Privacy Factsheet

Avaya OneCloud Private CCaaS

(Document version 1.0, September 2021)

DISCLAIMER – *the processing of certain 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 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. This Privacy Factsheet is intended for Avaya corporate customers only.*

1. General Description of the Product

Avaya OneCloud™ Private CCaaS is a private contact-center-as-a-service *("CCaaS")* that offers a hassle-free, always-on contact center that delivers a comprehensive, integrated, and open CCaaS architecture with scalability, security, and in-depth analytics across the customer journey, delivering a simple and flexible cloud experience. CCaaS enables customers to use voice and digital (short message service (*"SMS")/co-browse/email/chat*) interactions on a browser-based desktop.

For more information, please visit our website or review the Service Description which can be provided upon request to your Avaya sales representative.

2. Data Categories Containing Personal Data and Data Flow

2.1 Data Categories Containing Personal Data. CCaaS processes the following personal data as part of customer workflows, reporting, maintenance, and troubleshooting:

	Personal Data Category	General Description and Purpose	Personal Data Examples (Types)	Storage Location	Default Retention Period
1.	*"Sessions"*	Sessions hold context information about the End-User and the communication	A Session entity contains identifiers that an external chat connector provides CCaaS	**Avaya provided data center	90 days*

		channel used by the End-User.	with, e.g., chat account handle, name, unique user identifier, etc.		
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 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.	An Engagement entity contains identifiers that an external chat connector provides CCaaS with, e.g., phone number, chat account handle, email, first and last name, unique End-User identifier, etc.	eGain Datacenter - contact your Avaya Sales representative for applicable datacenter location..	90 days*
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	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	**Avaya provided data center	90 days*

		with the contact center across different channels, e.g. voice, chat, async messaging and email.	Center, e.g., social media handle, employee ID, etc.		
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.	The message and / or transcript.	**Avaya provided data center	90 days*
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	The recording and associated metadata e.g. End-User’s phone number).	**Avaya provided data center	90 days*

		monitoring purposes.			
6.	*"Screen Capture"*	The screen scraping functionality of AWFO Screen Capture captures the screens of the Agent.	Screen content and associated metadata (e.g., phone number, chat handle, email address).	**Avaya provided data center	90 days*
7.	*"User Accounts"*	Depending upon the role associated, an employee / associate of a CCaaS Customer assumes personas like Agent, Supervisor and Administrator.	CCaaS has artifacts store the following personal data fields: first name, last name, email address (also used as username).	**Avaya provided data center	90 days*
8.	*"Logs"*	CCaaS may generate application level logs that contain personal data. These logs are securely transmitted to the log destination and stored encrypted. Application logs are used to troubleshoot problems and ensure CCaaS functionality and performance.	Application logs may contain End-User Identifiers used in Sessions, Engagements and Transcripts.	**Avaya provided data center	30 days or 365 days for audit trails*

9.	*"Analytics"*	Digital Cloud Analytics provides digital reporting for insights into digital channel traffic and performance metrics of individuals, queues, and activities over specified time intervals.	Analytic reports may contain End User Identifiers used in in Sessions, Engagement and Transcripts.	**Avaya provided data center	30 days or 365 days for audit trail.*

* *The Administrator can create a request to Avaya via Avaya OneCare portal for additional options on keeping certain personal data for a different retention period.*

