Webex App & Webex Messaging

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by the Webex App and Messaging (the "Service" or "Webex" or the "Webex App").

The Webex App is a cloud-based collaboration solution made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from the Webex App in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the customer relationship. Cisco is the Data Processor for the personal data processed by the Webex App to provide its functionality.

1. Overview

Webex App 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"). 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.

Because the Service enables collaboration among users, you will be asked to provide your personal data to use it.

For more information about Webex, visit the Webex homepage.

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 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 Webex, Webex Meetings functionality will be used. Accordingly, please see the Webex Meetings Privacy Data Sheet (available on The Cisco Trust Center) for a description of how recordings are collected and processed. If you use Webex Calling through the Webex App, please see the Webex Calling Privacy Data Sheet (here), which includes details related to personal data processing for Webex Calling.

If you use the Vidcast service from within the Webex App, see the Vidcast Privacy Data Sheet (available on The Cisco Trust Center) for descriptions of the data that may be collected and processed in connection with that service.

The table below lists the personal data processed by Webex to provide its services and describes why the data is processed.

The Webex App does not:

- Produce decisions that would result in legal or other significant effects impacting the rights of data subjects

based solely by automated means.
- Sell your personal data.
- Serve advertisements on our platform.
- Track your usage or content for advertising purposes.
- Monitor or interfere with the content within your space(s) on Webex App.

Table 1 Webex App

Personal Data Category	Type of Personal Data	Purpose of Processing
User Information	• Activation Codes • Display Name • Email Address • Name • Profile Picture or Avatar image (optional, only applicable if provided by you) • Password • Company Name • Billing Contact Name • Organization ID • Universal Unique Identifier (UUID) • User information included in your organization directory • Pronouns (optional, only applicable if enabled by your organization and you)	We use User Information to: • Provide you with the Service • Enroll you in Webex • Display your Profile Picture and other optional identifiers to other users • Notify you about features and updates • Understand how the Service is used • Manage customer account and services • Provide you remote access support • Authenticate and authorize access to your account
Host and Usage Information	• Device Name • Country Code • IP Address • User Agent Identifier • Operating System Type and Version • Client Version • IP Addresses Along the Network Path • MAC Address • Time Zone • Domain Name • Activity Logs • Hardware Type (if applicable)	We use Host and Usage Information to: • Understand how the Service is used • Diagnose technical issues • Conduct analytics and statistical analysis for Customer to provide Customer administrators visibility into usage • 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 and whiteboard content) • Meetings and Calls Information (title, invitation content, participants, link, date, time, duration and quality ratings)* • Recordings* • Transcriptions of Webex Meetings recordings (optional, only applicable if enabled by you) • Presence (user status) • Admin-generated information, e.g., Contact Service contact list • Voice (optional, only applicable if provided by user)	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; and • Collaboration Insights feature (including Personal Insights) (optional)

	* Webex Meetings functionality will be used when you launch a meeting in Webex.	
Information Collected Related to Optional Features	• Information collected by cookies, local storage, and other browser storage technologies	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 and Contact Information (Optional)	• Calendar and Contact Information	If a Customer admin or end user chooses to integrate calendar and contact information with their use the Service, 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 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 for Customer to provide Customer administrators visibility into usage • 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

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.

Cisco Webex Device Subscription

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

Table 2 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	We use User Information to: • Authenticate and authorize access to 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 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

	• SIP Identifier • Phone Number • Directory Extension • Voicemail Box Number	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 for Customer to provide Customer administrators visibility into usage • Respond to Customer support requests

3. Data Center Locations

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 Webex Meetings and/or Webex Calling. For specific privacy data sheets for Webex Meetings or Webex Calling, please visit The Cisco Trust Center.

