Cisco Webex app & Webex Messaging

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

1. Overview of Cisco Webex Service Protection Capabilities

Cisco Webex app and messaging (the “Service” or “Webex”) is a cloud-based service made available by Cisco to companies or persons (“Customer,” “you,” or “your”) who acquire it for use by their authorized users (“user”). Cisco Webex provides a complete collaboration suite for your team to create, meet, message, make calls, and share, regardless of whether they are together or apart—in one continuous workstream before, during, and after meetings. For more information about the Service, please visit the Cisco Webex homepage.

Because the Service enables collaboration among users, you will be asked to provide your personal data in order to use it. The following sections 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. Note that this Privacy Data Sheet is a supplement to the Cisco Privacy Statement.

2. Personal Data Processing

If you are a user and your employer is the Customer that acquired the Service, your employer serves as the “data controller.” All of the information described in this Privacy Data Sheet is subject to your employer’s policies regarding retention, monitoring, deletion, and export of information associated with the Service. This may include access to the keys used to encrypt or decrypt your User-Generated Information.

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

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

This Privacy Data Sheet covers the Service and Technical Support Assistance included with the Service. When you launch a meeting in Cisco Webex, Cisco Webex Meetings functionality will be used. Accordingly, please see the Cisco Webex Meetings Privacy Data Sheet (available on The Cisco Trust Center) for a description of how recordings are collected and processed. The tables below list the categories of personal data processed by the Service and describe why we process such data.

Table 1 Cisco Webex

Personal Data Category	Types of Personal Data	Purpose of Processing
User Information	• Activation Codes • Display Name • Email Address • Name • Profile Picture • Password • Company Name • Billing Contact Name • Organization ID • Universal Unique Identifier (UUID)	We use User Information to: • Enroll you in Cisco Webex • Display your user avatar identity to other users • Notify you about features and updates • Understand how the Service is used • Manage customer account and services • Make improvements to the Service and other Cisco products and services • Provide you remote access support • Authenticate and authorize access to your account
Host and Usage Information	• Device Name • Geolocation • IP Address • User Agent Identifier • Operating System Type and Version • Client Version • IP Addresses Along the Network Path • MAC Address • Time Zone • Domain Name • Activity Logs	We use Host and Usage Information to: • 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
User-Generated Information	• Spaces Activity (date, time, person engaged and the activity) • Messages (content, sender, recipients, date, time, and read receipts) • Content Shared (files, file names, sizes and types) • Whiteboard Content • Meetings and Calls Information (title, invitation content, participants, link, date, time, duration and quality ratings)* • Recordings* • Presence (user status) ***** Cisco Webex Meetings functionality will be used when you launch a meeting in Cisco Webex.	We use User-Generated Information to: • Provide the Service Message metadata (e.g., sender, date, frequency) may be used for tagging, sorting and organization of your spaces, messages, and interactions with other users. • •
Information Collected Related to Optional Features	• Geographic Location • Information collected by cookies, local storage, and other browser storage technologies	• If you choose to enable optional location-sharing, we will collect your geographic location when you send a message or share content in a space. • When you use the Service in your web browser, we use cookies, local storage, and other browser storage technologies to ensure that you can stay logged into the Service until you choose to log out and to improve the performance of the Service. These technologies may store User Information, Host, and/or Usage Information. Cookies are always sent using transport encryption.

Calendar Information (Optional)	• Calendar and Contact Information on Your Mobile Device	If you choose to use the Service on your mobile device, upon sign-up you will have the option of sharing your calendar and/or contacts with the Service mobile application. This calendar and contact information is accessed only by the application locally on your mobile device and is not shared with Cisco unless and until: • you interact with a contact from your mobile device contact list using the Service, in which case we collect information only about that user. The Service mobile application uses this information to make it easier for you to connect with your contacts. • you create a space from a calendar event using the Service, in which case, we collect the information in the meeting invitation, including the date, time, duration and meeting participants
Tabs Functionality Information (Customer may Opt-out)	• Browser cookies (maintained locally on user's device) • URL shortcuts (only if saved in Team application by user) • Activity logs (e.g., URL shortcut additions, use of feature)	• Provide 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

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 and Webex Analytics Platform

Cisco Webex Control Hub 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 Host and Usage information to provide advanced analytics capabilities and reports.

