Privacy Factsheet

Avaya OneCloud CCaaS Public Omnichannel

(Document version 2.0, June 2021)

DISCLAIMER – the processing of personal data by CCaaS does not mean (by default) that Avaya (and/or its sub-processors) may have access to such data. Access control and use cases depend on the specific configuration/customization of CCaaS. This document is an overview of personal data processing activities within CCaaS, including, but not limiting to, privacy by design built-in tools and controls made available to protect personal data processed within CCaaS.

1. General Description of CCaaS

Avaya OneCloud CCaaS Public (Omnichannel) is a contact-center-as-a-service ("CCaaS") solution that provides a suite of capabilities to orchestrate, track, interact and report across voice and digital (email, chat and messaging) channels. It is built on an open, API-first architecture leveraging REST based API's for all capabilities to enable easy customization and integration into a CCaaS Customer's back/front office ecosystem.

CCaaS gives organizations the power to:

- Connect digital touchpoints throughout the entire customer journey — from email, messaging, chat, social, and the ability for organizations to Bring Your Own Channel ("BYOC").
- Intelligently match End-Users with the best Agents based on business rules, internal and external context and desired business outcomes.
- Personalize Agent experiences with a customizable, modern workspace that easily brings End-User insights from different applications and systems into a single pane of glass.
- Get ahead of every End-User interaction by predicting needs and proactively engaging End-User with journey intelligence.
- Quickly and easily layer-on innovative cloud technologies to deliver the exact experience that provides their End-Users more options, faster responses, and a more personalized approach.

Digital capabilities of CCaaS

For more information, please visit our website, review the Service Description and/or Service Catalog (the latter can be provided upon request).

2. Processing of Personal Data within CCaaS

The table below provides overview of the main personal data categories processed within CCaaS.

No.	Personal Data Category	General Description and Purpose	Personal Data Examples	Storage Location
1.	*"Sessions"*	Sessions hold context information about the End-User and the communication channel used by the End-User.	A Session entity contains identifiers that an external chat connector provides CCaaS with, e.g., chat account handle, name, unique user identifier, etc.	Microsoft's Azure datacenter
2.	*"Engagements"*	Engagements constitute a record of a contact initiated by an End-User and handled by contact center resources like Agents, Supervisors and Self-Service applications. A record of the Engagements of	An Engagement entity contains identifiers that an external chat connector provides CCaaS with, e.g., phone number, chat account handle, email, first and	Microsoft's Azure datacenter

		an End-User with the contact center is used by Agents to provide better End-User experience. It is also used by a Supervisor to keep track of Agent performance, carry out work assignment and other contact center operations.	last name, unique End-User identifier, etc.	
3.	*"End-User Identifiers"*	End-User Identifiers are bits of information that allow the contact center applications and Agents to uniquely identify an End-User. During an engagement, these identifiers are used to build a consolidated view (journey) of an End-User's interaction with the contact center across different channels, e.g. voice, chat, async messaging and email.	CCaaS has some out of the box End-User Identifiers, e.g., email address and phone number. It allows a CCaaS Customer to manage identifiers of its choice from CCaaS Application Center, e.g., social media handle, employee ID, etc.	Microsoft's Azure datacenter
4.	*"Transcripts"* and *"Messages"*	An End-User's engagement with CCaaS results in the exchange of many messages. A Message is the record of an email, text or media sent by an End-User and/or Agent. Many messages shared during a dialog are consolidated into a Transcript. Transcripts contain End-User identifiers that help associate messages to a rightful End-User. CCaaS stores the last 50 (fifty) messages shared during a dialog.	The message and / or transcript.	Microsoft's Azure datacenter and Smooch's datacenter (provisionally)

