Cisco Webex Contact Center Enterprise

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco Contact Center Enterprise.

Cisco Webex Contact Center Enterprise ("Webex CCE" or the "Service") is a cloud-based contact center solution made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from Webex CCE 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 Webex CCE in order to provide its functionality.

1. Overview

Cisco Webex Contact Center Enterprise ("Webex CCE" or the "Service") delivers intelligent contact routing, by combining multichannel automatic call distribution functionality with telephony in a unified solution. The Service is made available by Cisco to companies or persons ("Customers," "you," or "your") who purchase it for use by their authorized users ("Users" or "Agents") and people who access contact centers enabled by the Service (each an "End-User"). A Customer may purchase the Service through a Cisco partner ("Partner").

The Webex CCE solution is accomplished by call treatment, network-to-desktop computer telephony integration (CTI), and multichannel contact management over an IP infrastructure. Webex CCE is powered by Cisco's Collaboration Solution for Contact Center and Unified Communications (UC). The major services provided are Contact Center as a Service (CCaaS) and Unified Communications as a Service (UCaaS) for contact center agents. Cisco Unified Communications Manager (CUCM) is the core call processing software for the Cisco Unified Communications System.

Because the Service enables collaboration among its users through voice conversations and text, personal data may be stored with the use of the Service. The following describes 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. If you choose to purchase the Service, you will need to disclose personal data to Cisco in order to use it. Cisco will use personal data consistent with this Privacy Data Sheet.

The Service integrates with various Cisco products, including Webex Calling Dedicated Instance, Webex Connect, and Webex Contact Center, Webex Connect, Webex WFO, and Webex Control Hub Please see the applicable Privacy Data Sheet for details regarding processing of personal data by the Cisco product receiving and sending personal data from and to the Service.

Note, the Service may also be integrated with products that the customer purchased from 3rd parties (including purchases through Cisco's Soultions Plus resale program). Cisco is not responsible for customer data once it leaves the Service for a non-Cisco product. Protection of data within the applicable third-party system is governed by the contract(s) and policies of the applicable third party.

For more information about Webex CCE, visit https://www.cisco.com/c/en/us/products/contact-center/webex-contact-center-enterprise/index.html?dtid=osscdc000283.

2. Personal Data Processing

The Service allows Customer Agents and End-Users to interact through an IP telephone, chat and outbound email. The Service processes personal data that is provided during the installation and use of Webex CCE. Webex CCE can store personal data in voice recordings and chat transcripts for quality management and system training purposes.

This Privacy Data Sheet covers the personal data that may be collected and/or processed in connection with those services. The table below lists the personal data processed by Webex CCE to provide its services and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
Admin Registration Data	• Name • Username • Email Address • Password • IP Address • Phone Number • Active Directory Information (optional)	• Provide the Service • Enroll you in Webex CCE • Improve the Service • Authenticate / authorize access to Webex CCE • Provide support • Understand how the Service is used • Route calls • Display information to other Agents • Send product notifications
User Registration Data	• Name • Email Address • Phone Number • User ID or display name • Other/Customized data (this is defined and configured by Customer – it may contain personal data) • IP address • Data provided by end-user through Dual Tone Multiple Frequencies (DTMF)	• Provide the Service • Improve the Service • Provide support • Understand how the Service is used • Route calls • Display information to other Agents
Telemetry Data	• Agent Identifier • Client Version • Device Information (e.g., phone type) • MAC Address • Software Version • Call Information, including durations, hold time, called number, calling number, time, date • Message Logs	• Understand how the Service is used • Provide support • Diagnose technical issues • Provide the Service • Improve the Service
Customer Content	• Call Recordings • Transcriptions of Call Recordings • Chat transcripts • Screen Captures • Emails	• Provide the Service • Ensure quality and training • Diagnose technical issues • Improve the Service

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.

3. Data Center Locations

Cisco uses its own data centers to deliver the Service globally. Webex CCE is located in data centers around the world to keep data as regionally as possible. Webex CCE 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, published here):

Cisco Data Center Locations
Netherlands
USA

UK
Singapore
Hong Kong
Australia
Brazil

User-Generated Information is stored in the data center closest to the Customer's location or as otherwise defined by Customer at the time of enrollment. All other data may be sent to Texas and Colorado through MPLS circuits for system and security monitoring.

There are three conductivity configurations used with the Webex CCE solution; Internet, Data Center to Data Center (DC-to-DC) and Customer Connectivity. The DC to DC connection is through MPLS circuits with a SDWAN overlay. Customer Connectivity only occurs over private and dedicated access. Internet access to customer interfaces is not permitted. The Internet circuit allows Cisco Support of the Cisco solution through a VPN and a Jumpbox. There is no direct internet access.

