



Privacy Fact Sheet: Avaya Experience Platform

DISCLAIMER: The processing of personal data by Avaya Experience Platform 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 Avaya Experience Platform. This document is an overview of personal data processing activities within Avaya Experience Platform, including, but not limiting to, privacy by design built-in tools and controls made available to protect personal data processed within Avaya Experience Platform.

1. General Description of Avaya Experience Platform

Avaya Experience Platform is a contact-center-as-a-service 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 APIs for all capabilities to enable easy customization and integration into an Avaya Experience Platform Customer's back/front office ecosystem.

Avaya Experience Platform 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”). Regarding data privacy practices within BYOC, please review stand-alone Privacy Fact Sheet for Avaya Communication APIs.
- 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.

Avaya Experience Platform Capabilities



For more information, please visit avaya.com, review the [Service Description](#) and/or Service Catalog (the latter can be provided upon request).

2. Processing of Personal Data within Avaya Experience Platform

The table below provides overview of the main personal data categories processed within Avaya Experience Platform.

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 Avaya Experience Platform 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 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 Avaya Experience Platform with, e.g., phone number, chat account handle, email, first and last name, unique End-User identifier, etc.	Microsoft's Azure datacenter

No.	Personal Data Category	General Description and Purpose	Personal Data Examples	Storage Location
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.	Avaya Experience Platform has some out of the box End-User Identifiers, e.g., email address and phone number. It allows a Avaya Experience Platform Customer to manage identifiers of its choice from the Avaya Experience Platform Application Center, e.g., social media handle, employee ID, etc.	Microsoft's Azure datacenter (managed via Aiven Inc.)
4.	Transcripts and Messages	<p>An End-User's engagement with Avaya Experience Platform 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.</p> <p>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.</p> <p>Avaya Experience Platform stores the last 50 messages shared during a dialog.</p>	The message and / or transcript.	<p>Microsoft's Azure datacenter (managed via Aiven Inc.)</p> <p>and</p> <p>Smooch's datacenter (provisionally)</p>
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.	Screen content and associated metadata (e.g., phone number, chat handle, email address).	Microsoft's Azure datacenter (managed via Verint Systems Inc.)
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 (managed via Verint Systems Inc.)
7.	Reports	Avaya Experience Platform analytics application captures metrics related to Engagements, Agents and quality of service in Avaya Experience Platform. 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

No.	Personal Data Category	General Description and Purpose	Personal Data Examples	Storage Location
8.	User Accounts	Depending upon the role associated, an employee / associate of an Avaya Experience Platform Customer assumes personas like Agent, Supervisor and Administrator.	Avaya Experience Platform 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 Google's GCP datacenter and Verint's datacenter

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

Datacenter Location (Microsoft's Azure)	Provides Avaya Experience Platform services to Customers in...
United States of America	Bolivia, Canada, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Panama, Peru, Puerto Rico, United States of America
United Kingdom	United Kingdom, South Africa
Germany	Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Ghana, Greece, Hungary, Iceland, Ireland, Israel, Italy, Kenya, Kuwait, Latvia, Lithuania, Luxembourg, Malta, Morocco, Netherlands, Nigeria, Norway, Oman, Poland, Portugal, Qatar, Romania, Saudi Arabia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, United Arab Emirates, Uganda, Ukraine
Brazil	Argentina, Brazil, Chile, Uruguay
Singapore	Hong Kong, Indonesia, Japan, Malaysia, Philippines, Singapore, Sri Lanka, Taiwan, Thailand

Datacenter Location (Google's GCP)	Provides Avaya Experience Platform services to Customers in...
United States of America	Bolivia, Canada, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Panama, Peru, Puerto Rico, United States of America
United Kingdom	United Kingdom, South Africa
Germany	Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Ghana, Greece, Hungary, Iceland, Ireland, Israel, Italy, Kenya, Kuwait, Latvia, Lithuania, Luxembourg, Malta, Morocco, Netherlands, Nigeria, Norway, Oman, Poland, Portugal, Qatar, Romania, Saudi Arabia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, United Arab Emirates, Uganda, Ukraine
Brazil	Argentina, Brazil, Chile, Uruguay
Singapore	Hong Kong, Indonesia, Japan, Malaysia, Philippines, Singapore, Sri Lanka, Taiwan, Thailand