5.	*"Call Recordings"* (i.e., SIP and Media)	Recording of inbound and outbound voice calls and metadata associated with a call. This is used by Agent / Supervisor for playback and monitoring purposes.	The recording and associated metadata e.g. End-User's phone number).	Microsoft's Azure datacenter
6.	*"Screen Recordings"*	Recording of an Agent and Supervisor's actions on their desktop while an interaction with the End-User is in-progress. This is used by Agent / Supervisor for playback and monitoring purposes.	Screen content and associated metadata (e.g., phone number, chat handle, email address).	Microsoft's Azure datacenter
7.	*"Reports"*	CCaaS analytics application captures metrics related to Engagements, Agents and quality of service in CCaaS. This data shows up in real-time and historical Reports.	An engagement's sender and recipient information contain personal data (e.g., phone number, email address, chat handle, etc.). For an email engagement, the subject line is recorded and depending upon how the contact center is configured, it may contain personal data.	Microsoft's Azure datacenter
8.	*"User Accounts"*	Depending upon the role associated, an employee / associate of a CCaaS Customer assumes personas like Agent, Supervisor and Administrator.	CCaaS user object has the following personal data fields: first name, last name, email address (also used as username) and password.	Microsoft's Azure datacenter and Verint's datacenter
9.	*"Logs"*	CCaaS may generate application level logs that contain personal data. These logs are securely transmitted to the log destination and stored encrypted. Application	Application logs may contain End-User Identifiers used in Sessions, Engagements and Transcripts.	Datadog's datacenter

		logs are used to troubleshoot problems and ensure CCaaS functionality and performance.		

Note: the location of datacenters depend on the geographical location where the CCaaS Customer is based. For further reference please see the tables below:

Datacenter Location (Microsoft's Azure)	**Provides CCaaS services to CCaaS Customers in…**
United States of America	USA, Canada, Mexico
United Kingdom	UK, Ireland
Germany	Austria, Belgium, Czech Republic, Denmark, France, Germany, Greece, Hungary, Italy, Luxembourg, Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Saudi Arabia, Turkey, South Africa, Romania, Israel, Algeria, Egypt, Kuwait, Qatar, UAE
Brazil	Brazil, Argentina, Chile, Colombia, Costa Rica, Jamaica, Panama, Peru

In addition, in countries where data privacy laws and regulations require (Call and/or Screen) Recordings to be stored locally, CCaaS Customers have the choice to offload such recordings to a Customer's designated (i) storage facility or (ii) proxy cloud location. The foregoing options are custom and require CCaaS Customers to pay an extra fee to Avaya. The Administrator can create a request to Avaya via *Avaya OneCare portal* to initiate the change of the storage of the (Call and/or Screen) Recordings.

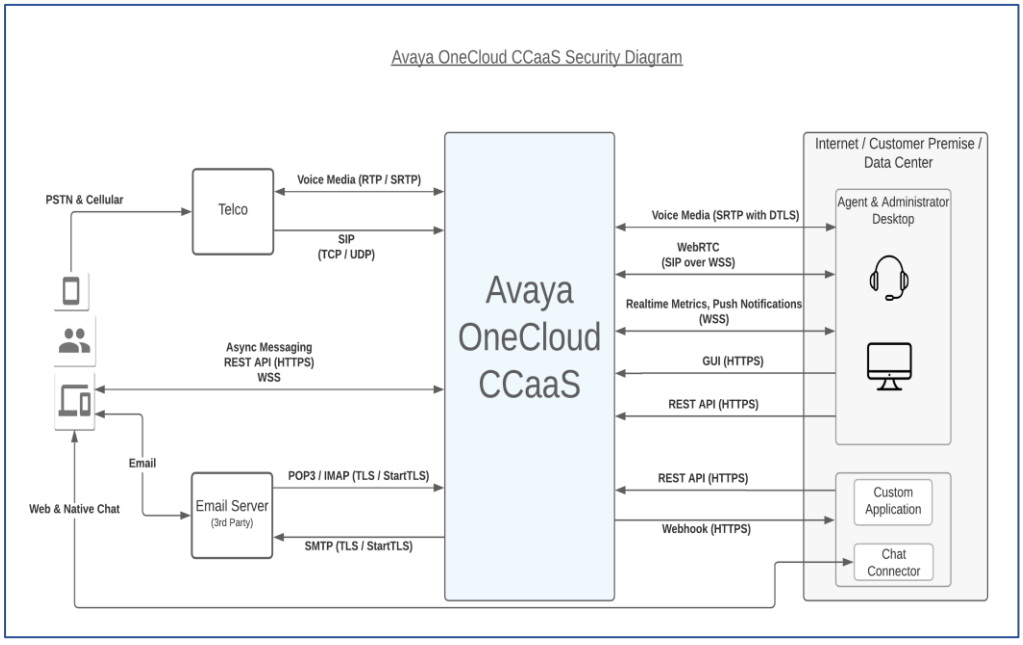
Datacenter Location (Verint) *WFO component*	**Provides CCaaS services to CCaaS Customers in…**
United States of America	USA, Canada, Mexico Brazil, Argentina, Chile, Colombia, Costa Rica, Jamaica, Panama, Peru
United Kingdom	UK, Ireland
Germany	Austria, Belgium, Czech Republic, Denmark, France, Germany, Greece, Hungary, Italy, Luxembourg, Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Saudi Arabia, Turkey, South Africa, Romania, Israel, Algeria, Egypt, Kuwait, Qatar, UAE