4. 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

5. Access Control

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

Personal Data Category	Who has Access	Purpose of the Access
Admin Registration Data	• Cisco	• Configure system for use by the Customer • Support the Service in accordance with Cisco's data access and security controls process
	• Customer	• Access, manage, edit and view users
User Registration Data	• Cisco	• Support the Service in accordance with Cisco's data access and security controls process
	• Customer	• Access, manage, and view use of the Service
Telemetry Data	• Cisco	• Support and improvement of the Service.
	• Customer	• Access and view Service usage and configuration information
Customer Content	• Cisco	• While Cisco operates the Service, Cisco will not access the data unless it is shared with Cisco by the Customer and will only access in accordance with Cisco's data access and security controls
	• Customer	• Access, view, modify, control, and delete in accordance with Customer's personal data policy

If a Customer purchases the Service through a partner, we may share any or all of the information described in this Privacy Data Sheet with the Partner to support the Service. Similarly, if a Customer purchases supplemental third-party services that may be used with the Service, Cisco may share some of the information described in this Privacy Data Sheet to enable the provision and function of that third-party service.

6. Data Retention

Customers can request deletion of other personal data retained on Webex CCE platform by submitting a request 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 may retain personal data.

Users seeking deletion of personal data retained on the Webex CCE platform must request deletion from their employer's site administrator. End-Users seeking deletion of personal data retained on the Webex CCE platform must request deletion from the Customer directly.

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

Type of Personal Data	Retention Period	Reason for Retention
Admin Registration Data	• Cisco will retain this information as long as Customer has an active subscription • After Customer has terminated the Service, Agent or User Information will be deleted within 28 days	• Provide the Service • Data collected as part of registration, including information provided by Customers as part of Cisco's financial due diligence, constitute Cisco business records and are kept to comply with Cisco financial and audit policies, as well as tax requirements
User Registration Data	• Cisco will retain this information as long as Customer has an active subscription • After Customer has terminated the Service, End- User Information will be deleted within 28 days	• Provide the Service
Telemetry Data	• Cisco will retain this information as long as Customer has an active subscription • After Customer has terminated the Service, Calling Information will be deleted within 60 days • Other Host and Usage information may be retained and deleted after 1 year	• 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
Customer Content	• Cisco will retain this information as long as Customer has an active subscription • After Customer has terminated the Service, User Generated Information will be deleted within 28 days •	• Provide the Service

If a Customer purchases supplemental third-party services that may be used with the Service, any data shared by Customer with those third-party service providers are subject to the privacy, security and retention polices of such third parties.

7. 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.

Personal Data Category	Security Controls and Measures
Admin Registration Data	• Encrypted in transit and at rest • Passwords encrypted and hashed in transit and at reast
User Registration Data	• Encrypted in transit and at rest
Telemetry Data	• Encrypted in transit and at rest
Customer Content	• All User-Generated Information is encrypted in transit and at rest • Data may not be encrypted for Real Transfer Protocol Traffic transmitted on private or local protected networks

Protecting Data at Rest

The Service encrypts the above-referenced data at rest through the use of self-encrypting drives and Transparent Data Encryption (TDE) with both using AES 256 bit key strength. Any data not encrypted at rest is protected by highly-secure data center protection mechanisms and operational procedures. Webex CCE data centers feature communication infrastructure with industry-leading performance, integration, flexibility, scalability, and availability.

Encryption with Webex CCE

Webex CCE platform utilizes encryption when information in transit utilizing TLS 1.2.

8. 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 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. The table below lists the current sub-processors for the Service. This list may change from time to time and this Privacy Data Sheet will be updated accordingly.

Sub-processor	Personal Data	Service Type	Location of Data Center
Google (Optional)	Customer Content	Google CCAI provides transcription services. This service is provided in the region where Customer is provisioned. When a Google CCAI customer creates a project in the GCP portal, that customer may select where certain Customer Data will be stored, and Google will store it there in accordance with the Service Specific Terms found here.	Google Cloud Platform data storage facilities are located here. in these countries and regions https://cloud.google.com/about/locations,
Calabrio (Optional)	Voice Communication Recordings	Cloud Infrastructure Storage. Customers can elect to use Calabrio for long term storage of recordings. This service is provided in the region where Customer is provisioned.	Calabrio Data Center locations include the following: USA: Ohio, Oregon and Virginia Canada: Montreal, Quebec LATAM: Sao Paulo, Brazil EU: Dublin, Ireland UK: London, England ANZ: Sydney, Australia SGP: Singapore

Amazon Web Services	Registration Data	To faciliate email transfers (Simple Email Service)	USA

9. 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), 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 Requirements

The Security & Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

-

Further, in addition to complying with our stringent internal standards, the Service has received the following certifications which are available in Cisco's Trust Portal:

- PCI- DSS
- SOC 2 Type II Attestation
- HIPAA Attestation
- ISO 27017:2015
- ISO 2700/17
- ISO 27018:2019

11. 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.

Only Cisco Authorized Administrators may bulk export User-Generated information. Customers may request an export from Cisco, or a Partner who must submit a request to Cisco. The availability of the data is subject to the deletion and retention policies described in Section 7 below. Customers may also export Call Information as defined above in the table in section 2.

All call and chats exports use AES 256 bit encryption. Individual Agent historical Webex CCE related statistics may be exported by Customer through the Webex CCE reporting platform.

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.

12. 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.