Table 2 Cisco Webex Calling (formerly Cisco Spark Call)

Personal Data Category	Types of Personal Data	Purpose of Processing
User Information	• SIP Identifier • Phone Number • Directory Extension • Direct Line • Voicemail Box Number • Voicemail PIN • Device Activation Codes • Email Address • Name • Profile Picture • Password	We use User Information to: • Enroll you in Cisco Webex Calling (formerly Cisco Spark Call) • Display Caller ID • Notify you about features and updates • Understand how the Service is used • Send you Cisco marketing communications • Make improvements to the Service and other Cisco products and services • Enable Directory Services within your organization • Provide you remote access support • Authenticate and authorize access to your account • Route calls to your users and places • Allow internal and external dialing • Allow you to activate your IP Phones • Access your voicemail • Respond to Customer support requests
Host and Usage Information	• Device Name • Geolocation • IP Address • Mobile Type • MAC Address • Time Zone • Universal Unique Identifier • Domain Name • Activity Logs	We use Host and Usage Information to: • 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
User-Generated Information	• Recordings • Transcripts • Voicemail	We use User-Generated Information to: • Provide the Service, enabling collaboration among users in different locations • Provide customized music on hold • Provide voicemail and voicemail transcription services Note: We route audio and video call content and screen sharing content between call participants, but we do not retain or store the content.

Table 3 Cisco Webex App Hub (APIs)

Personal Data Category	Types of Personal Data	Purpose of Processing
User Information	• Activation Codes • Display Name • Email Address • Name • Password • Company Name • Billing Contact Name • Organization ID • PIN • SIP Identifier • Phone Number • Directory Extension • Voicemail Box Number	We use User Information to: • Authenticate and authorize access to Cisco Webex App Hub • Notify you of features and updates • Understand how the Service is used • Provide you remote access support • If you choose to use Cisco Webex App Hub to add a third-party integration or bot to a space, the third party may share information and content associated with your third-party service or application account with us. We do not receive or store your passwords for these third-party services or applications, although we do store authentication tokens associated with them.

Host and Usage Information	• Device name • Geolocation • IP Address • Mobile Type • MAC Address • Time Zone • Universal Unique Identifier • Domain Name • Activity Logs	We use Host and Usage Information to: • Provide the Service • Diagnose technical issues • Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service • Respond to Customer support requests

3. Cross-Border Transfers

Cisco leverages its own data centers as well as third-party cloud hosting providers to deliver the Service globally. These 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). Note, that the data centers listed below are those that may be used where the Service is used in conjunction with Meetings and/or Calling. For specific privacy data sheets for Webex Meetings or Webex Calling, please visit The Cisco Trust Center.

Cisco Data Center Locations	Cloud Infrastructure Provider Locations	Media Data Center Locations
Dallas, TX, USA	Dallas, TX, USA	Dallas, TX, USA
San Jose, CA, USA	Frankfurt, Germany	San Jose, CA, USA
Ashburn, VA, USA	Ohio, USA	Ashburn, VA, USA
Toronto, Canada	Portland, OR, USA	Amsterdam, Netherlands
Amsterdam, Netherlands		Frankfurt, Germany
Bangalore, India		London, UK
London, UK		Sao Paulo, Brazil
Singapore, Singapore		Singapore, Singapore
Tokyo, Japan		Sydney, Australia
Sydney, Australia		Tokyo, Japan
New York, USA		Portland, OR, USA
		San Francisco, CA, USA

Media Data Centers represent infrastructure where real-time media stream traffic may be processed but retained.

Webex specific data is stored as listed below:

Product	Processing	Storage
Cisco Webex	US locations + Worldwide Media Data Center locations Europe locations (if optional 'Data Locality' features are selected when Cisco Webex is initially provisioned).	Data Centers located in the US (For meeting recordings, reference the Cisco Webex Meetings Privacy Data Sheet.) Data Centers located in Europe (decision is based on country selected from a drop down during the provisioning of the organization). More information is here. For free user accounts, the data defined in this privacy data sheet may be stored in a Webex data center outside the account holder's region.
Cisco Webex Calling (formerly Spark Call)	US locations only	US locations only

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

4. Access Control

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

Personal Data Category	Who has access	Purpose of the access
User Information	Customer through the Webex Control Hub	Process 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	Customer through the Webex Control Hub	Process in accordance with Customer's personal data policy
	Cisco	Support and improvement of the Service by the Cisco Webex Support and Development Team
User-Generated Information (excluding Recordings, discussed below)	Customer through the Webex Control Hub	Process in accordance with Customer's personal data policy
	Cisco	While Cisco operates the Service, Cisco does not access or monitor this data unless it is shared with Cisco by Customer and will only do so in accordance with Cisco's data access and security controls process. Additionally, if users invite Cisco into a user-hosted space, or join a Cisco-owned space, users should be aware that as part of Cisco's security process, Cisco may scan (but does not retain) uploaded files.
	• Other Customers (when users share with other Customers) • Bots (when users add them to their spaces and communicate with the bot directly)	To the extent users post User-Generated Information in spaces that include users from other companies, those users and their administrators may be able to access the data posted. Users can see the other participants (including bots) in a space, and any user in a non-moderated space and the moderator in a moderated space can remove another user or bot at any time
Recordings	User through the My Webex Meetings Page	Modify, control, and delete meeting recordings based on user's preferences
	Customer using APIs provided with the Service or through the Site Admin Page	Modify, control, and delete in accordance with Customer's personal data policy
	Cisco	While Cisco operates the Service, Cisco does not access or monitor this data unless it is shared with Cisco by Customer, and will only do so in accordance with Cisco's data access and security controls process
	Other Customers and users (when shared during a meeting)	Content you choose to share during a meeting may be accessed by users in the meeting, wherever they are located. Even after you remove information from Webex Meetings, copies of that content may remain viewable elsewhere to the extent it has been shared with others.

