

# 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 the People Insights and Facial Recognition 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” for user generated content (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 visible 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 Cisco Webex Teams, see the Cisco Webex Teams 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.

Personal data processing by the Service does not produce decisions that would result in legal or other significant effects impacting the rights of data subjects based solely by automated means.

| Personal Data Category     | Types of Personal Data   | Purpose of Processing / Legitimate Interest   |
|----------------------------|--|---|
| Registration Information   | <ul style="list-style-type: none"> <li>Name</li> <li>Email Address</li> <li>Password</li> <li>Public IP Address</li> <li>Browser</li> <li>Phone Number (Optional)</li> <li>Mailing Address (Optional)</li> <li>Geographic region</li> <li>Avatar (Optional)</li> <li>Billing Information</li> <li>User information included in the Customer's Active Directory (if synced)</li> <li>Unique User ID (UUID)</li> </ul>   | <p>We use Registration Information to:</p> <ul style="list-style-type: none"> <li>Provide you with the Service</li> <li>Enroll you in the Service</li> <li>Display your user avatar identity to other users</li> <li>Make improvements to the Service and other Cisco products and services</li> <li>Provide you support</li> <li>Notify you about features and updates</li> <li>Send customer assigned admins marketing communications</li> <li>Authenticate and authorize access to your account</li> <li>Bill you for the Service</li> <li>Display directory information to other Webex users</li> <li>Provide step-by-step guidance on how to use Webex online via WalkMe (optional)</li> </ul> |
| Host and Usage Information | <ul style="list-style-type: none"> <li>IP Address</li> <li>User Agent Identifier</li> <li>Hardware Type</li> <li>Operating System Type and Version</li> <li>Client Version</li> <li>IP Addresses Along the Network Path</li> <li>MAC Address of Your Client (As Applicable)</li> <li>Service Version</li> <li>Actions Taken</li> <li>Geographic Region</li> <li>Meeting Session Information (title, date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity)</li> <li>Number of Meetings</li> <li>Number of Screen-Sharing and NonScreen-Sharing Sessions</li> <li>Number of Participants</li> <li>Meeting Host Information* <ul style="list-style-type: none"> <li>Host Name</li> <li>Meeting Site URL</li> <li>Meeting Start/End Time</li> </ul> </li> <li>Subscription Type</li> <li>Meeting Attendee Information* <ul style="list-style-type: none"> <li>Username of attendees</li> <li>Meeting Start/End time</li> <li>Subscription Info</li> </ul> </li> <li>Screen Resolution</li> <li>Join Method</li> <li>Performance, Troubleshooting, and Diagnostics Information</li> <li>Call attendee information, including email addresses, IP address, username, phone numbers, room device information</li> </ul> <p>* Used for billing purpose</p> | <p>We use Host and Usage Information to:</p> <ul style="list-style-type: none"> <li>Provide you with the Service</li> <li>Understand how the Service is used</li> <li>Diagnose technical issues</li> <li>Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service</li> <li>Respond to Customer support requests</li> <li>Bill you for the Service</li> </ul>  |
| User-Generated Information | <ul style="list-style-type: none"> <li>Meeting and Call Recordings</li> <li>Transcriptions of Call Recordings</li> <li>Uploaded Files (for Webex Events and Training only)</li> </ul>  | <p>We use User-Generated Information to:</p> <ul style="list-style-type: none"> <li>Provide the Service, optional components which include recording meetings</li> </ul>  |