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

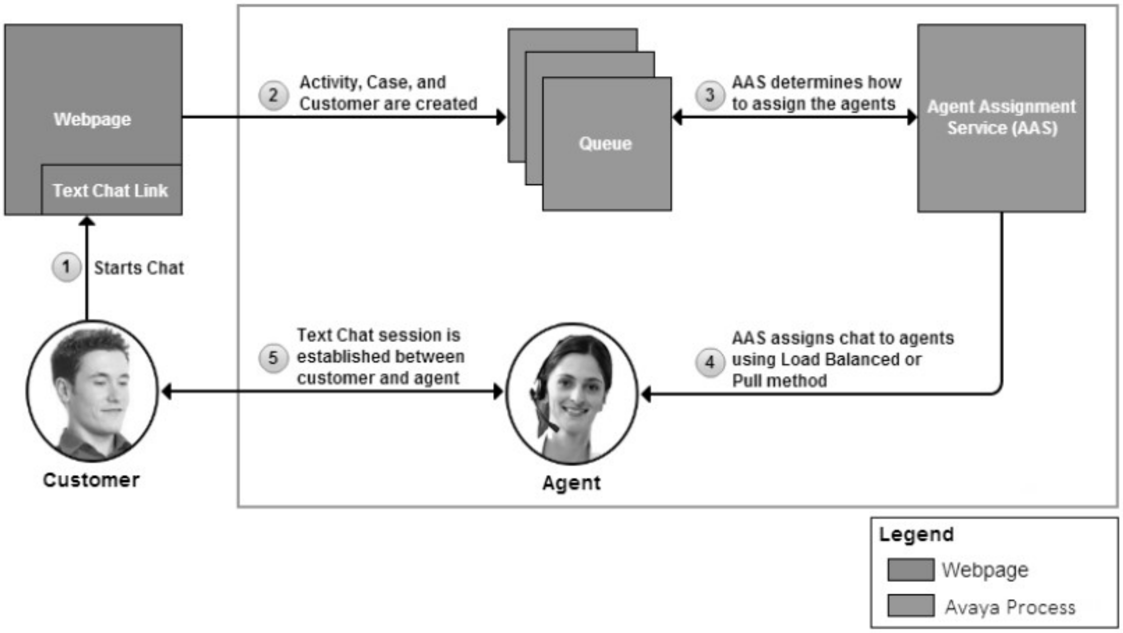
Datacenter Location	**Provides CCaaS services to CCaaS Customers in…**
United States of America	North or South America
United Kingdom	UK, Ireland
Germany	Austria, Belgium, Czech Republic, Denmark, France, Germany, Greece, Hungary, Italy, Luxembourg, Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Turkey, South Africa, Romania, Algeria, Egypt, UAE
Japan	Japan
Singapore	Australia, Hong Kong, Indonesia, Malaysia, Philippines, Singapore, South Korea, Taiwan, Thailand, New Zealand

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.

