Cisco Webex Contact Center Service

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

Cisco Webex Contact Center 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 Cisco Webex Contact Center 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 Cisco Webex Contact Center in order to provide its functionality.

1. Overview

Cisco Webex Contact Center (the "Service") is a cloud-based contact center solution made available by Cisco or its resale partners ("Partners") to companies ("Customer", "you", "your") who purchase it for use by their authorized users ("Administrators"), their contact center agents ("Agents") and people who access contact centers enabled by the Service ("Users").

2. Personal Data Processing

The information described in this Privacy Data Sheet is accessible by Customers, Cisco, and Partners as described below. Administrators, Agents and Users' information is also subject to a Customer's policies regarding access, use, monitoring, deletion, preservation, and export of information associated with the Service. Cisco has no control over, and is not responsible or liable for, the privacy of information that Administrators, Agents and Users have shared with others. Even after information has been removed from the Service, copies of that information may remain viewable elsewhere to the extent it has been shared with others by Administrators, Agents, Users or a Customer.

The table below lists the personal data used by the Service and describes why we process that data.

Cisco Webex Contact Center 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.

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	Authentication Token Name and aliases Email Address Phone Number User ID Password Designation Cookies Company Name Company Contact Name Company Physical Address Company Time-Zone SIP IP Address Organization ID	We use Registration Information to: Provision the Service Provide operational support Communicate with you on the status and availability of the Service Enroll you in the Service Authenticate and authorize access to the Service Understand how the Service is used Make improvements to the Service Route calls and multimedia services

Host and Usage Information	Log / Billing Files Agent Identifier Login URL Cookies Automatic Number Identification Information End User Phone Numbers and associated Call Detail Records ("CDRs") Multimedia traffic data with associated identifiers (including sender, recipients, date, time and duration) Alert Message Data Time Zone Geolocation Domain Name	We use Host and Usage Information to: Understand how the Service is used Billing Diagnose technical issues Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service Respond to Customer support requests Enforcing compliance with our terms of use and other policies in connection with legal claims, compliance, regulatory and investigatory purposes. Marketing communication (with consent)
Agent and User Generated Data	Voice Communication Recordings Non-voice communications data (email, instant messages and chat histories) Uploaded Media Files Agent Call Associated Data (CAD)	We use Agent and User-Generated Information to: Provide the Service, and enable training and quality control Provide customized prompts Provide data processing services for voice recordings and/or transcription Agent CAD information based on business requirements

3. Data Center Locations

Cisco Webex Contact Center leverages third-party hosting providers and business partners to deliver the Service globally. The Service's 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):

Cloud-Hosted Application Processing Locations:	**Virtual Point of Presence (vPOP) Locations**
AWS US	Amsterdam, Netherlands
AWS United Kingdom	Calgary, Canada
AWS Germany	London, UK
AWS Australia	Los Angeles, USA
AWS Canada	New York, USA
	Toronto, Canada
	Tokyo, Japan
	Osaka, Japan
	Sydney, Australia
	Melbourne, Australia

4. Cross-Border Data Transfer Mechanisms

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

- Binding Corporate Rules
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

5. Access Control

Administrators, managers, supervisors, and agents who have been granted authorized Roles Based Access Controls (RBAC) can monitor real-time and historical information transacted on their specific tenant only through the Management Portal of Webex Contact Center.

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

Personal Data Category	Who has access	Purpose of the access
Registration Information	Administrators and Agents through the Tenant Management Portal	Modify, control, and delete information.
	Customer through the Tenant Management Portal	Modify, control, and delete in accordance with Customer's personal data policy.
	Partner through the Partner and Tenant Management Portal. Partners do not have access to Authentication Tokens or Passwords	Modify, control, and delete in accordance with Partner's personal data policy.
	Cisco	Support the Service in accordance with Cisco's data access and security controls process.
Host and Usage information	Administrators and Agents through the Tenant Management Portal and Agent Desktop	View Interaction Information and History.
	Customer through the Tenant Management Portal	Analysis to improve user performance and customer satisfaction
	Partner through the Partner and Tenant Management Portal	Analysis to improve user performance and customer satisfaction
	Cisco	Support and improvement of the Service
Agent and User Generated Information	Agents through the Tenant Management Portal	Access and view historical data.
	Customer and Administrators through the Tenant Management Portal	Modify, control, and delete in accordance with Customer's personal data policy
	Partner through the Partner and Tenant Management Porta	Modify, control, and delete in accordance with Partner's personal data policy
	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by the Customer and will only access in accordance with Cisco's data access and security controls process.