**Technical Support Assistance**

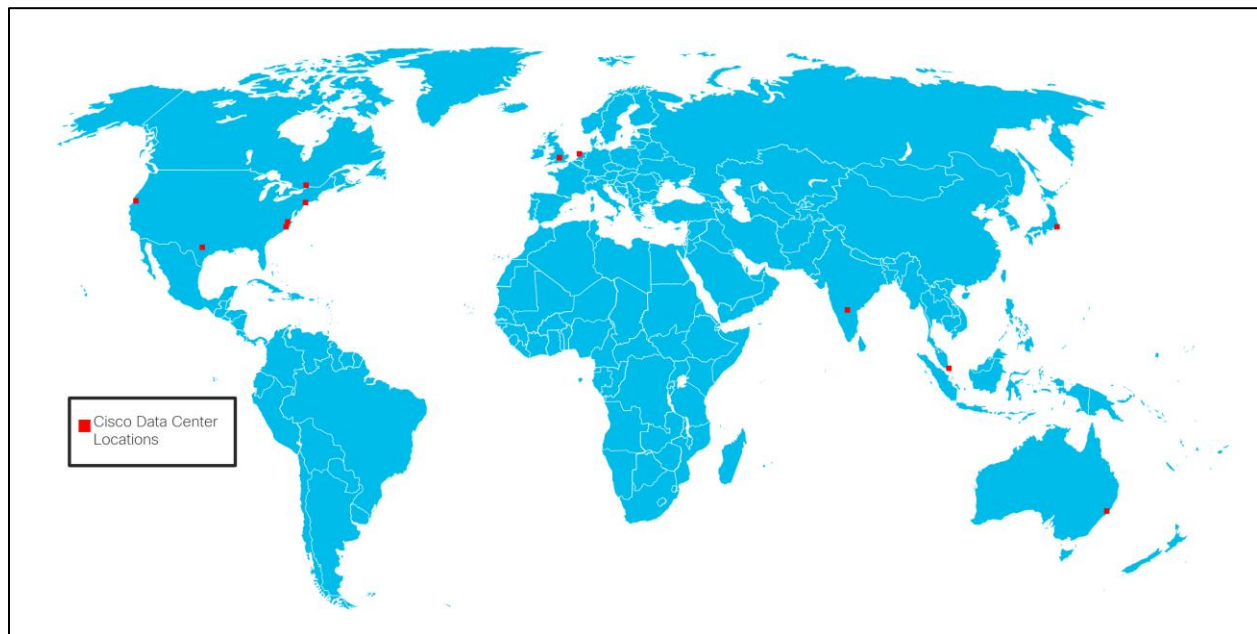
If a Customer reaches out to Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from the Service. [The Cisco TAC Service Delivery Privacy Data Sheet](#) describes Cisco's processing of such data.

**Webex Analytics Platform**

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. The Webex Analytics Platform utilizes Registration, Host and Usage information to provide advanced analytics capabilities and reports.

### 3. Cross-Border Transfers

The Service leverages its own data centers to deliver the Service globally. If you join a meeting using Cisco Webex Teams, please see the Cisco Webex Teams 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 closest to a Customer's location or as provided during the ordering process. Billing data is stored in Texas, USA and North Carolina, USA. Webex Analytics data is stored in California, USA and Texas, USA.

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) 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 these internet point of presence points remains encrypted and is not stored.

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-US Privacy Shield Framework](#)
- [Swiss-US Privacy Shield Framework](#)
- [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   |
|----------------------------|--|---|
| Registration Information   | User through the My Webex Page   | Modify, control, and delete 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.

Customers can request deletion of other personal data retained on the Webex Meetings platform by sending a request to Cisco (see contact options in Section 11 below) or opening a TAC service request, and unless the personal data is required to be retained for Cisco's legitimate business purposes or other legal requirement, Cisco endeavors to delete the requested data from its systems within 30 days. The table below describes the retention period and the business reasons that Cisco retains the personal data. Users seeking deletion of other personal data retained on the Webex Meetings platform must request deletion from their employer's site administrator.

| Personal Data Category     | Retention period  | Reason and Criteria for Retention   |
|----------------------------|---|---|
| Registration Information   | 7 years from when the Service is terminated   | Data collected as part of registration, including information provided by Customers as part of Cisco's financial due diligence, constitute Cisco business records and are kept to comply with Cisco financial and audit policies, as well as tax requirements.                          |
| User Generated Information | Active Subscriptions:<br><ul style="list-style-type: none"> <li>At Customer's or user's discretion</li> </ul> Terminated Service:<br><ul style="list-style-type: none"> <li>Deleted within 60 days</li> </ul> | User-Generated Information is not retained on the Webex Meetings platform when Customer or user deletes this data.  |
| Host and Usage Information | 7 years from when the Service is terminated   | Information generated by instrumentation and logging systems created through the use and operation of the Service is kept as part of Cisco's record of Service delivery. Usage information used to conduct analytics and measure statistical performance is retained but pseudonymized. |