Data Center Locations	Media Data Center Locations
Dallas, TX, USA	Dallas, TX, USA
San Jose, CA, USA	San Jose, CA, USA
Ashburn, VA, USA	Ashburn, VA, USA
Toronto, Canada	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
Frankfurt, Germany	San Francisco, CA, USA

Media Data Centers represent infrastructure where real-time media stream traffic may be processed but not retained. If you use Webex App bots, information shared with the bots may be processed or stored in the United States.

4. Webex Data Residency

Webex data residency provides Customer administrators the ability to choose where their organization's data is stored. Data residency is currently available for Customers in the European Union (EU) ("EU Customers") and Customers in the US ("US Customers") for personal data processed by the Webex App and Messaging, including User Information, Host and Usage Information, and User-Generated Information (other than as noted below). EU Customers that became Webex App and Messaging Customers after July 2021, can choose to provision their data in the EU. For EU Customers who were provisioned before July 2021, Customer administrators will be offered the option to migrate their user Messaging data to the EU. US Customers who are provisioned in the US by their Customer administrators will have their personal data processed and stored in the US.

To facilitate certain operations and aspects of the Service, certain exceptions to Webex data residency exist; specifically, cross-border transfers of personal data may still occur when (a) a user registers on any Cisco platform (for example, through www.webex.com or www.cisco.com) or through any Cisco service to learn more about Cisco products or events; (b) a Customer provides ordering information (business contact information); (c) a user engages in collaboration with users outside of their region; (d) a user requests technical support, including through Cisco TAC (in which case the information that a user provides within the initial TAC request may be transferred outside the region); (e) a user enables certain optional functionalities; or (f) a user enables cell phone "push" notifications (in which case the cell phone provider associated with iOS or Android functionality may transfer data outside of the region).

For free user accounts, the data defined in this Privacy Data Sheet may be stored in a Webex data center outside the account holder's region, including for EU Customers.

5. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses
- EU-U.S. Data Privacy Framework and the U.K. Extension to the EU-U.S. Data Privacy Framework
- Swiss-U.S. Data Privacy Framework

6. 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.

The table below lists the personal data used by Webex to carry out the service, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
User Information	Customer through 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 Webex Control Hub	Process in accordance with Customer's personal data policy.
	Cisco	Support and improvement of the Service by the Webex Support and Development Team.
User-Generated Information **(excluding Recordings & Transcripts, discussed below)**	Customer through 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)	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

	• Bots (when users add them to their spaces and communicate with the bot directly)	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 & Transcripts	User through the My Webex Meetings Page	Modify, control, and delete Webex Meetings 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 Webex Meeting may be accessed by users in the meeting, wherever they are located. Even after you remove information from Webex Meetings, copies of that content may remain viewable elsewhere to the extent it has been shared with others.
Information Collected Related to Optional Features	Cisco	While Cisco operates the Service, Cisco does not access or monitor this data unless it is shared with Cisco by Customer, and will do so to support and improve the Service, in accordance with Cisco's data access and security controls process.
Calendar and Contact Information (Optional)	User	End user may decide to share with Webex App calendar and contact information.
	Cisco	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)	Cisco	If a customer does not opt out, Cisco's access is limited to support and improve the Service, in accordance with Cisco's data access and security controls process.

7. Data Portability

Webex allows Customers to export up to 90 days of User-Generated Information using APIs provided with the Service (except for Webex Meetings recordings, discussed below). Additionally, Customers that purchase Pro Pack for Webex Control Hub can use the APIs that come with that service to export User-Generated Information 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 organizations that have participants in the space can export only those messages and files posted by their own users. In a one-on-one space, both organizations' administrators can export all of the information posted in the one-on-one space.

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

When you launch a meeting in Webex, Webex Meetings functionality will be used. Webex Meetings allows Customers to export all Webex Meetings recordings stored on the Webex Meetings platform. A Customer's administrator may do so using APIs provided with the Webex Meetings Service or through the Webex Meetings Site Admin Page; while individual users may do so through the My Webex Meetings Page. Webex Meetings recordings are available in standard mp4 format.