Verint Datacenter Location (Microsoft's Azure)	Provides Avaya Experience Platform services to Customers in...
Recorder and User Interface component	
United States of America	Bolivia, Canada, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Panama, Peru, Puerto Rico, United States of America
United Kingdom	United Kingdom, South Africa
Germany	Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Ghana, Greece, Hungary, Iceland, Ireland, Israel, Italy, Kenya, Kuwait, Latvia, Lithuania, Luxembourg, Malta, Morocco, Netherlands, Nigeria, Norway, Oman, Poland, Portugal, Qatar, Romania, Saudi Arabia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, United Arab Emirates, Uganda, Ukraine
Brazil	Argentina, Brazil, Chile
Singapore	Hong Kong, Indonesia, Japan, Malaysia, Philippines, Singapore, Sri Lanka, Taiwan, Thailand

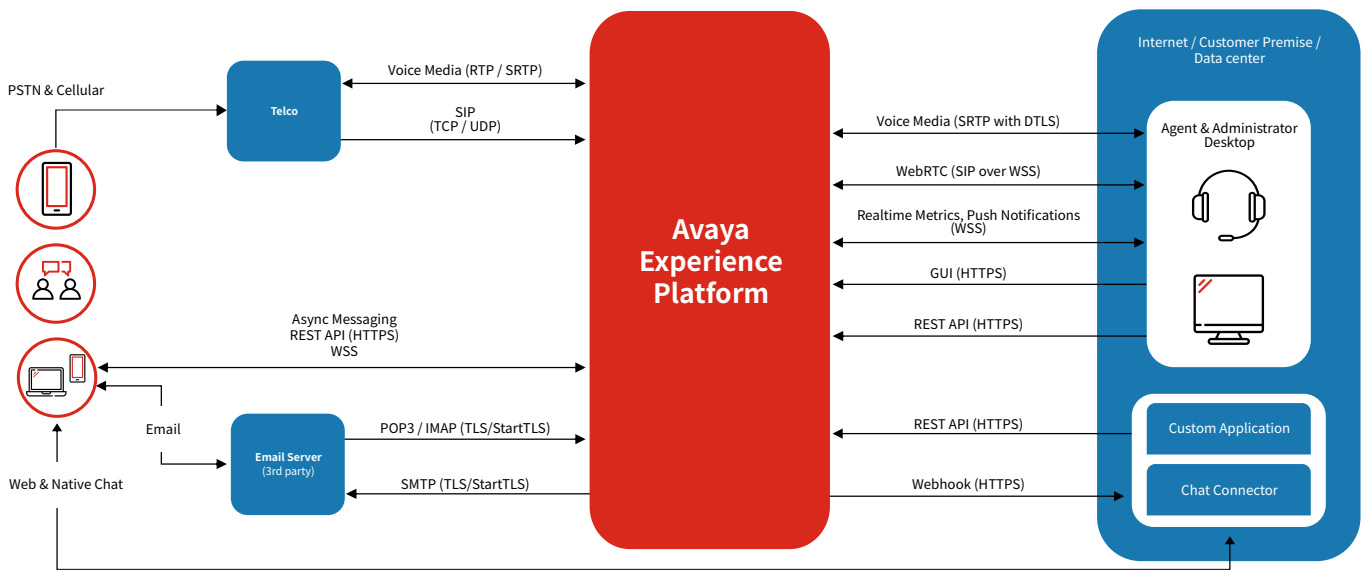
In addition to the above, in countries where data privacy laws and regulations require (Call and/or Screen) Recordings to be stored locally, Avaya Experience Platform Customers have the choice to offload such recordings to a Customer's designated (i) storage facility or (ii) proxy cloud location. The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

Datacenter Location (Smooch)	Provides Avaya Experience Platform services to Customers in...
United States of America	USA, Canada, Mexico, Brazil, Argentina, Colombia, Jamaica, Panama
Ireland	Austria, Belgium, Bahrain, Czech Republic, Denmark, France, Germany, Indonesia, Ireland, Japan, Greece, Hungary, Italy, Luxembourg, Malaysia, Nigeria, Netherlands, Norway, Poland, Portugal, Singapore, Spain, Sweden, Switzerland, Saudi Arabia, Turkey, South Africa, Romania, Israel, Kuwait, Qatar, Taiwan, Thailand, UAE, UK

Note: Smooch services are only offered on the countries listed above.

3. Security Overview within Avaya Experience Platform

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



Encryption Controls

- All data at rest is encrypted by default by the cloud service provider (Azure - Microsoft Corporation, GCP – Google Cloud Platform). 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 Avaya Experience Platform REST APIs, external interfaces and storage resources hosted by the cloud service provider (Azure - Microsoft Corporation).

