Cisco WebEx
Privacy Data Sheet

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

1. Overview of Cisco WebEx Capabilities

Cisco WebEx (the "Service") is a cloud-based web and video conferencing solution made available by Cisco to companies or persons ("Customers," "you," or "your") who purchase it for use by their authorized users (each, a "user"). Cisco WebEx enables global employees and virtual teams to collaborate in real time from anywhere, anytime, on any mobile device or video system as though they were working in the same room. Solutions include meetings, events, training, and support services. For a detailed overview of Cisco WebEx, please visit the Cisco Web Conferencing homepage.

Because Cisco WebEx enables collaboration among its users, you may be asked to provide your personal data in order to use the Service. The following paragraphs describe Cisco's processing of personal data in connection with the delivery of Cisco WebEx, the location and transfers of that data, and how it is secured in accordance with privacy principles, laws, and regulations. If you choose to purchase Cisco WebEx, you will need to disclose personal data to Cisco in order to use it. 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

Cisco WebEx allows users to instantly connect in a way that is as personal as a face-to-face meeting. The meeting host has the option to record meetings and all users have the option to upload and preserve files shared during and outside of WebEx meetings. If the meeting host opts not to preserve the meeting content, it disappears from the Cisco WebEx platform immediately after the meeting concludes. If you are a user and your employer is the Customer that purchased the Service, all of the information described in this Privacy Data Sheet is accessible by 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. *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 platform, copies of that information may remain viewable elsewhere to the extent it has been shared with others.*

This Privacy Data Sheet covers WebEx Meeting Center, Event Center, Support Center, and Training Center and Technical Support Assistance included with the Service. If you use the Service together with Cisco Spark or WebEx Meetings (purchased online), see the see the Privacy Data Sheet pertaining to those services for descriptions of the data that may be collected and processed in connection with those services. The tables below list the categories of personal data used by Cisco WebEx and describe why we process such data.

WebEx Meeting Center, Event Center, Support Center, and Training Center

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Name • Email Address • Password • Public IP Address • Browser • Phone Number (Optional) • Mailing Address (Optional) • Avatar (Optional) • Billing Information	We use Registration Information to: • Enroll you in the Service • Display your user avatar identity to other users • Make improvements to the Service and other Cisco products and services • Provide you support
Host and Usage Information	• IP Address • User Agent Identifier • Hardware Type • Operating System Type and Version • Client Version • IP Addresses Along the Network Path • MAC Address of Your Endpoint (As Applicable) • Service Version • Actions Taken • Meeting Session Information (title, date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity) • Number of Meetings • Number of Screen-Sharing and Non-Screen-Sharing Sessions • Number of Participants • Host Name • Screen Resolution • Join Method • Performance, Troubleshooting, and Diagnostics Information	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	• Meeting and Call Recordings • Uploaded Files	We use User-Generated Information to: • Provide the Service, optional components which include recording meetings and file sharing

Technical Support Assistance (TAC)

Personal Data Category	Types of Personal Data	Purpose of Processing
TAC Support Information	• Name • Email Address • Phone Number of the Employee Appointed to Open the Service Request • Authentication Information (exclusive of passwords) • Information About the Condition of the System • Registry Data About Software Installations and Hardware Configurations • Error-Tracking Files	We use TAC Support Information to: • Provide you support • Review quality of the support service • Perform analysis of the service solution

3. Cross-Border Transfers

Cisco WebEx leverages its own data centers to deliver the Service globally. If you join a WebEx meeting from a Cisco Spark endpoint or using a Cisco Spark client, please see the Cisco Spark Privacy Data Sheet for applicable privacy information, including data center locations. The Cisco WebEx 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	Illinois, USA
Hong Kong, China	New York, USA
London, UK	Sydney, Australia
New York, USA	Texas, USA
Singapore, Singapore	
Texas, USA	
Tokyo, Japan	
Toronto, Canada	
Virginia, USA	

User-Generated Information is stored in the data center closest to a Customer's location as provided during the ordering process.

Cisco uses a number of transfer mechanisms to enable the lawful use of data across jurisdictions, depending on context, including:

- EU-U.S. and Swiss-U.S. Privacy Shield Frameworks
- APEC Cross Border Privacy Rules
- EU Standard Contractual Clauses

- Binding Corporate Rules are currently in-process

4. Access Control

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

Personal Data Category	Who Has Access	Purpose of Access
Registration Information	User through the My WebEx Page	Modify, control, and delete information
	Customer through the Site Admin Page	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 through the Site Admin Page	View Meeting Session Information
	Cisco	Support and improvement of the Service by the Cisco WebEx 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	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 WebEx, copies of that content may remain viewable elsewhere to the extent it has been shared with others.