Datacenter Location (Smooch)	Provides CCaaS services to CCaaS Customers in…
United States of America	USA, Canada, Mexico, Brazil, Argentina, Chile, Colombia, Costa Rica, Jamaica, Panama, Peru
Ireland	Austria, Belgium, Czech Republic, Denmark, France, Germany, UK, Ireland, Greece, Hungary, Italy, Luxembourg, Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Saudi Arabia, Turkey, South Africa, Romania, Israel, Algeria, Egypt, Kuwait, Qatar, UAE

Datacenter Location (Datadog)	Provides CCaaS services to CCaaS Customers in…
United States of America	USA, Canada, Mexico, Brazil, Argentina, Chile, Colombia, Costa Rica, Jamaica, Panama, Peru, Austria, Belgium, Czech Republic, Denmark, France, Germany, Greece, Hungary, Italy, Luxembourg, Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Saudi Arabia, Turkey, South Africa, Romania, Israel, Algeria, Egypt, Kuwait, Qatar, UAE, UK, Ireland

3. Security Overview within CCaaS

The visual diagram below identifies the interfaces on which authorized users (e.g., Administrators, Agents, Supervisors) and external applications communicate with CCaaS. The sub-sections following this chart provide more details of the control measures employed by CCaaS to safeguard CCaaS Customer's data.



Encryption Controls

- All data at rest is encrypted by default by the cloud service provider (Azure - Microsoft Corporation). It uses AES 256-bit encryption.

- Confidential data such as passwords and secrets at rest is additionally encrypted using envelope encryption that employs a combination of AES 256-bit encryption and 2048-bit RSA asymmetric encryption.

- All data in transit over external and internal interfaces is secured using TLS protocol (version 1.2+). This applies to common protocols like HTTPS, WSS, POP3, IMAP and SMTP.

- Voice media can be encrypted using SRTP and SRTP with DTLS.

- X509 certificates issued by well-known Public CAs secure CCaaS's REST APIs, external interfaces and storage resources hosted by the cloud service provider (Azure - Microsoft Corporation).

Security Controls

- Edge security to protect CCaaS's external interfaces from DDoS attacks, bots, and other malware.
- Web application firewall with OWASP and managed rules sets to protect against existing and new web vulnerabilities.
- REST APIs and web-based portals (Workspaces Agent Desktop and Application Center) are the only external interfaces. All storage services are inaccessible from the external network. Restrictive network access control policies further limit access between applications and storage services.
- CCaaS uses cloud service provider's (Azure - Microsoft Corporation) recommended tools to manage the security posture and perform a regular threat analysis against its infrastructure.

4. Personal Data Human (Manual) Access Controls

- CCaaS leverages Microsoft's Azure automation capabilities to host and manage its resources. Access to these resources is restricted to a small number of Avaya cloud operations engineers.

- Avaya will not access CCaaS Customer's content data without permission from CCaaS Customer and only for specific contractual purposes.

- Access control measures in place include integration with Avaya IDP for SSO and MFA for authentication and RBAC enforced by CSP's IAM solution.

- Users accessing CCaaS web-based portals (Workspaces Agent Desktop and Application Center) are subjected to OIDC based authentication and RBAC enforced by CCaaS's IAM service.

    - Agents have access to CCaaS Workspaces Agent Desktop web-based portal. An Agent has access to chats, emails, transcripts, recordings, and engagements. These have personal data like an End-User's first and last name, email address, phone numbers, chat and social

media handles, and any other personal data an End-User shares with an Agent during a conversation.

- Supervisors have access to CCaaS Workspaces Agent Desktop and Application Center web-based portals. A Supervisor has access to chats, emails, transcripts, recordings, engagements in customer journey, real-time and historical reports. These have personal data like an End-User's first and last name, email address, phone numbers, chat and social media handles and any other personal data an End-User shares with an Agent during a conversation.