5. Data Portability

Cisco Webex allows Customers to export up to 90 days of User-Generated Information using APIs provided with the Service (except for recordings, discussed below). Additionally, Customers that purchase Pro Pack for Cisco Webex Control Hub can use the APIs that come with that service to export User-Generated Information for any period that the Customer sets, in accordance with its corporate policies. Customers that have terminated the Service and users with a free Webex account can request to export User-Generated Information by submitting a request using the Privacy Request Form or opening a TAC support request. The User-Generated Information posted by users who are using Cisco Webex purchased by their employer is treated as data of the employer (Cisco's Customer). Accordingly, the Customer's corporate policies will apply. If users wish to export their User-Generated Information, the user must consult the Customer administrator or the person within their employer authorized to make determinations regarding the disposition of data belonging to the Customer. In a group space, the administrator of the organization that created the space can export all of the information posted in the group space; whereas the administrator of the organizations that have participants in the space can export only those messages and files posted by their own users. In a one-on-one space, both organizations' administrators can export all of the information posted in the one-on-one space.

There are several ways Customers may export their personal data from the Webex platform. Customers may export limited categories of personal data via the Webex Control Hub (as CSV exports) and all types of personal data (except authentication tokens) using APIs.

When you launch a meeting in Cisco Webex, Cisco Webex Meetings functionality will be used. Cisco Webex Meetings allows Customers to export all meeting recordings stored on the Webex Meetings platform. A Customer's administrator may do so using APIs provided with the Webex Meetings Service or through the Webex Meetings Site Admin Page; while individual users may do so through the My Webex Meetings Page. Meeting recordings are available in Webex Meetings proprietary ARF and standard mp4 formats depending on the account type. Cisco offers a free Webex Meetings ARF player to convert ARF files to mp4 format.

6. Data Deletion & Retention

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

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

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

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: • Customer has ability request deletion by opening a ticket with TAC. • Deleted once the Service is terminated • Name and UUID are maintained 7 years from termination*	* Name and UUID are archived for 7 years as part of Cisco's business records and are maintained to comply with Cisco's financial and audit requirements. Any billing account information provided to Cisco during the provisioning of the service is also subject to this retention period.
User-Generated Information (excluding Recordings and Voicemail for Cisco Webex Calling (formerly Cisco Spark Call), discussed below)	Active Subscriptions: • User-Generated Information will be maintained as long as Customer maintains active subscription. • If Customer purchases Pro Pack for Cisco Webex Control Hub, it can customize a specific retention period.	User-Generated Information is persistent because the Service was built to allow Customers to leverage this information to collaborate with other users over long periods of time.

	• Cisco provides free account users up to 6 months of free storage. User-Generated content will be deleted after 6 months. Terminated Service: User-Generated Information will be deleted once account is disactivated or terminated.	
Recordings	Active Subscriptions: • At Customer's or user's discretion on Webex Meetings Platform Terminated Service: • Deleted within 60 days on Webex Meetings Platform	When you launch a meeting in Cisco Webex, Cisco Webex Meetings functionality will be used. Meeting recordings are not retained on the Webex platform when Customer or user deletes this data.
Host and Usage Information	3 years from when the Service is terminated	Information generated by instrumentation and logging systems created through the use and Service delivery are maintained as part of Cisco's business records. After the retention period, Usage Information used to conduct analytics and measure statistical performance is retained but pseudonymized, aggregated or anonymized.
Tabs Functionality Information	URLs saved as shortcuts within the Webex app embedded browser functionality will be retained until the User deletes the shortcut or the Customer account is terminated.	URL shortcuts maintained to provide the Service.

7. Personal Data Security

Cisco Webex is ISO 27001:2013 certified and in accordance with those standards adopts technical and organizational security measures to protect your personal data from unauthorized access use or disclosure as required by law. Additional information about our encryption architecture is summarized in the table and paragraphs below.