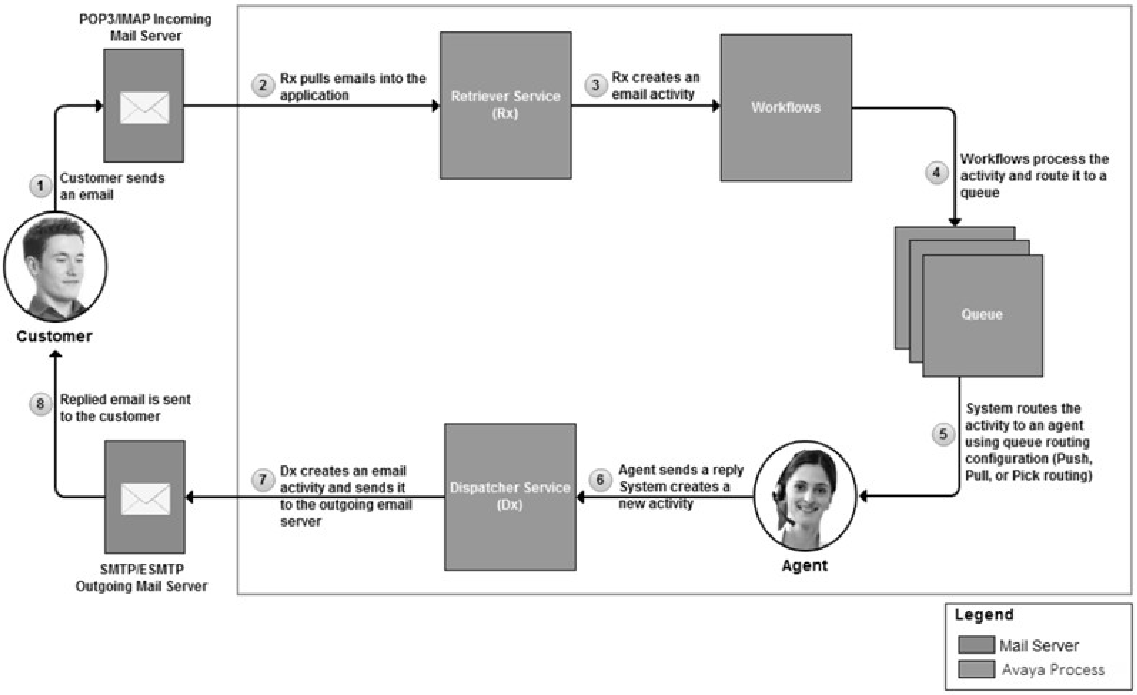
2.2 CCaaS Data Flow

The visual chart below provides a high-level overview of data flows in CCaaS.

CCaaS SMS data flow chart


Webpage
Text Chat Link
1 Starts Chat
2 Activity, Case, and Customer are created
Queue
3 AAS determines how to assign the agents
Agent Assignment Service (AAS)
4 AAS assigns chat to agents using Load Balanced or Pull method
5 Text Chat session is established between customer and agent
Customer
Agent
Legend
Webpage
Avaya Process

CCaaS email data flow chart


POP3/IMAP Incoming Mail Server
1 Customer sends an email
2 Rx pulls emails into the application
Retriever Service (Rx)
3 Rx creates an email activity
Workflows
4 Workflows process the activity and route it to a queue
Queue
5 System routes the activity to an agent using queue routing configuration (Push, Pull, or Pick routing)
Agent
6 Agent sends a reply System creates a new activity
Dispatcher Service (Dx)
7 Dx creates an email activity and sends it to the outgoing email server
SMTP/ESMTP Outgoing Mail Server
8 Replied email is sent to the customer
Customer
Legend
Mail Server
Avaya Process

3. Personal Data Human (Manual) Access Controls

Human access control is available through the *"Customer Admin Server"* which is an add on for the Admin Portal:

- Administrators can create and manage agents/supervisors through the Customer Admin Server; and
- Supervisors or Administrators can access user and agent data, reports, recordings, and screen capture through the Customer Admin Server.

4. Security and Personal Data Encryption Controls

Encryption Controls

Security and privacy are of primary importance to us. We have adopted a combination of security technologies (including encryption), technical measures, and organizational controls to protect personal data. CCaaS enforces strict security groups, identity access management policies, logging, and industry-standard encryption to secure the personal data *"at rest"* and *"in transit."*

- *"In-transit"* (i.e., transmission) connections are encrypted via Transport Layer Security ("***TSL***"), an encryption protocol intended to keep data secure when transferred over a network, at 1.2 or higher cryptographic protocols designed to provide communications security over a network. This includes the SIP telephony protocol, all media streams Secure Real-Time Transport Protocol ("***SRTP***") (which is an extension to Real Time Transport Protocol that incorporates enhanced security features), and web-based services. TLS certificates signed by a trusted party are used for data integrity and confidentiality.

- *"At rest"* (i.e., storage) all data which includes user data and voice metadata, emails, chat, SMS, MMS data, screen captures, call recordings, and logs are encrypted at rest.

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 recommended tools to manage the security posture and perform a regular threat analysis against its infrastructure.

Additionally, Avaya has security services (e.g. auditing, hardening, and integration) built into the CCaaS. The following highlights these security services.

Strict Access Control through authentication and authorization based on need-to-know/least-privilege principles are a key element to safeguard against non-privileged access. These principles are applied to all layers, from physical data center access up to application usage by end users and administrative services.

Firewalls, Session Border Controllers, Intrusion Detection and Prevention (IDP) systems inspect and control data access to the OneCloud Private. Centralized logging and Security Incident and Event Management (SIEM) systems complement the IT Security tools infrastructure providing audit insights and correlated alarming on security incidents.

All customer's applications connect to Avaya OneCloud Private cloud via reverse proxy. The architecture in the Service is a set of logically separate environments where all customer data, processing, and data transmission is separate from other customers. Each Customer environment (Customer Container) has a set of dedicated subnets:

Core: core application services.

Tools: infrastructures services; and

DMZ: internet facing services along with client application connectivity.

All subnets are segregated by firewalls and monitored by security tools to restrict inbound and outbound traffic.