- Administrators have access to CCaaS Application Center web-based portal. They have access to CCaaS user accounts (e.g., Agent, Supervisor, etc.) and historical reports which have personal data like an End-User's first and last name, email address, phone number, chat and social media handles, and any other personal data an End-User shares with an agent during a conversation. Administrators can create, modify and/or delete Agent and Supervisor accounts.

- Authentication to CCaaS web-based portals (Workspaces Agent Desktop and Application Center) can be federated to CCaaS Customer's Enterprise IDP using SAMLv2.

5. Personal Data Programmatic (API) Access Controls

- CCaaS uses REST APIs to exchange data with its web-based portals and other authorized external applications. CCaaS web-based portals (Workspaces Agent Desktop and Application Center) and REST APIs are protected by CCaaS's IAM service that enforces authentication and authorization based on OAuth2 Access Tokens and RBAC.

- Refer to the CCaaS developer website to learn more about CCaaS APIs.

6. Personal Data Retention Period Controls

The table below provides personal data retention periods within CCaaS.

No.	Personal Data Category	Default Retention Period
1.	Sessions	Up to 24 hours
2.	Engagements	18 months
3.	End-User Identifiers	18 months
4.	Transcripts and Messages	18 months
5.	Call Recording (SIP and Media)	90 days*
6.	Screen Recording	90 days*
7.	Reports	12 months
8.	User Accounts	Until deleted by Administrator
9.	Logs	Up to 30 days

** The Administrator can reach out to CCaaS support team at Avaya by creating a service request via Avaya OneCare portal to request the change of the default retention period.*

7. Personal Data Export Controls and Procedures

The Administrator can create a request to Avaya via *Avaya OneCare portal* to export personal data.

8. Personal Data View, Modify, Delete Controls and Procedures

- Administrators, Supervisors and Agents have (view and/or modify) access to personal data described in Section 2. Access control for these users is implemented through measures set out in Section 4.

- The Administrator can create a service request via *Avaya OneCare portal* to delete personal data within Engagements, Transcripts, Messages, Call Recordings, Screen Recordings, and Contact Center Metrics. The request must contain one or more identifiers of the End-User whose personal data needs to be deleted.

- Depending on the category of personal data, it will be either deleted or anonymized. Transcripts, Messages and Logs are deleted/purged. End-User Identifiers and personal data within Engagements and metrics collected in analytics application are anonymized.

9. Privacy Features for Recording

- A record of End-User's interaction with CCaaS over digital channels is recorded in Transcripts and Messages.

- Controls to *start*, *stop*, *pause*, and *resume* screen and voice call recording can be customized across a CCaaS Customer's corporate account level or left down to Agents and/or Supervisors to implement controls. The Administrator can create a request to Avaya support team via *Avaya OneCare portal* for desired customization.

- It is the responsibility of CCaaS Customer to inform the End-User that a conversation/interaction will be recorded. This may be achieved through automated replies, automated applications, IVRs, manually by an Agent/Supervisor, etc.

10. Sub-Processors

The table below provides a list of Avaya's third-party sub-processors that process personal data within CCaaS. Section 2 above sets out where the personal data is hosted.

No.	Full Legal Name	Country of Incorporation	Service Description
1.	Microsoft Corporation	United States of America	Cloud service provider hosting CCaaS infrastructure.
2.	Verint Systems Inc.	United States of America	Cloud based service providing work force optimization ("WFO") and recording capabilities.
3.	Aiven Inc.	United States of America	Cloud based managed Database as a Service ("DaaS") provider.
4.	MicroStrategy Inc.	United States of America	Cloud based managed service that provides business intelligence capabilities.
5.	Smooch Technologies ULC (DBA Zendesk Inc.)	United States of America	Cloud based messaging platform.
6.	2600hz Inc.	United States of America	Managed cloud switch.
7.	Datadog Inc.	United States of America	Cloud Monitoring as a Service ("MaaS").

11. Usage Metering

CCaaS Customers are billed based on peak concurrent active users (e.g., Agents / Supervisors, etc.). CCaaS passes the "Usage Data" (as defined below) to Avaya's billing application for processing. Usage Data contains data such as the user's ID (generated by CCaaS when the user's account is created), login time, logout time and CCaaS bundle ID (digital/voice/omni) a user is associated to. Avaya will process such data as a Data Controller for billing purposes.

