



Offer Disclosure

Webex Engage

This Offer Disclosure provides detailed information about data handling practices, security controls, and AI features specific to this Cisco Offer. It complements the [General Disclosures](#), which outline Cisco's overarching approach to handling Customer Systems Information and Customer Content, and the [Cisco Online Privacy Statement](#), which offers a more in-depth explanation of how Cisco manages personal data. Together, these documents provide transparency by addressing data handling at both a high level and an Offer specific level, helping you understand how Cisco protects and processes information across its Offers.

Capitalized words not otherwise defined in this Offer Disclosure have the meanings set forth in the Cisco General Terms or General Disclosures. To the extent this document differs from the Cisco Online Privacy Statement or General Disclosures, this document will take precedence regarding Offer specific information. If there is a difference in the translated, non-English versions of this document, the US-English version will take precedence.

Cisco will review and update this disclosure on an annual basis, or as needed, to reflect material changes in the processing of Customer Systems Information or Customer Content. For updates, subscribe via the "subscribe" link in the upper right corner of the [Trust Portal](#).

1. Overview

Webex Engage is a cloud application built for Contact Centers to enable customer service agents to easily have live two-way conversations with their customers over Short Message Service (SMS), Facebook Messenger, Twitter, web and email, whilst working alongside their existing voice systems.

For more information about Webex Engage, visit [Webex Engage](#).

2. Data Handling

2a. Collection, Purpose & Retention

Cisco believes in transparency when it comes to how Cisco handles Customer Content and Customer Systems Information. This disclosure provides details about the types of data Cisco collects, specific data elements involved, the purposes for which they are used, and how long Cisco retains them for this Cisco Offer.

Table 1: Customer Content

Data Category	Data Elements (Examples)	Purposes	Retention Period
Registration Data	Personal Data: - Account Contact name - User Email Address - User ID	- Provision and enroll you in the service - Authenticate and authorize access to the service - Enable product operations and functionality - Communicate on status and availability of service - Send product and support notifications - Technical configuration - Troubleshooting	When you are an active customer: - Indefinitely until a deletion request is received. Upon termination/expiration: - Upon customer request for deletion of data, registration data is obfuscated and pushed into archive and this obfuscated data is deleted after 7 days.
Host and Usage Data	Personal Data: - End user IP address (personal devices) - Geolocation * - Log Files - Session ID - User Identifier - Web Browser IP Address	- Provision and delivery of the service to Customer end users - Maintain user session connectivity to the service - Diagnose technical issues - Provide endpoint security - Provide security analytics and forensics - Provide malware analysis and threat intelligence - Respond to customer support requests - Provide profile details to customer service agent - Technical configuration - Troubleshooting	When you are an active customer: 180 days from the end of a session Upon termination/expiration: - Upon customer request for deletion of data, data deleted after 7 days.
User Generated Data	Personal Data: - Email messages and attachments - Instant messages / chats / conversations - Uploaded Media Files - Tweets	- Enable product operations and functionality - Provide messaging services for customers - Provision of the service - Technical configuration - Troubleshooting	When you are an active customer: - Between 1 and 18 months in live and up to a further 24 months in archive, based on the chosen configuration Upon termination/expiration: - Upon customer request for deletion of data, data deleted after 7 days.

System Generated Data	Personal Data: • Audit Records • Mobile Identifier • System Generated Email messages and attachments • System Generated, chats, conversations. • User Agent • User Location • Gender ** • Profile photo **	• Enable product operations and functionality • Provision of service • Technical configuration • Troubleshooting	When you are an active customer: • Audit Records: 90 days • Mobile Identifier, User Agent, User Location, Gender and Profile photo: Indefinitely until deletion after termination or expiration. • System Generated Email messages, attachments, chats, and conversations: Between 1 and 18 months in live and up to a further 24 months in archive, based on the chosen configuration Upon termination/expiration: • Audit Records: Deleted after 7 days • Mobile Identifier: Data is obfuscated and stored for 7 days and then purged • System Generated Email messages, attachments, chats, conversations; User Agent; User Location; Gender ** and Profile photo **: Upon customer request for deletion of data, data deleted after 7 days.
-----------------------	--	---	---

*Geolocation is only collected on the live chat channel, and only if selected by you, the Customer.

**This is collected by the Customer from the Facebook profile of individuals contacting the Customer, only when using the Facebook channel. It is not collected if it has been disabled by the individual in Facebook.