8. Data Retention

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

The table below lists the personal data used by Webex, the length of time that data needs to be retained, and why we retain it.

Type of Personal Data	Retention Period	Reason for Retention
User Information	Active Subscriptions: • User Information will be maintained as long as the Customer maintains an active subscription (paid or free). Terminated Service: • Customer has the ability to 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.
Host and Usage Information	3 years	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.
User-Generated Information **(excluding Recordings & Transcripts, discussed below)**	Active Subscriptions: • User-Generated Information will be maintained as long as the Customer maintains an active subscription. • If Customer purchases Pro Pack for Webex Control Hub, it can customize a specific retention period. For Customers who purchase Pro Pack and do not define a retention policy, the new	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.

	default retention period is 1095 days. • For enterprise Customers who do not purchase Pro Pack for Webex Control Hub, the default retention period is 360 days. • 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 deactivated or terminated.	
Recordings & Transcripts	Active Subscriptions: • At Customer's or user's discretion on Webex Meetings Platform • If Customer purchases Pro Pack for Webex Control Hub, it can customize a specific retention period. Terminated Service: • Deleted within 60 days on Webex Meetings Platform	When you launch a meeting in Webex, Webex Meetings functionality will be used. Webex Meetings recordings are not retained on the Webex platform when Customer or user deletes this data. Recordings are "soft deleted" and retained for 30 days before being removed from the platform, to allow a Customer or user to retrieve a recording they have inadvertently deleted.
Information Collected Related to Optional Features	3 years	If a Customer opts in to certain optional features, information collected related to those optional features is maintained as part of Cisco's business records.
Calendar and Contact Information (Optional)	Active Subscriptions: • Calendar Information will be maintained as long as the Customer maintains an active subscription. • If Customer purchases Pro Pack for Webex Control Hub, it can customize a specific retention period. Terminated Service: • Calendar Information will be deleted once account is deactivated or terminated.	Calendar Information is persistent because the optional functionality was built to allow Customers to leverage and access this information to collaborate with other users over long periods of time.
Tabs Functionality Information (Customer may opt out)	URLs saved as shortcuts within the Webex App embedded browser functionality will be retained until the user administrator deletes the shortcut or the Customer account is terminated.	URL shortcuts maintained to provide the Service.

9. Personal Data Security

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

Personal Data Category	Security Controls and Measures
User Information (excluding Passwords, discussed below)	Encrypted in transit and at rest
Passwords	Encrypted in transit and at rest
Host and Usage Information	Encrypted in transit and at rest
User-Generated Information (excluding Recordings & Transcripts, 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 Webex Control Hub and deploys Hybrid Data Security, which allows Customer to hold keys.
Recordings & Transcripts	When you launch a meeting in the Webex App, Webex Meetings functionality will be used. Recordings and transcripts created after May 2018 are encrypted in transit and at rest by default.
Information Collected Relating to Optional Features	Encrypted in transit and at rest
Calendar and Contact Information (Optional)	Encrypted in transit and at rest
Tabs Functionality Information (Customer may Opt-out)	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.

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, Webex Control Hub provides the option to transmit voicemails via Webex instead of email. Faxes are not encrypted.

Transport encryption (also known as HTTPS) is used to protect all connections to and from the 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.

10. 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 Privacy Data Sheet with the partner. Below is a current list of third-party service providers with access to personal data.