## 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   |
|---|--|
| Registration Information (excluding Passwords, discussed below) | Encrypted in transit, but not at rest  |
| Passwords   | 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 sensitive data 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. 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 businesses requiring a higher level of security, the Service also provides end-to-end encryption. With this option, the Service does not decrypt the media streams. In this model, traffic cannot be deciphered by the Cisco Webex Meetings server. The end-to-end encryption option is available for Webex Meetings and Webex Support. Note that when end-to-end encryption is enabled, the following features are not supported:

- Network-based recordings
- Join Before Host
- Cisco Webex Video Platform (formerly known as Collaboration Meeting Rooms Cloud)

## 8. Third Party Service Providers (Sub-processors)

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

| Sub-processor   | Personal Data   | Service Type  | Location   |
|---|---|---|--|
| <b>Amazon Web Services (AWS)</b>  | Limited Host & Usage Information, meeting media traffic | <p>AWS cloud infrastructure is used to host the Webex signaling service that processes real-time meeting lifecycle information such as meeting participant UUIDs, meetings start and end times. Data will be deleted within 15 days of the meeting. (location maps to Customer's Webex data center assignment)</p> <p>AWS cloud infrastructure is used to host Webex media nodes that may process real-time meeting data such as VoIP, video and high frame rate sharing data. This information is not retained in AWS once your meeting has ended.</p> | United States<br>Germany<br>Netherlands<br>United Kingdom<br>Brazil<br>Australia<br>Japan<br>Singapore |
| <b>WalkMe*</b><br><br>*Feature will be enabled for Enterprise sites in June 2020, 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-US Privacy Shield Framework](#)
- [Swiss-US Privacy Shield Framework](#)
- [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, and 27018
- 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) sending an email to [privacy@cisco.com](mailto:privacy@cisco.com)
- 2) by postal mail:

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

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 (Optional)

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 Teams.

## 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.

Only the Customer’s site administrator has the ability to enable the Feature for their organization and users. Individual users cannot opt-in to use People Insights independently of their site administrator. 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”

## 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   |
|---|--|---|
| <b>Publicly Available Business and Professional Biographical Data</b> | <ul style="list-style-type: none"> <li>Profile Photos</li> <li>News</li> <li>Tweets</li> <li>Authored Works</li> <li>Bios</li> <li>Employment History</li> <li>Education History</li> <li>Web Links for a specific person</li> </ul>   | <ul style="list-style-type: none"> <li>To source the People Insights profile and to enable search within the feature.</li> </ul>  |
| <b>Account &amp; Usage Information</b>                                | <ul style="list-style-type: none"> <li>User Level Account Details (including email, name, and web interactions and platform usage)</li> </ul>  | <ul style="list-style-type: none"> <li>To provide support and improvement of the Feature</li> <li>Product analytics (e.g. frequency of profile edits, # of successful profile loads in a meeting, etc.)</li> </ul>  |
| <b>Directory Data</b>   | <ul style="list-style-type: none"> <li>If the Active 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 site administrator):               <ul style="list-style-type: none"> <li>Title</li> <li>Phone Number</li> <li>Location</li> <li>Organization</li> <li>Department</li> <li>Photo</li> <li>Role</li> <li>Reporting Structure</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>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.</li> </ul> |

| Personal Data Category     | Types of Personal Data   | Purpose of Processing  |
|----------------------------|--|--|
| User Generated Information | <ul style="list-style-type: none"> <li>Information that the user adds in their People Insights profile.</li> </ul> | <ul style="list-style-type: none"> <li>Augment the user's own People Insights profile (visible to Insights users)</li> </ul> |

### 3. Cross-Border Transfers

People Insights data is stored on third party servers provided by Amazon Web Services ("AWS") and Algolia. AWS servers are located in Oregon, Ohio and Virginia. Algolia servers are located in California.

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 or Teams Privacy Data Sheets.

### 4. Access Control

| Personal Data Category   | Who has access   | Purpose of the access  |
|--|--|--|
| Publicly Available Business and Professional Biographical Data | Customer<br>Cisco<br>People Insight users within the Customer's organization | To provide the Feature   |
| Account Information  | Cisco  | Registration Support<br>Correlate users with correct profiles<br>Analytics to improve service                          |
|  | Customer   | Feature enablement/disablement.  |
| Customer Directory Data  | Customer (Admin)<br>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](mailto:privacy@cisco.com)