Table 2: Customer Systems Information

Data Category	Data Elements (Examples)	Purposes	Retention Period
Administrative Data	Personal Data: ▪ Cisco.com ID ▪ First and last name ▪ Email address ▪ Physical address ▪ User ID	Offer Delivery Customer billing Account administration	When you are an active customer: • Indefinitely until a deletion request is received. Upon termination/expiration: • Customer Systems Information stored on primary database is deleted immediately upon customer request. • Customer Systems Information stored on archive databases is deleted 7 days after customer request.
Administrative Data	Non-Personal Data: • Company email • Company physical address • User ID		
Configuration Data	Personal Data: • User Settings	• Configuration data is typically used to tailor the functionality	When you are an active customer:

	Non-Personal Data: - Settings - Hardware Settings - Software Configuration - Network Setting	of a system to specific requirements or preferences. Configure functionality	Indefinite until deletion Upon termination/expiration: - Customer Systems Information stored on primary database is deleted immediately upon customer request. - Customer Systems Information stored on archive databases, is deleted 7 days after customer request.
Events Data	Non-Personal Data: - Logs - Events data refers to records or logs of specific occurrences, actions, or incidents that take place within a system, application, network, or environment. Events typically represent significant or noteworthy activities, such as system events, errors, warnings, transactions, changes in state, or other noteworthy occurrences.	Events data is often used for troubleshooting, auditing, monitoring, analysis, and reporting purposes to understand the behavior and performance of systems and applications.	When you are an active customer: 6 months live (transactional data which is visible to Customer from the application) and 2 years in archive (not visible to client, can be retrieved and shared offline based on the client request) Upon termination/ expiration: - Customer Systems Information stored on primary database is deleted immediately upon customer request. - Customer Systems Information stored on archive databases is deleted 7 days after customer request.
Telemetry Data	Non-Personal Data: - Measurements - Readings - Status updates - Performance metrics - Environmental conditions In the context of technology and systems, telemetry data often refers to real-time or near-real-time data streams generated by sensors, instruments, devices, or software systems. This data can include measurements, readings, status updates, performance metrics, environmental conditions, and other relevant information used for monitoring and analysis purposes.	- Monitoring - Analysis - Reporting Telemetry data is information collected from remote sources and transmitted to receiving equipment for monitoring, analysis, or control purposes.	When you are an active customer: 6 months live (transactional data which is visible to Customer from the application) and 2 years in archive (not visible to client, can be retrieved and shared offline based on the client request) Upon termination/expiration: - Customer Systems Information stored on primary database is deleted immediately upon customer request. - Customer Systems Information stored on archive databases is deleted 7 days after customer request.

2b. Storage and Processing

Data Centers. Cisco uses its own data centers as well as third-party infrastructure providers to deliver this Cisco Offer’s capabilities globally.

Table 3: Data Centers

Infrastructure Provider	Infrastructure Provider Locations
Amazon Web Services (AWS) North America Cloud	North America (USA)
Amazon Web Services (AWS) North America Cloud	North America (Canada)
Amazon Web Services (AWS) UK Cloud	Europe (UK)
Amazon Web Services (AWS) EU Cloud	Europe (Ireland)
Amazon Web Services (AWS) Asia Pacific Cloud	Asia Pacific (Singapore)
Amazon Web Services (AWS) Asia Pacific Cloud	Asia Pacific (Australia)
Amazon Web Services (AWS) Asia Cloud	Asia (India)

Webex Engage leverages third party cloud hosting providers to provide service globally.

For this Cisco Offer, your information is stored and processed in the data center closest to your principal place of business as provided to Cisco during the ordering process. For example purposes only, if you are based in Europe your information will be stored and processed in the AWS EU or UK Cloud at your choice.

Service Providers. Cisco may share Customer Systems Information and Customer Content with a trusted ecosystem of suppliers. In each instance, each participant has agreed to confidentiality terms, compliance with applicable law, and adherence to information security, privacy, and other data processing requirements with Cisco that are consistent with Cisco’s commitments to you.

Subcontractors assist with broader data processing services, while subprocessors specifically process Personal Data on Cisco’s behalf to support the functionality of the Cisco Offer. Both are listed below. For updates, subscribe via the “subscribe” link in the upper right corner of the Trust Portal.

