Cisco Contact Center Enterprise Solution

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

1. Overview of Cisco Contact Center Enterprise Solution Capabilities

The Cisco Contact Center Enterprise Solution (the "Solution") consists of three distinct product offerings:

- Cisco Packaged Contact Center Enterprise ("PCCE") provides a contact center in a prepackaged deployment model designed for customers with 2,000 or fewer contact center seats. PCCE is an on-premise deployment hosted and operated by Customer. For additional details, see Cisco Packaged Content Center Enterprise.
- Cisco Unified Contact Center Enterprise ("UCCE") offers omnichannel customer care for service providers, outsourcers, and large enterprise companies scaling to 24,000 contact center seats. UCCE is an on-premise deployment hosted and operated by Customer. For additional details, see Cisco Unified Contact Center Enterprise.
- Cisco Hosted Collaboration Solution for Contact Center ("HCS-CC") delivers the capabilities of UCCE and Cisco Unified Customer Voice Portal with the benefits of cloud computing. HCS-CC is hosted and operated by a service provider to offer you Contact Center as a Service ("CCaaS"). For additional details, see Cisco Hosted Collaboration Solution for Contact Center.

Cisco does not host or operate the Solution on your behalf. As a result, we do not process any personal data that is described in this Privacy Data Sheet. However, if you choose to configure Cisco Context Service ("Context Service") with the Solution, then Cisco will process personal data within Context Service. The Cisco Context Service Privacy Data Sheet describes such processing of personal data and will be available on The Cisco Trust Center.

2. Personal Data Processing

This Privacy Data Sheet describes how personal data may be processed and stored by you ("Customer", "you", "your") or an HCS-CC service provider when the Solution is used in its default configuration. Note that you have the ability to change settings on how personal data is processed and stored, which is outside of Cisco's control and visibility. *If you change the default configuration of the Solution, parts of this Privacy Data Sheet may no longer be applicable.*

The table below lists the personal data used by you or an HCS-CC service provider to carry out the services and describes the purpose for processing such data.

Table 1 UCCE, PCCE, and HCS-CC

Personal Data Category	Types of Personal Data	Purpose of Processing
Outbound campaign contact list	• End-user name • End-user phone number • End-user account number • Custom fields (note, the custom fields collected are Customer-defined and may contain sensitive information if you so choose)	The contact list is built by the Contact Center Administrator ("CC Admin") and fed to the Outbound Dialer to provide the contact details for an outbound campaign.

Call Detail Records ("CDRs")	• End-user phone number and call metadata • Contact Center Agent ("CC Agent") statistics (call-handling metrics such as Agent name and call metadata such as hold time and speed of answer) • Other generated statistics	CDRs capture the history of the call. The aggregate of these entries makes up the Contact Center historical record. Real-time CC Agent statistics are also captured to generate real-time reports.

Table 2 PCCE Only

Personal Data Category	Types of Personal Data	Purpose of Processing
Configuration User credentials	• Username and password of user designated to configure PCCE ("Configuration User")	Validation of Configuration User. Collection of Configuration User credentials is configured by the CC Admin.
Peripheral Components Configuration User credentials	• Username and password of user designated to configure peripheral components ("Peripheral Components Configuration User") metadata such as hold time and speed of answer) • Other generated statistics	Validation of Peripheral Components Configuration User. Collection of Peripheral Components Configuration User credentials is configured by the CC Admin.

Table 3 Enterprise Chat and Email (ECE) feature

Personal Data Category	Types of Personal Data	Purpose of Processing
End-user data	• End-user name • End-user email address • End-user contact number • End-user photo attachments • End-user ID • End-user address • End-user account number	Establishing the email or chat session or generating real-time reports. End-user data is exchanged across components of the Solution. End-user address and end-user account number are collected if provided by the end-user.