6. Data Portability

Data Records such as Call Detail Records and/or personal data collected about Customers, Administrators, and Users (as described in Section 2 above) are available to Cisco's Partners and Customers in machine readable format upon Partner request. Data must be requested within 60 days post contract termination and is subject to data retention policies (as described in section 7 below). Users of the Service that wish to access their personal data must request it from the Customer.

7. Data Deletion and Retention

Partner may request deletion of personal data retained on the Service on behalf of Customer, Agents, Administrators or Users by sending a request as set forth in Section 12 below or open a TAC support request. When Partner makes a request for deletion, Cisco endeavors to delete the requested data from its systems within 30 days, unless the data is required to be retained for Cisco's legitimate business purposes. If we are required to retain certain categories of data, the reason why we retain it, and the retention period are described in the table below.

Personal Data Category	Retention Period	Reason 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	7 years	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 and to comply with Cisco financial and audit policies, as well as tax requirements
Agent and User Generated Data	Active Subscriptions: • Voice Communication Recordings at Customers' contractual requirements • Chat, email, SMS and social media digital channel transcripts: 6 months via Cisco/IMI Engage and an additional 18 months upon request. • Historical reporting data: 36 months Inactive Subscriptions: • Deleted within 60 days.	• Communication recordings and histories are retained in order to provide the service and enable training. • Customers have the ability to set organization-wide retention periods for voice communication recordings. • Uploaded media files are not retained on the Service when Customer or an Administrator deletes this data.

8. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and from unauthorized access, use, alteration or disclosure. The Service's technical and organizational security measures are certified annually in accordance with SOC 2, Type II, PCI-DSS standards, and HIPAA.

Personal Data Category	Type of Encryption
Registration Information	Encrypted in transit, and disk encrypted at rest
Passwords	Encrypted in transit and hashed at rest
Host and Usage Information	Encrypted in transit, and disk encrypted at rest
Agent and User Generated Data	Encrypted in transit, and disk encrypted at rest
Voice Communication Recordings	Encrypted in transit and at rest

Additional controls include:

- Encryption of all voice recordings and payment card details.
- Session encryption and secure file transmission.
- Authenticating Cisco employee, vendor and contractor access to information systems.
- All call recordings are access controlled.
- Regular audits to address the ongoing confidentiality, integrity, availability and resilience of Cisco processing systems and services.

9. Sub-processors

Sub-processor	Personal Data	Service Type
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: Montral, Quebec LATAM: Sao Paulo, Brazil EU: Dublin, Ireland UK: London, England ANZ: Sydney, Australia SGP: Singapore
Acqueon (Optional)	• Telephone Numbers	Acqueon is utilized to make outbound calling campaign management. This service is provided in the region where Customer is provisioned. Acqueon Data Center locations include the following: USA: Virginia UK: London, England ANZ: Sydney, Australia
Google (Optional)	• User Generated Data	Google CCAI provides transcription services. This service is provided in the region where Customer is provisioned. Google Cloud Platform data storage facilities are located here. in these countries and regions https://cloud.google.com/about/locations, 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.

We may share data with other Cisco entities and/or 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 Partner, we may share any or all of the information described in this Data Sheet with the Partner. 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. The table below lists the Service's current sub-processors.

10. 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.

11. Certifications and Compliance with Privacy Laws

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. Cisco 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.

See Section 4 above, for information about how Cisco leverages the personal data transfer mechanisms related to the lawful use of data across jurisdictions.

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

- PCI-DSS v 3.2 Certification
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27701
- SOC 2 Type II
- SOC 3
- HIPAA
- C5
- CSA-Star
- GDPR (Self- attested)

12. How to Exercise Your Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.

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 redirect to their employer for a response.

Requests can be made by submitting a request via:

1) submitting a request using the Privacy Request Form
2) by postal mail:

<table>
<tr><td colspan="3">Chief Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td></tr>
<tr><td>Americas Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td><td>APJC Privacy Officer
Cisco Systems, Inc.
Bldg. 80, Lvl 25, Mapletree Biz City
80 Pasir Panjuang Road
Singapore, 117372
SINGAPORE</td><td>EMEAR Privacy Officer
Cisco Systems, Inc.
Haarlerbergweg 13-19, 1101 CH
Amsterdam-Suidoost
NETHERLANDS</td></tr>
</table>

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.

13. General Information

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

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. 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.