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	Host and Usage Information, User-Generated Information	AWS cloud infrastructure is used to host the Webex Service.	Dallas, TX, USA Frankfurt, Germany Ohio, USA Portland, OR, USA
Microsoft	User-Generated Information	Microsoft is leveraged to provide some of the Webex AI features	European Union United States
Rackspace	Avatar image or Profile Picture	Cloud Infrastructure Use of avatar images or profile pictures is optional for Webex users. *Only applicable to data stored prior to October 2019.	Global; existing EU customer data is stored within the EU
Software AG (formerly called Built.io)	Webex Teams ID (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. Use of bot requests is optional for Webex users.	United States
Snowflake	Host and Usage Information (as requested by Customer)	This service is used to produce customized reports when expressly requested by Customer.	United States (AWS) Ireland (AWS) Frankfurt (AWS) Sydney (Australia) (AWS) Azure US -East Azure Europe West
Sparkpost Email Service	Name, Email address	Send communications to Customers.	Global

Optional Third-Party Integrations

- Webex integrations: Customers may incorporate third-party industry leading applications right into the Webex workflow. Such third-party applications have their own privacy policy applicable to the data shared by the Customer through the integration. To use such third-party applications, Customers must enable each integration. For more information, please visit the Webex Integration Site. Unencrypted messages may be shared with third-party services and applications that you choose to integrate with the 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 App on iOS and Android devices by sending push notifications through Apple Push Notification service and Google Firebase Cloud Messaging respectively. Users may opt-out of receiving these notifications at any time by changing their device's notification settings.
- GIPHY: Users can share animated GIFs by accessing GIPHY directly from the Webex App. While GIPHY appears within the user interface by default in latest versions of the Webex App, Customers may opt-out of the GIPHY feature at any time through the Control Hub portal. If GIPHY is available and users choose to utilize GIPHY's functionality to personalize their message, GIPHY may receive the user's IP address and GIF search terms. For more information, you may visit GIPHY's terms of service and privacy policy.

11. Information Security Incident Management

Breach and Incident Notification Processes

The Information Security 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), the Advanced Security Initiatives Group (ASIG), and Cisco Legal.

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.

12. Certifications and Compliance with Privacy Requirements

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 security and privacy in mind and is designed so that it can be used by Cisco customers in a manner consistent with global security and privacy requirements, including the EU General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and Personal Health Information Protection Act (PHIPA), Health Insurance Portability and Accountability Act (HIPAA), and Family Educational Rights and Privacy Act (FERPA).

Further, in addition to complying with our stringent internal standards, Cisco also maintains third-party certifications and validations to demonstrate our commitment to information security and privacy. Webex has received the following certifications:

- EU Cloud Code of Conduct Adherence by SCOPE Europe
  - For more information about the EU Cloud of Conduct see: Cisco Webex EU Cloud Code of Conduct and the Verification of Declaration of Adherence.
- ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27701:2019 Certification
- SOC 2 Type II Report
- BSI Cloud Computing Compliance Criteria Catalogue (German C5)
- CSA STAR Level 2 Certification
- HIPAA Attestation
- Spanish ENS (Esquema Nacional de Seguridad) Certification
- Italian AgID (Agency for Digital Italy) Certification
- Australian IRAP (Information Security Registered Assessors Program) Certification
- Japanese ISMAP (Information System Security Management and Assessment) Certification

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

13. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, data portability and / or deletion of the personal data processed by the Service as well as object to processing.

We will confirm identification (typically with the email address associated with a Cisco account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the Customer/Controller, may be redirected to their employer for a response.
Requests can be made by submitting a request via:

1) the Cisco Privacy Request form
2) by postal mail:

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

We will endeavor to timely and satisfactorily respond to inquiries and requests. If a privacy concern related to the personal data processed or transferred by Cisco remains unresolved, contact Cisco's US-based third-party dispute resolution provider. 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.

14. General Information

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

This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement. To the extent this document differs from the Cisco Online Privacy Statement, this document will take precedence. If there is a difference in translated, non-English versions of this document, the U.S.-English version will take precedence.

Cisco frequently evolves and updates its offerings. Cisco Privacy Data Sheets are subject to change, and are reviewed and updated on an annual basis, or as reasonably needed to reflect a material change in the processing of Personal Data. For the most current version, go to the Personal Data Privacy section of the Cisco Trust Center.

To receive email notifications of updates to the Privacy Data Sheet, click the "Subscribe" link in the upper right corner of the Trust Portal.