Data Encryption in transit and at rest using strong protocol versions and cypher-suites are implemented to guard against loss in confidentiality. This applies to external user connections as well as to internal machine to machine communications and administrative access.

File Integrity Management (FIM) in combination with centralized logging and SIEM ensures that data is real and accurate.

Regular scanning for vulnerabilities, penetration tests, prompt system patching and more complete the technical security safeguards. Additionally, Avaya has implemented appropriate policies, procedures, and operational controls to maintain this level of security in Avaya OneCloud Private instantiations.

Contingency Plans for disaster recovery, emergency operations and testing support high cloud services availability even in crisis situations.

Change Management and Risk Management controls and audits user management and ensures that risk is minimized for customer data assets and the entire cloud solution are not exposed to any risk at any time.

Workforce security safeguards make sure that only those administrators have access to a customer environment who have a need to. Proper authentication through Multi-Factor-Authentication (MFA), compliance and data privacy trainings as well as detailed termination procedures and employee policies are just some of the personnel security safeguards in Avaya OneCloud Private.

5. Personal Data Export Controls and Procedures

Customer's Administrator may raise a service request to CCaaS service team at Avaya to request an export file via the AMSP customer portal using the link that your Avaya Service Delivery Manger (SDM) provides. AMSP provides authorized users the ability to create, view, and update work items that require Avaya engagement.

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

- Agents and supervisors can view and modify their first name, last name, address, email, and phone number in the Admin Portal and Admin Server Add-on.
- Administrators can view, modify the first name, last name, email, address, phone number of all agents and supervisors in the Admin Server Add-on.
- Administrators can request CCaaS support team at Avaya to delete other personal data (such as logs, screen captures, call recordings, and user interactions via SMS/MMS, email, chat) in the event the administrator is not able to do that because of technical limitations.

7. Indicators for call / video recording (Privacy Features for Call / Screen Recordings)

CCaaS provides features for customizable indicators (visible / audible) as a capability of the call recording and screen capture add-ons to. For more information visit Avaya Aura® Workforce Optimization Product Documents or contact your Avaya sales representative.

8. Logging and Accountability

An individual person may request a modification or change to their Personal Data within CCaaS by submitting a service ticket through the Avaya Manages Services Platform (AMSP), a moves, additions, changes, or deletions ("***MACD***") request, or alternatively the Customer's administrator has the ability to make changes and modification via the Admin Portal to Personal Data. For more information please visit Documentation Reference for Avaya OneCloud™ - Private Admin Portal or contact your Avaya sales representative.

9. CCaaS Components Management

9.1 CCaaS components managed by Avaya:

CCaaS components managed by Avaya are hosted in the Avaya provided data centers located – see Section 2 for more details.

9.2 CCaaS components managed by Avaya's sub-processors:

The full legal name of the sub-processor	Country of incorporation	Description of a managed component
eGain Corporation	United States	A cloud-based solution for routing digital channels (such as email, chat, SMS/MMS), administration, and data extract for analytics.
911 Secure LLC	United States	Sentry™ is a Service to address US Legislation Kari's Law and Tay Baum Act. The solution tracks the movement of hard and soft phones to provide the PSAP with a dispatchable End User location detail. Architected for high availability the service provided Customer with two notification options that a 911 evet is occurring. For more detail visit http://avaya.com/en/documents/fs-911-secure-ind15410en.pdf
Verint Systems Inc.	United States	Avaya Workforce Optimization (WFO) applications (i) encourage businesses to use their contact center strategically rather than just as a mechanism to field customer calls, (ii) helps business gain a deeper understanding of customer trends and balances efficiency with effectiveness to enable an optimized customer experience. For more detail visit http://avaya.com/en/documents/fs-avaya-wfo-cc15255en.pdf
Amazon Web Services Inc.	United States	AWS (Amazon Web Services) is a comprehensive, evolving cloud computing platform provided by Amazon that includes platform as a service (PaaS).

International Business Machines Corp.	United Stated	IBM PaaS provider, provides complete, flexible cloud platform for developing, running and managing applications.

– END OF THE PRIVACY FACTSHEET –