Personal Data Category	Type of Encryption
User Information (excluding Passwords, discussed below)	Encrypted in transit, but not at rest
Passwords	Encrypted in transit and at rest
Host and Usage Information	Encrypted in transit, but not at rest
User-Generated Information (excluding Recordings, discussed below)	Encrypted end to end (except as explained below) with Cisco holding keys on Customer's behalf unless Customer purchases the Pro Pack for Cisco Webex Control Hub and deploys Hybrid Data Security, which allows Customer to hold keys
Recordings	When you launch a meeting in Cisco Webex, Cisco Webex Meetings functionality will be used. Beginning May 2018, Cisco released encryption of recordings at rest. Any new recordings created on your site after the enablement of this feature will be automatically encrypted end to end.
Tabs Functionality Information	Encrypted in transit and at rest

The Service uses different kinds of encryption to protect different kinds of data in transit and in storage. In this section, "you" and "your" refers to the user.

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

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

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

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

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

8. Third Party Integrations and Sub-processors

We may share personal data with service providers, contractors, or other third parties to assist in providing and improving the Service. The data shared may include aggregate statistics or individualized 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. **We do not rent or sell your information**. If a Customer purchases the Service through a Cisco partner, we may share any or all of the information described in this Data Sheet with the partner. Below is a current list of third-party service providers with access to personal data.

Sub-processor	Personal Data Handled	Description of Service Provided
Amplitude	Usage Information (Pseudonymous)	Analytics
Amazon Web Service	Host and Usage Information, User-Generated Information	AWS cloud infrastructure is used to host the Webex Service.
Rackspace	Avatar image	Cloud Infrastructure *Only applicable to data stored prior to October 2019.
Software AG (formerly called Built.io)	Bot Request Command (Pseudonymous)	Software AG provides cloud infrastructure used to build and host bots for use within Webex. Software AG utilizes UUID to fulfill a user bot request.

Sub-processor	Personal Data Handled	Description of Service Provided
Snowflake	Host and Usage Information (as requested by Customer)	This service is used to produce customized reports when expressly requested by Customer.
Sparkpost Email Service	Name, Email address	Send communications to Customers.
WalkMe	Unique User Identification (UUID)	Provides user with a step-by-step tour and guidance on how to use Webex.

Optional Third-Party Integrations

- **Cisco Webex integrations:** Customers may incorporate third-party industry leading applications right into the Webex workflow. Such third-party applications have their own privacy policy applicable to the data shared by the Customer through the integration. To use such third-party applications, Customers must enable each integration. For more information, please visit our Webex Integration Site. Unencrypted messages may be shared with third-party services and applications that you choose to integrate with the Service, but not with any other third parties without your permission or unless required by law.
- **Device Push Notifications:** Cisco may send user updates about the Webex Application on iOS and Android devices by sending push notifications through Apple Push Notification service and Google Firebase Cloud Messaging respectively. Users may opt-out of receiving these notifications at any time by changing their device's notification settings.
- **GIPHY**: Users can share animated GIFs by accessing GIPHY directly from the Webex app. Customers may opt-out of the GIPHY feature at any time through the Control Hub portal. If users choose to utilize GIPHY's functionality to personalize their message, GIPHY may receive the user's IP address and GIF search terms. For more information, you may visit GIPHY's terms of service and privacy policy.

9. Information Security Incident Management

Breach and Incident Notification Processes

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

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

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

10. Certifications and Compliance with Privacy Laws

The Security and 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 (GDPR), California Consumer Privacy Act (CCPA), Canada's

Personal Information Protection and Electronic Documents Act (PIPEDA), Personal Health Information Protection Act (PHIPA), Health Insurance Portability and Accountability (HIPPA), and Family Educational Rights and Privacy Act (FERPA).

Cisco leverages the following privacy transfer mechanisms related to the lawful use of data across jurisdictions:

- Binding Corporate Rules
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- EU Standard Contractual Clauses
- 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. Cisco Webex has received the following certifications:

- ISO 27001, 27017, 27018
- SOC 2 Type II Attestation
- SOC 3 Attestation
- Cloud Computing Compliance Controls Catalogue (C5)
- HITRUST

Customers can review the certifications at the Cisco Trust Center (some of which will require an NDA).

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"><b>Chief Privacy Officer</b>
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td></tr>
<tr><td><b>Americas Privacy Officer</b>
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td><td><b>APJC Privacy Officer</b>
Cisco Systems, Inc.
Bldg 80, Lvl 25, Mapletree Biz City,
80 Pasir Panjang Road,
Singapore, 117372
SINGAPORE</td><td><b>EMEAR Privacy Officer</b>
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 Autoritiet Persoonsgegevens.

12. General Information and Privacy Regulations FAQ

For more information and FAQs related to Cisco Webex technical and operational security features, please see the Cisco Webex Tech Ops and Security FAQs page and the Cisco Webex Security, Compliance, and Management page.

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