## 6. Data Deletion & Retention

| Type of Personal Data                                      | Retention Period   | Criteria for retention   |
|--|--|--|
| <b>Publicly Available Business &amp; Professional Data</b> | <p>Obtained from public websites: Indefinite</p> <p>Obtained through third-party APIs: In accordance with contractual requirements</p> | <p>Publicly Available Business &amp; 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.</p> <p>As publicly available data originates from outside of Cisco WebEx, any permanent changes or deletions must be addressed and requested with the primary source.</p> <p>At the request of users, the data can be archived 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.</p> |
| <b>Account Information</b>                                 | <p>Active Subscriptions: At Customer's or user's discretion</p> <p>Deactivated Accounts: Deleted within thirty (30) days</p>           | Users can request to remove their Account Information by opening a TAC service request. Cisco will respond to such requests within 30 days.  |
| <b>Directory Data</b>                                      | <p>Active Subscriptions: At Customer's or user's discretion</p> <p>Deactivated Accounts: Deleted within thirty (30) days</p>           | 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.   |
| <b>User-Generated Information</b>                          | <p>Active Subscriptions: At Customer's or user's discretion</p> <p>Deactivated Accounts: Deleted within thirty (30) days</p>           | Users can delete User-Generated Information from their profile at any time.  |

## 7. Personal Data Security

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

## 8. 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    |
|----------------------------|---|------------------|----------------------------|
| <b>Amazon Web Services</b> | <ul style="list-style-type: none"> <li>Publicly Available Business &amp; Professional Data</li> <li>Host &amp; Usage Information</li> <li>Directory Data</li> <li>User-Generated Information</li> </ul> | Cloud Storage    | Oregon<br>Ohio<br>Virginia |
| <b>Algolia</b>             | <ul style="list-style-type: none"> <li>Publicly Available Business and Professional Biographical Data</li> </ul>  | Full Text Search | California                 |
| <b>Amplitude</b>           | <ul style="list-style-type: none"> <li>Host &amp; Usage Information</li> </ul>  | User Analytics   | California                 |

# 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.

## 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 web page 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   |
|--------------------------|--|---|
| Registration             | <ul style="list-style-type: none"> <li>Name (First, Last)</li> <li>Email</li> <li>User ID</li> </ul>   | <ul style="list-style-type: none"> <li>To display name of recognized user</li> <li>Enroll you in the Feature and enable opt-in</li> </ul>   |
| Biometrics               | <ul style="list-style-type: none"> <li>User facial image</li> <li>Facial vector mapping</li> </ul>   | <ul style="list-style-type: none"> <li>To create facial vector mapping and provide the facial recognition feature</li> <li>To generate a new facial vector in case of a modification or update to the Feature algorithm</li> <li>To provide the Facial Recognition feature</li> </ul> |
| Host & Usage Information | <ul style="list-style-type: none"> <li>Information regarding accuracy of product, including:               <ul style="list-style-type: none"> <li>Successful and unsuccessful facial vector matching</li> <li>User feedback</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>To provide support and product analytics</li> </ul>  |
| Location                 | <ul style="list-style-type: none"> <li>Meeting Room Proximity data</li> </ul>  | <ul style="list-style-type: none"> <li>Proximity data is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations</li> </ul>   |

| Personal Data Category | Types of Personal Data  | Purpose of Processing   |
|------------------------|---|---|
| Calendar               | <ul style="list-style-type: none"> <li>Meeting Room Calendar Information</li> </ul> | <ul style="list-style-type: none"> <li>Calendar information is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations</li> </ul> |

### 3. Access Control

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

### 4. Data Portability

While Webex Meetings allows Customers and users to export data as described in 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  |
|-----------------------|---|--|
| Registration          | <p>User ID is maintained for all active Webex Meetings users. Once a user is deleted from a Customer's account, the User ID is also deleted from the Facial Recognition service.</p> <p>All other registration information is not stored or retained by the Facial Recognition service as this information is already stored by Webex Meetings.</p> | <p>UserID is used to track your enrollment in the Feature</p> <p>Names are displayed upon a match in the facial recognition feature.</p> |

| Type of Personal Data    | Retention Period  | Reason and Criteria for Retention   |
|--------------------------|---|---|
| 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. | 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. |
|                          | Images for all users are deleted upon customer's discontinuation of the service.  |   |
|                          | Facial vectors are retained as long as the facial images, but are stored separately.<br><br>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                        |
|--------------------------|---|
| Registration             | 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 |