Security Controls

- Edge security to protect Avaya Experience Platform 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 (Avaya 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.
- Avaya Experience Platform uses cloud service provider's (Azure - Microsoft Corporation, GCP – Google Cloud Platform) recommended tools to manage the security posture and perform a regular threat analysis against its infrastructure.

For more detailed security information, please review the Avaya Experience Platform Security Playbook which can be provided upon request to your Avaya sales representative.

4. Personal Data Human (Manual) Access Controls

- Avaya Experience Platform 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 Avaya Experience Platform Customer's content data without permission from Avaya Experience Platform 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 Avaya Experience Platform web-based portals (Workspaces Agent Desktop and Application Center) are subjected to OIDC based authentication and RBAC enforced by Avaya Experience Platform IAM service.
 - Agents have access to Avaya Experience Platform 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 Avaya Experience Platform 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 Avaya Experience Platform Application Center web-based portal. They have access to Avaya Experience Platform 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 Avaya Experience Platform web-based portals (Avaya Workspaces Agent Desktop and Application Center) can be federated to Avaya Experience Platform Customer's Enterprise IDP using SAMLv2.

5. Personal Data Programmatic (API) Access Controls

- Avaya Experience Platform uses REST APIs to exchange data with its web-based portals and other authorized external applications. Avaya Experience Platform web-based portals (Workspaces Agent Desktop and Application Center) and REST APIs are protected by Avaya Experience Platform IAM service that enforces authentication and authorization based on OAuth2 Access Tokens and RBAC.
- Refer to the Avaya Experience Platform developer [website](#) to learn more about Avaya Experience Platform APIs.

6. Personal Data Retention Period Controls

The table below provides personal data retention periods within Avaya Experience Platform.

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 Recordings (i.e., SIP and Media)	90 days
6.	Screen Capture	90 days
7.	Reports	12 months
8.	User Accounts	Until deleted by Administrator

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 Avaya Experience Platform 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 Avaya Experience Platform 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 Avaya Experience Platform 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

Please refer to the [Avaya Trust Center](#) for information on the sub-processors used to provide Avaya Experience Platform.

11. Usage Metering

Avaya Experience Platform Customers are billed based on peak concurrent active users (e.g., Agents / Supervisors, etc.). Avaya Experience Platform 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 Avaya Experience Platform when the user's account is created), login time, logout time and Avaya Experience Platform 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.	Full Legal Name	Country of Incorporation
1.	Administrator	An Avaya Experience Platform Customer's employee/associate specializing in contact center management. An Administrator uses Avaya Experience Platform 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	An Avaya Experience Platform Customer's employee/associate specializing in customer service. An Agent uses Avaya Workspaces Agent Desktop web portal to handle End-User interaction with the contact center.
5.	Avaya Experience Platform	Cloud-based Contact Center as a Service.
6.	Contact Center Metrics	Metrics related to Engagements, Agents and quality of service in Avaya Experience Platform.
7.	CSP	Microsoft Azure is the Cloud Service Provider hosting Avaya Avaya Experience Platform.
8.	Avaya Experience Platform Customer	An organization that has subscribed to Avaya Experience Platform.

No.	Full Legal Name	Country of Incorporation
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 Avaya Experience Platform 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 Avaya Experience Platform 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. Internet Message Access Protocol (IMAP) is a protocol used by email clients to retrieve email messages from a mail server.
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 Avaya Experience Platform 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) conforming to RESTful architecture style.
25	RSA	Rivest, Shamir, and Adleman (RSA) is a public-key cryptosystem that is widely used for secure data transmission.

No.	Full Legal Name	Country of Incorporation
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 Avaya Experience Platform.
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 Avaya Experience Platform Customer's employee/associate specializing in customer service. A Supervisor uses Avaya 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	Avaya 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.



About Avaya

Businesses are built by the experiences they provide, and every day millions of those experiences are delivered by Avaya Holdings Corp. (NYSE: AVYA). Avaya is shaping what's next for the future of work, with innovation and partnerships that deliver game-changing business benefits. Our cloud communications solutions and multi-cloud application ecosystem power personalized, intelligent, and effortless customer and employee experiences to help achieve strategic ambitions and desired outcomes. Together, we are committed to help grow your business by delivering Experiences that Matter. Learn more at www.avaya.com.