5. Data Portability of User-Generated Information and Other Personal Data

Cisco WebEx 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 WebEx proprietary ARF and standard mp4 formats depending on the account type. Cisco offers a free WebEx ARF player to convert ARF files to mp4 format.

Customers are permitted to export personal data collected about their users on the Cisco WebEx platform using APIs or via the Site Admin Configuration. There is no time restriction on exporting this data.

6. Data Deletion & Retention

Subject only to their employer's corporate retention policies, users with an active WebEx subscription have complete control over how long their User-Generated Information (*e.g.*, recordings and files they initiate or upload) is stored on the Cisco WebEx platform and can delete such 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. After the Service is terminated or expires, User-Generated Information is deleted from the Cisco WebEx platform within 60 days.

Customers can request deletion of other personal data retained on the Cisco WebEx platform by sending a request to privacy@cisco.com or opening a TAC service request, and unless the personal data is required to be retained for Cisco's legitimate

business purposes, 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 Cisco WebEx 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.
TAC Support Information	Until Customer (i) requests deletion via email to privacy@cisco.com or (ii) by opening a TAC service request	TAC Support Information is retained to ensure efficient support in case of recurring issues and to comply with Cisco audit policies related to business records of services provided to Customers.
User-Generated Information	Active Subscriptions: • At Customer's or user's discretion Terminated Service: • Deleted within 60 days	User-Generated Information is not retained on the Cisco WebEx 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

Cisco WebEx is ISO 270001, SSAE – 16, and SOC 2 Type II 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
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	Encrypted in transit, but not at rest

Protecting Data at Rest

Cisco WebEx encrypts sensitive data at rest. Any data not encrypted at rest is protected by highly-secure data center protection mechanisms and operational procedures. Cisco WebEx data centers feature communication infrastructure with industry-leading performance, integration, flexibility, scalability, and availability.

Encryption at Run Time

All communications on the Cisco WebEx platform occur over encrypted channels. After a session is established, all media streams (audio, VOIP, video, screen share, and document share) are encrypted. Cisco WebEx 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 endpoints, those attendees may be sending your meeting data unencrypted on the internet. Media streams flowing from a user to Cisco WebEx servers are decrypted after they cross the Cisco firewalls. The 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, Cisco WebEx also provides end-to-end encryption. With this option, Cisco WebEx does not decrypt the media streams. In this model, traffic cannot be deciphered by the Cisco WebEx server. The end-to-end encryption option is available for WebEx Meeting Center and Support Center. Note that when end-to-end encryption is enabled, the following features are not supported:

- Network-based recordings
- Join Before Host
- Collaboration Meeting Rooms Cloud

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

We may share Registration Information, Host Information, and/or Usage Information with service providers, contractors or other third parties to assist in providing and improving the Service. The data shared may include aggregate statistics 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. We do not rent or sell your information.

If a Customer subscribes to the Service through a Cisco partner, we may share Host and/or Usage Information about the Customer's employees' use of the Service with the partner. If a Customer chooses to purchase support for the Service through a Cisco partner, any or all of the information described in this Data Sheet may be shared with the partner.

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. Cisco WebEx and its underlying processes are designed to meet Cisco's obligations under the EU General Data Protection Regulation and other privacy laws around the world.

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

- EU-U.S. and Swiss-U.S. Privacy Shield Frameworks
- APEC Cross Border Privacy Rules
- EU Standard Contractual Clauses
- Binding Corporate Rules are currently in-process

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

- ISO 27001
- SOC 2 Type II Attestation
- FedRAMP
- The WebTrust Seal of Assurance for CA and the Web Trust Seal of Assurance for CA–SSL

11. Corporate Quality Compliance and Certifications

Cisco holds a Global ISO 9001 Certification and ISO 14001 Registration, managed by the Corporate Quality Compliance and Certifications program, which establishes and maintains policies that ensure quality management of processes and environmental responsibilities. Visit our Quality Certifications page to understand the scope of these compliance certifications and read more information.

12. FAQs

For more information related to Cisco WebEx's technical and operational security features, please see the WebEx Security White Paper.

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