Table 4 Contact Center Management Portal (CCMP) and Contact Center Domain (CCDM) feature

Personal Data Category	Types of Personal Data	Purpose of Processing
Customer data	• Group data (CCMP/CCDM normal user or security group login, dimensions display name, dimensions XML data, custom XML data associated with dimensions, name of all pkey dimensions, XML data associated	Provisioning Customer's authorized users in Contact Center. Collection of Customer data is configured by the CC Admin and collected as individuals are provisioned.

	with pkey dimensions, custom XML data associated with pkey dimensions, and hostname or IP address of the client of the machine where the session was originated) • Individual-specific data of Customer's authorized users (CCMP/CCDM user or group description, name, dimensions description, description of all pkey dimensions, and name of the person)	

Table 5 Customer Voice Portal (CVP)

Personal Data Category	Types of Personal Data	Purpose of Processing
End-user dial-pad input	• Data provided by end-user through Dual Tone Multiple Frequencies (DTMF) via their phone for inbound/outbound calls (note, user-dial pad input collected is customer-defined and may contain sensitive information if you so choose)	Processing an end-user's menu selection. End-user dial-pad input is not collected unless DTMF is configured by the CC Admin.
Call context data	• Extended Call Context (ECC) • Peripheral Call Variables (PV) Note, ECC and PV are customer-defined and may contain sensitive information if you so choose	Exchanging data fields across several components of the Solution. Call context data is not collected unless configured by the CC Admin. If configured, these fields are collected by default via system input. If you wish to collect call context data and not configure this feature, you can collect such data outside of CC
End-user data	• End-user phone number	Identifying the call. End-user data is also captured to generate real-time reports

Table 6 Finesse agent desktop

Personal Data Category	Types of Personal Data	Purpose of Processing
CC Agent credentials	• CC Agent username • CC Agent ID • CC Agent password	Validation of the CC Agent. Collection of CC Agent credentials is configured by the CC Admin. The CC Agent password is not collected unless configured by the CC Admin. If configured, such personal data is collected by default via system input.
Phonebook	• Name • Phone number	Organizing dialed numbers. The Phonebook is configured by the CC Admin.

Table 7 SocialMiner

Personal Data Category	Types of Personal Data	Purpose of Processing
End-user data	• End-user email address • End-user callback phone number • End-user details (e.g. name, address, phone number) and end-user IP address	Establishing a social media session. Collection of end-user data is configured by the CC Admin and is collected if provided by the end-user.

Table 8 Remote Expert Mobile (REM)

Personal Data Category	Types of Personal Data	Purpose of Processing
End-user data	• End-user computer or mobile device IP address • End-user username • End-user display name • End-user domain	Diagnosing issues to improve REM. Collection of this end-user data is configured by the CC Admin.
CC Agent credentials	• CC Agent IP address • CC Agent username • CC Agent display name • CC Agent domain • CC Agent ID	Validation of the CC Agent to establish a customer-to-agent session. Collection of this personal data is configured by the CC Admin.

3. Cross-Border Transfers

The Solution is not hosted or operated by Cisco. Accordingly, Cisco does not make or access cross-border transfers of personal data. If you choose to configure Context Service with the Solution, Cisco will conduct cross-border transfers of personal data within Context Service. The Cisco Context Service Privacy Data Sheet describes such processing of personal data and will be available on The Cisco Trust Center.

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

- Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- EU Standard Contractual Clauses

4. Access Control

The default settings of the Solution have the following access control characteristics.

Table 9 UCCE, PCCE, and HCS-CC

Personal Data Category	Access Control
Outbound campaign contact list	The CC Admin can access the contact list.
Call Detail Records	The CC Admin can access CDRs.

Table 10 PCCE Only

Personal Data Category	Access Control
Configuration User credentials	The CC Admin can access the Configuration User credentials.
Peripheral Components Configuration User credentials	The CC Admin can access the Peripheral Components Configuration User credentials.

Table 11 Enterprise Chat and Email (ECE) feature

Personal Data Category	Access Control
End-user data	The CC Admin can access end-user data.

Table 12 Contact Center Management Portal (CCMP) and Contact Center Domain (CCDM) feature

Personal Data Category	Access Control
Customer data	The CC Admin and Supervisor can access Customer data.

Table 13 Customer Voice Portal (CVP)

Personal Data Category	Access Control
End-user dial-pad input	The CC Admin can access the end-user dial-pad input.
Call context data	The CC Admin can access ECC and PV.
End-user data	The CC Admin can access end-user data.

Table 14 Finesse agent desktop

Personal Data Category	Access Control
CC Agent credentials	The CC Admin can access CC Agent credentials.
Phonebook	CC users and the CC Admin can access Phonebook.

Table 15 SocialMiner

Personal Data Category	Access Control
End-user data	The CC Admin can access end-user data.