Table 4: Subcontractors

Name	Service Type	Cisco Data Center Location
Amazon Web Services (AWS)	AWS cloud infrastructure is used to host Webex Engage.	Australia Canada India Ireland

		Singapore United Kingdom Oregon, United States
--	--	--

Table 5: Subprocessors

Name	Personal Data	Service Type	Cisco Data Center Location
Amazon Web Services (AWS)	• Host and Usage Data • Registration Data • System Generated Data • User Generated Data	AWS cloud infrastructure is used to host Webex Engage.	United States (Oregon and Virginia) Canada United Kingdom Ireland Singapore Australia India
Mailgun	• System Generated Data • User Generated Data	Mailgun provides email services for receiving emails into Webex Engage	USA UK
Sendgrid	• System Generated Data • User Generated Data	Sendgrid provides email services for receiving emails into Webex Engage	USA (Virginia, Illinois, and Las Vegas) UK
Maxmind	• Host and Usage Data	Maxmind provides the geolocation of users in the live chat channel	USA (Oregon and Virginia) UK
Meta	• Host and Usage Data	Facebook provides profile pictures and gender information of an individual contacting the Customer, only when using the Facebook channel, to display to the customer service agent. Sharing can be disabled by the individual in their own Facebook profile.	USA (Oregon, North Carolina, Iowa, and Texas) EU (Sweden, Ireland, Denmark) APAC (Singapore)

Technical Support and Operations

Customer support utilizes a 24/7 "follow the sun" technical support model, using support engineers in countries including India.

2c. Access and Sharing

Customers and their authorized third parties may directly access Data by using service-standardized data interfaces described in API documentation found [here](#), subject to the provisions of [Webex for Developers Terms of Service](#). Webex Engage APIs support both structured and unstructured data sets depending on the particular data set requested from Webex Engage. Depending on the standard implemented by the API, structured data sets may use JSON, XML, or other standardized data formats; while unstructured data sets may be in the form of text, PDF or other unstructured data file formats. For more details, please consult the API documentation referenced above.

Customers may send requests for expanded API or data interface capabilities through their usual Cisco support or account management channels.

Cisco will make data available for porting and switching through the standardized APIs, consistent with the specifications provided in [Cisco API Guidelines](#) and subject to the provisions of [Webex for Developers Terms of Service](#).

Cisco makes certain Customer Systems Information available to Customers and their authorized third parties in a structured, commonly used machine-readable format through the following standardized APIs, consistent with the specifications provided in the [Cisco API Guidelines](#).

- [API Documentation](#)

Webex Engage APIs support both structured and unstructured data sets depending on the particular data set requested from Webex Engage. Depending on the standard implemented by the API, structured data sets may use JSON, XML, or other standardized data formats; while unstructured data sets may be in the form of text, PDF or other unstructured data file formats. For more details, please consult the API documentation referenced above.

Customers may send requests for expanded API or data interface capabilities through their Cisco support or account management channels.

To the extent that any information comprising Cisco's algorithms, analysis, inferences, proprietary software, insights, derivations, or assigned values can be viewed, reverse engineered, reconstituted, or otherwise interpreted from the data, such information is a "Cisco Trade Secret," and subject to such confidentiality obligations.

3. Security

3a. Access Control and Encryption

Cisco has implemented reasonable and appropriate technical and organizational measures designed to protect data from accidental loss, unavailability, and unauthorized access, use, alteration, and disclosure.

Table 6: Access & Controls

Data Category	Who Has Access	Purpose of Access	Security Controls
Registration Data	Customers	• Configure, manage, and operate the service • Modify, control, and delete information • Manage users and administer service in accordance with your policies • Access, modify, and delete content in accordance with your personal data policy • Use the portal	Encrypted in transit and at rest
	Cisco:	• Enable product operations and functionality • Deliver, support, and improve the service • Create accounts • Grant access to the portal	
Host and Usage Data	Customers	• Configure, manage, and operate the service • Modify, control, and delete information • Access, modify, and delete content in accordance with your personal data policy • Use the portal	Encrypted in transit and at rest
	Cisco:	• Enable product operations and functionality • Deliver, support, and improve the service	
User Generated Data	Customers	• Access, modify, and delete content in accordance with your personal data policy • Obtain reported information	Encrypted in transit and at rest

	Cisco:	• Provide support when required	
System Generated Data	Cisco:	• Manage users and administer service in accordance with your policies • Modify, control, and delete features • Upload files for security analytics and forensics • Set policies, view incidents, troubleshoot	Encrypted in transit and at rest

3b. Reports & Resources

In addition to complying with internal standards, Cisco maintains third-party validations and certifications to demonstrate its commitment to robust information security and privacy. The General Disclosures describe Cisco’s enterprise-wide certifications.

Customers can view available certifications at the [Cisco Trust Portal](#) (some of which will require a Non-Disclosure Agreement).