Cisco Webex Messenger
Privacy Data Sheet

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

1. Overview of Cisco Webex Messenger

Cisco Webex Messenger ("Webex Messenger" or the "Service") is a cloud-based messaging service made available by Cisco to companies or persons ("Customers," "you" or "your") who purchase it for use by their authorized users (each, a "user"). Customers may access Webex Messenger through Cisco Jabber clients (Jabber for Windows, Jabber for Mac, Jabber for iPhone and iPad, and Jabber for Android) or third party clients. Webex Messenger enables collaboration via instant messaging, desktop sharing, and presence. For more details on Webex Messenger, please see Cisco Webex Messenger.

Because Webex Messenger enables collaboration among its users, if you choose to purchase Webex Messenger, you will 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 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 purchased the Service, all of the information described in this Privacy Data Sheet is subject to your employer's policies regarding access, 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. Copies of messages may remain viewable elsewhere to the extent they have been shared with others.*

The table below lists the categories of personal data processed by Webex Messenger and describes why we process such data.

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Display Name • Email Address • First Name • Last Name • Street Address • Customer Name • Org ID • Password • SIP URI • Directory Number • User Avatar	We use Registration Information to: • Activate and provision Webex Messenger • Display your user avatar identity to other users • 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 • Provide you remote access support • Authenticate and authorize access to your account

Personal Data Category	Types of Personal Data	Purpose of Processing
Host and Usage Information	• Device Name • User Activity • Time Zone • IP Address • Geolocation (precise longitude and latitude) • Locale Setting • Mobile ID • MAC Address • Oath Token • UUID • Domain Name • Real-Time Media • File Names • Uploaded Files • Search Queries • Space or Meeting Titles • Web User Agent • Email Content	We use Host and Usage Information to: • Understand how the Service is used • Track technical performance • Diagnose technical issues • Respond to customer support requests • Conduct analytics and statistical analysis in aggregate form to improve the technical performance of Webex Messenger
User-Generated Information	• Messages / Chats / Conversations	We use User-Generated Information to: • Provide the Service

Data for Analytics

Cisco collects a limited set of usage and performance data from the clients used to access Webex Messenger ("Analytics"). Cisco gathers Analytics without identifying users, analyzes only aggregated data, and uses such data only to improve performance of the Service.

The table below describes collection of data for Analytics and describes why we process such data.

What Cisco Collects	What Cisco Does Not Collect	Purpose of Processing
• Aggregated information about the clients such as the version and operating system on which they are running • A limited set of quantitative data concerning feature usage • A limited set of quantitative data concerning performance	• Information concerning the identity of individual recipients or senders of any communications • Information concerning the content of any communication, such as instant messages, video calls, or voice calls made using the Service • Information concerning the filenames or content of any files of any kind that are transferred or shared between clients	• Cisco collects, aggregates, and analyzes data to improve its products and services. • Cisco uses the data to analyze feature usage statistics and application performance.

Technical Support Assistance (TAC)

Cisco collects data to diagnose technical issues. The table below describes collection of TAC Support Information and describes why we process such data.

Personal Data Category	Types of Personal Data	Purpose of Processing

Personal Data Category	Types of Personal Data	Purpose of Processing
TAC Support Information	• First Name • Last Name • Email Address • Phone Number of the Employee Appointed to Open the Service Request • Authentication Information (exclusive of user password) • 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 remote access support • Review quality of the support service • Perform analysis of the service solution and resolve service issues

3. Cross-Border Transfers

Webex Messenger is hosted on Webex-owned and operated data centers in the United States and EU. Data center locations may change from time to time and this Privacy Data Sheet will be updated to reflect those changes.

Webex Messenger Data Center Locations:
Amsterdam, Netherlands
California, USA
London, UK
Texas, USA

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

- Binding Corporate Rules
- US-EU and Swiss-US Privacy Shields
- APEC Cross Border Privacy Rules
- EU Standard Contractual Clauses

4. Access Control

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

Personal Data Category	Who Has Access	Purpose of Access
Registration Information	• User • Customer • Cisco	User: Modify and control certain user information Customer: Manage users and administer Webex Messenger in accordance with Customer policies Cisco: Support Webex Messenger in accordance with Cisco's data access and security controls process
Host and Usage Information	• Customer • Cisco	Customer: Manage users and administer Webex Messenger in accordance with Customer policies Cisco: Support delivery and improvement of Webex Messenger in accordance with Cisco's data access and security controls process

Personal Data Category	Who Has Access	Purpose of Access
User-Generated Information	• User • Customer • Cisco	User: Users may access content that they generated or received for a variety of personal and business purposes Customer: Manage users and administer Webex Messenger in accordance with Customer policies Cisco: Support Webex Messenger in accordance with Cisco's data access and security controls process

5. Data Portability

An active user may export its individual roster of contacts using XMPP (eXtensible Messaging and Presence Protocol). An active Customer may export an enterprise-wide roster of all users' contacts by sending a request to privacy@cisco.com or opening a TAC support request. An inactive Customer may make a request to export an enterprise-wide roster within 30 days of becoming inactive.

6. Data Deletion and Retention

Customers may request deletion of data, including data related to deactivated users, retained on the Service by sending a request to privacy@cisco.com or opening a TAC support 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.

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.
Host and Usage Information	30 days from when the Service is deactivated	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.
User-Generated Information	No retention generally, unless certain features are enabled. See next column for retention periods associated with those features.	Cisco does not retain User-Generated Information. Two exceptions apply: 1. If a Customer enables logging of messages for its own corporate compliance purposes, Cisco will hold encrypted User-Generated Information for up to 8 hours and deliver messages to the Customer's secure endpoint. Once delivered, Cisco deletes the User-Generated Information from its systems. 2. For users who access Webex Messenger with push notifications enabled by users on Jabber for iOS, Cisco encrypts and holds User-Generated Information in memory for up to 72 hours to allow users to retrieve messages via push notifications. Once 72 hours have passed, Cisco deletes the User-Generated Information from its systems.
Data for Analytics	30 days from when the such data is collected	Aggregated information generated by instrumentation and logging systems created through the use and operation of the Service is kept for a limited period to improve performance of the Service.
TAC Support Information	Until Customer requests deletion via privacy@cisco.com or by opening a TAC service request for deletion	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.

7. Personal Data Security

Webex Messenger 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
Registration Information	Encrypted in transit, but not at rest (see below for how we protect this data at rest)
Host and Usage information	Encrypted in transit, but not at rest (see below for how we protect this data at rest)
User-Generated Information	Encrypted in transit. User-Generated Information is never at rest in our servers. If Customers access Webex Messenger through Cisco Jabber Clients, they may configure such client to use end-to-end encryption.

Protecting Data at Rest

Webex Messenger stores certain user data that may be critical to your business (when configured by a Customer to do so). Webex Messenger uses the following safeguards to protect this data at rest:

- We store all user passwords using hashing algorithm
- We encrypt passwords

8. Third Party Service Providers (Sub-processors)

Cisco performs the Service without sending Registration Information, Host and Usage Information, and User-Generated Information to any third party service providers.

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. 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. Webex Messenger 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.

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

- Binding Corporate Rules
- US-EU and Swiss-US Privacy Shields
- APEC Cross Border Privacy Rules
- EU Standard Contractual Clauses

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. Additional Information

For more information related to the Service's security architecture, please visit The Cisco Webex Messenger Security Architecture 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.