Table 16 Remote Export Mobile (REM)

Personal Data Category	Access Control
End-user data	Customer may manually delete server logs.
CC Agent credentials	Customer may manually delete server logs

5. Data Deletion & Retention

The default settings of the Solution have the following data deletion and retention characteristics. Retention of data varies depending on Customer's implementation and management of the components of the Solution.

Table 17 UCCE, PCCE, and HCS-CC

Personal Data Category	Data Deletion and Retention
Outbound campaign contact list	This list is retained and edited by the CC Admin. An end-user may request deletion of this personal data from Customer.
Call Detail Records	CDRs are retained per the backup and purging policy set by Customer. CC Agent statistics are stored and purged hourly in the CUIC database which is a closed appliance.

Table 18 PCCE Only

Personal Data Category	Data Deletion and Retention
Configuration User credentials	The Configuration User credentials are retained until a replacement has been added.
Peripheral Components Configuration User credentials	The Peripheral Components Configuration User credentials are retained until a replacement has been added.

Table 179 Enterprise Chat and Email (ECE) feature

Personal Data Category	Data Deletion and Retention
End-user data	Such data is retained for two years. It is retained in logs for <1 day after which the personal data is overwritten. End-user data is also retained in the CUIC database which is a closed appliance and purged hourly.

Table 20 Contact Center Management Portal (CCMP) and Contact Center Domain (CCDM) feature

Personal Data Category	Data Deletion and Retention
Customer data	This personal data is retained until a user is removed from the system.

Table 21 Customer Voice Portal (CVP)

Personal Data Category	Data Deletion and Retention
End-user dial-pad input	End-user dial-pad input is retained per the backup and purging policy set by CC Admin. It is stored in the CVP Reports server which is a closed appliance.
Call context data	Call context data is retained in logs for <1 day after which such data is overwritten. If the CC Admin sets this personal data to be persistent, it is stored in the CC database and subject to the backup and purging policy set by CC Admin.
End-user data	This personal data is retained in logs for <1 day after which such data is overwritten. End-user data is also retained in the CUIC database which is a closed appliance and purged hourly

Table 22 Finesse agent desktop

Personal Data Category	Data Deletion and Retention
CC Agent credentials	CC Agent credentials are retained in memory until the login session ends and are retained in logs for <1 day after which such data is overwritten. If the CC Agent is removed by the CC Admin, their credentials are removed from Finesse and CUIC as well. The CC Agent password is not retained by Finesse or CUIC.
Phonebook	The Phonebook is retained in memory until the login session ends and is retained in logs for <1 day after which such data is overwritten. If a CC Agent is removed by the CC Admin, their contact information will be removed from the Phonebook as well. An end-user may request deletion of such data from Customer.

Table 23 SocialMiner

Personal Data Category	Data Deletion and Retention
End-user data	The SocialMiner database is a closed appliance and retention is set by the default SM DB Purge configuration, which can be adjusted by CC Admin. End-user IP address is retained in logs until the end-user data is overwritten.

Table 24 Remote Export Mobile (REM)

Personal Data Category	Data Deletion and Retention
End-user data	The end-user may manually delete Mobile SDK logs on their local device. Logs submitted to TAC for problem diagnosis may be stored indefinitely in the issue tracking system.
CC Agent credentials	The end-user may manually delete Mobile SDK logs on their local device. Logs submitted to TAC for problem diagnosis may be stored indefinitely in the issue tracking system.

6. Personal Data Security

The default settings of the Solution have the following data protections applied to personal data in motion and at rest.

Table 25 UCCE, PCCE, and HCS-CC

Personal Data Category	Type of Encryption
Outbound campaign contact list	The contact list is stored in the Blended Agent database table. This personal data is unencrypted. Customer may elect to apply IPsec and self-encrypting drive
Call Detail Records	CDRs are stored in the RCV/TCV tables of the AW-HDS-DDS historical database. This personal data is unencrypted. Customer may elect to apply IPsec and self-encrypting drive. For real-time reports, real-time CC Agent statistics are protected in-motion with TLS 1.2. CC Agent statistics are unencrypted when stored to a CC logger database. Customer may elect to apply self-encrypting drive. CDRs are also stored temporarily to the CUIC database which is a closed appliance. CC Agent statistics are protected with TLS 1.2 when the real-time report is displayed

Table 26 PCCE Only

Personal Data Category	Type of Encryption
Configuration User credentials	This personal data is encrypted with HTTPS. Customer may elect to apply self-encrypting drive.
Peripheral Components Configuration User credentials	This personal data is encrypted with HTTPS. Customer may elect to apply self-encrypting drive.