12. Definitions

No.	Term	Description
1.	Administrator	A CCaaS Customer's employee/associate specializing in contact center management. An Administrator uses CCaaS Application Center web-based portal to manage user accounts like Agents, Supervisors, and other contact center features.
2.	Application Center (portal)	Web-based application for Agents and Supervisors to carry out their responsibility in a contact center.

3.	AES	Advanced Encryption Standard is a symmetric block cipher used to encrypt sensitive data.
4.	Agent	A CCaaS Customer's employee/associate specializing in customer service. An Agent uses Workspaces Agent Desktop web-portal to handle End-User interaction with the contact center.
5.	CCaaS	Cloud based Contact Center as a Service.
6.	Contact Center Metrics	Metrics related to Engagements, Agents and quality of service in CCaaS.
7.	CSP	Microsoft Azure is the Cloud Service Provider hosting Avaya CCaaS.
8.	CCaaS Customer	An organization that has subscribed to CCaaS.
9.	DDoS	Distributed Denial of Service is a malicious attempt to disable a service's normal operation.
10.	DTLS	Datagram Transport Layer Security is a communications protocol that provides security for datagram-based applications by allowing them to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
11.	End-User	A data subject (likely a client of CCaaS Customer) interacting with contact center on voice and digital channels.
12.	HTTPS	Hypertext Transfer Protocol Secure used for secure communication over a computer network.
13.	IAM	Identity and Access Management service ensuring authorized access to CCaaS web-based portals, APIs, infrastructure, and platform resources.
14.	IDP	An Identity Provider is a service that stores and manages digital identities like user accounts and provides mechanism to verify identities through via protocols like SAMLv2.
15.	IMAP	Internet Message Access Protocol (IMAP) is a protocol used by email clients to retrieve email messages from a mail server.
16.	MFA	Multi Factor Authentication is an authentication process that requires the user to provide two or more verification factors.
17.	OAuth2	An industry standard protocol for authorization.
18.	OAuth2 Access Token	OAuth2 Access Token represents the authorization of a specific application to access specific parts of a user's data.

19.	OIDC	OpenID Connect is a browser-based workflow that standardizes user authentication process with an IDP or IAM service.
20.	OWASP	Open Web Application Security Project is an online community that produces freely available articles, methodologies, documentation, tools, and technologies in the field of web application security.
21.	POP3	Post Office Protocol 3 is a protocol used by email clients to retrieve email messages from a mail server.
22.	Public CA	Public Certificate Authority is a well-known and trusted organization that issues digital certificates.
23.	RBAC	Role Based Access Control is used in CCaaS to ensure authorized access to its web-portals, APIs, infrastructure, and platform resources.
24.	REST API	A REST API is an application programming interface (API) confirming to RESTful architecture style.
25.	RSA	Rivest, Shamir, and Adleman (RSA) is a public-key cryptosystem that is widely used for secure data transmission.
26.	SAMLv2	Security Assertion Markup Language 2.0 is a standard for exchanging authentication and authorization information between an IDP and applications that are also called service providers or relying parties.
27.	Self-Service application	Applications that carry out common and repetitive tasks in a contact center.
28.	SIP	The Session Initiation Protocol (SIP) is a signaling protocol used for initiating, maintaining, and terminating real-time voice calls in CCaaS.
29.	SMTP	Simple Mail Transfer Protocol is a standard protocol for sending emails.
30.	SRTP	Secure Real-time Transport Protocol is a profile for Real-time Transport Protocol intended to provide encryption, message authentication and integrity, and replay attack protection.
31.	SSO	Single sign-on is an authentication scheme that allows a user to log-in once and access other trusted services without re-entering authentication factors.
32.	Supervisor	A CCaaS Customer's employee/associate specializing in customer service. A Supervisor uses Workspaces Agent Desktop web-portal to monitor agent performance, resolve complaints and assign work.
33.	TLS	Transport Layer Security is a cryptographic protocol designed to provide communications security over a computer network.

34.	X509	X509 is a standard defining the format of public key certificates.
35.	Workspaces Agent Desktop (portal)	Web-based application for Agents and Supervisors to carry out their responsibility in a contact center.
36.	WSS	WebSocket Secure is a computer communications protocol designed over the HTTP protocol, to provide full duplex communication channels.

– END OF THE PRIVACY FACTSHEET –