the Webex Assistant service.
	Customer	Provision Webex Assistant licenses to specific Webex Meeting users or to an entire organization or site
Audio Information	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer and will only access in accordance with Cisco's data access and security controls process.
	Customer	Customer will continue to have access to Meeting Recordings in accordance with Customer's personal data policy and as described in the Meetings Privacy Data Sheet.
	User	A meeting host will be able to view, access and/or delete Highlights. A host may share and give certain edit permissions to other Webex Meetings users.
Transcript Information	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer and will only access in accordance with Cisco's data access and security controls.
	User	A meeting host will be able to view, access and/or share Transcript Information. A host may share and give certain edit permissions to other Webex Meetings users.
Host and Usage Information	Cisco	Support and improve the Service in accordance with Cisco's data access and security controls.
	Customer	View and analyze usage information.

4. Cross Border Transfers

Cisco leverages its own data centers as well as third-party hosting providers and business partners to deliver the Service globally. Webex Assistant Audio and Transcript Information will be stored in the same location in which the Customer is provisioned for Webex Meeting recordings. Although Webex Assistant may process data in AWS as listed in Section 8 below, no data will be stored there.

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions, as fully described in the Cisco Webex Meetings privacy data sheet.

5. Data Portability

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

6. Data Deletion & Retention

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

Type of Personal Data	Retention Period	Reason and Criteria for Retention
User Information	User Information is not separately stored or retained by the Webex Assistant service as this information is already stored by Webex Meetings.	User Information is not separately stored or retained by the Webex Assistant service as this information is already stored by Webex Meetings.
Audio Information	Active Subscriptions: Audio Information deleted at Customer's or user's discretion. Terminated Service: Deleted within 60 days	Audio Information is retained in order to provide you with the service and will be deleted once it is no longer necessary to provide the service. Audio Information retained after services are terminated is done in order to make it available to Customers for download
Transcript Information	Active Subscriptions: Highlights may be deleted at Customer's or user's discretion. Terminated Service: Deleted within 60 days	Transcript Information is retained in order to provide you with the service and will be deleted once it is no longer necessary to provide the service. Transcript Information retained after services are terminated is done in order to make it available to Customers for download
Host and Usage	Deleted after 3 years.	Usage information used to conduct analytics and measure statistical performance is retained but pseudonymized.

7. Personal Data Security

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

Personal Data Category	Type of Encryption
User Information	Webex Assistant does not store or retain this information separately than already maintained by Webex Meetings.
Audio Information	Encrypted in transit, and at rest.
Transcript Information	Encrypted in transit, and at rest.
Host and Usage	Encrypted in transit, and at rest.

8. Third Party Service Providers (Sub-processors)

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

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	Audio Information	Cloud Infrastructure (transient storage only)	US, Germany, Singapore
Google Cloud	Audio and transcript of Voice Command *only* (e.g., "Ok, Webex, ***create a note***"). Please note that the core transcription technology that processes and stores all other Audio and Transcript Information is owned, managed and executed by Cisco.	• Speech to Text service (voice commands only) • Text to Speech service (voice command responses only)	US, Germany, Singapore

Addendum Four: Webex Assistant for Rooms

This addendum to the Webex Meetings Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by the Webex Assistant for Rooms feature for Cisco Webex Rooms.

1. Overview of Webex Assistant Capabilities

Webex Assistant for Rooms 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 is disabled by default and can be enabled by the Organization's administrator in Webex Control Hub.

Webex Assistant 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 Rooms 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 tables below list the personal data used by Webex Assistant for Rooms and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing

User Information	• Synched Corporate Directory information (e.g., name, email, title)
	• For users who pair with Cisco endpoint device:
	  ○ Unique User Identifier
	  ○ First Name
	  ○ Display name
		• Provide the Webex Assistant service
		• Improve Webex Assistant's accuracy to user's command

Audio	• User audio commands	• Provide the Webex Assistant service
Transcripts	• Text of command	• Provide the Webex Assistant service • Train and/or improve Cisco language services
Usage	• Webex Assistant usage information (e.g., number of queries from endpoint devices, dates) • Endpoint devices used	• Understand how the service is used • Diagnose technical issues • Improve the technical performance of the Webex Assistant service

3. Access Control

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

4. Cross Border Transfers

Cisco leverages its own data centers as well as third-party hosting providers and business partners to deliver the Service globally. These entities are currently located in the following locations (data center locations may change from time to time and this Privacy Data Sheet will be updated to reflect those changes):

Data Center Locations
Germany
United States

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions, as fully described in the Cisco Webex Meetings Privacy Data Sheet.

5. Data Portability

While Webex Meetings allows Customers and users to export data as described in Section 5 of the Webex Meetings Data Privacy Sheet, it does not support the export of Webex Assistant for Rooms data.

6. Data Deletion & Retention

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

Type of Personal Data	Retention Period	Reason and Criteria for Retention
Usage	Deleted within 1 year	Usage is retained to evaluate the service and understand how the product is being used.

7. Personal Data Security

The table below summarizes encryption architecture of data stored specifically for the Facial Recognition feature.

Personal Data Category	Type of Encryption
User Information	Encrypted in transit, encrypted at rest
Audio	Encrypted in transit, no storage at rest
Transcript	Encrypted in transit, encrypted at rest
Usage	Encrypted in transit, encrypted at rest

8. Third Party Service Providers (Sub-processors)

Cisco partners with service providers who 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
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