Table 27 Enterprise Chat and Email (ECE) feature

Personal Data Category	Type of Encryption
End-user data	This personal data is unencrypted. Customer may elect to apply IPsec and self-encrypting drive. Customer may also elect to mask end-user data from CC Agent view. For real-time reports, end-user data is protected in-motion with TLS 1.2. Such data is unencrypted when stored to a CC logger database. Customer may elect to apply self-encrypting drive. End-user data is also stored temporarily to the CUIC database which is a closed appliance. Such data is protected with TLS 1.2 when the real-time report is displayed.

Table 28 Contact Center Management Portal (CCMP) and Contact Center Domain (CCDM) feature

Personal Data Category	Type of Encryption

Customer data	Customer data is encrypted with HTTPS. Customer may elect to apply IPsec and self-encrypting drive. Customer may also elect to mask this personal data from CC Agent view

Table 29 Customer Voice Portal (CVP)

Personal Data Category	Type of Encryption
End-user dial-pad input	End-user dial-pad input is protected in-motion with AES256-bit. Customer may elect to suppress trace/log for this personal data. If Customer elects to report on such data, end-user dial-pad input is stored in CVP Reports Server, which is unencrypted. Customer may elect to apply self-encrypting drive.
Call context data	Call context data is unencrypted. Customer may elect to apply IPsec and self-encrypting drive.
End-user data	End-user data is unencrypted. Customer may elect to apply IPsec and self-encrypting drive. For real-time reports, end-user data is protected in-motion with TLS 1.2. This personal data is unencrypted when stored to a CC logger database. Customer may elect to apply self-encrypting drive. End-user data is also stored temporarily to the CUIC database which is a closed appliance. Such data is protected with TLS 1.2 when the real-time report is displayed.

Table 30 Finesse agent desktop

Personal Data Category	Type of Encryption
CC Agent credentials	CC Agent credentials are protected in-motion with TLS 1.2. Customer may elect to apply self-encrypting drive. For phone-based access with Finesse Internet Protocol Phone Agent (FIPPA), CC Agent credentials are sent unencrypted via HTML.
Phonebook	The Phonebook is protected in-motion with TLS 1.2. Customer may elect to apply self-encrypting drive. For phone-based access (FIPPA), the Phonebook is sent unencrypted via HTML.

Table 31 SocialMiner

Personal Data Category	Type of Encryption
End-user data	End-user data is protected in-motion with TLS 1.2. This personal data is stored unencrypted to the SM database and the SM log which are in a closed appliance

Table 32 Remote Export Mobile (REM)

Personal Data Category	Type of Encryption
End-user data	End-user data is protected in-motion with HTTPS and stored unencrypted in the SIP message logs. Customer may elect to apply self-encrypting drive
CC Agent credentials	CC Agent Credentials are stored unencrypted in the SIP message logs. Customer may elect to apply self-encrypting drive.

7. Third Party Service Providers (Sub-processors)

The Solution is not hosted or operated by Cisco. Accordingly, Cisco provides the Solution to Customer without sending personal data to any third-party service providers. If you choose to configure Context Service with the Solution, Cisco may share personal data with third party service providers. The Cisco Context Service Privacy Data Sheet describes such sharing of personal data with sub-processors and will be available on The Cisco Trust Center. If you choose an HCS-CC service provider to host and operate CCaaS, any or all of the information described in this Privacy Data Sheet will be accessible to such service provider.

8. Information Shared by Customer for Support

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 Solution. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data. Note that Cisco may share personal data received through TAC with development partners in order to provide diagnosis and resolution for your TAC request.

9. 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 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 leverages the following privacy transfer mechanisms related to the lawful use of data across jurisdictions:

- Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- EU Standard Contractual Clauses

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

- ISO 27001

10. General Information and GDPR FAQ

For more information related to the Solution's technical and operational security features, please see the Cisco Contact Center Enterprise Solution 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.