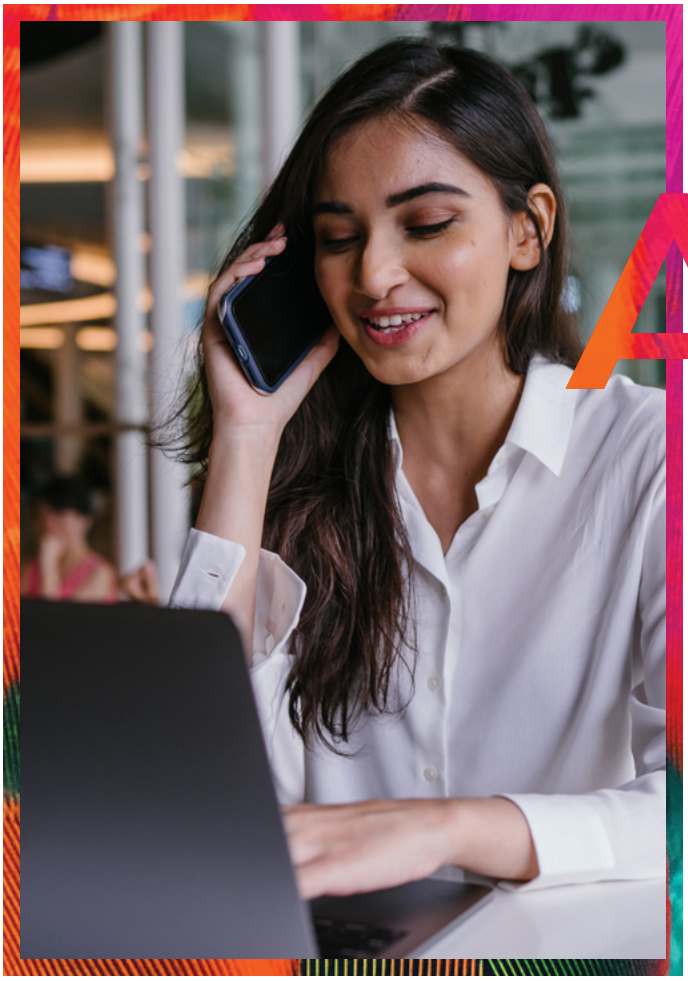

FACT SHEET

PRIVACY FACT SHEET: AVAYA EXPERIENCE PLATFORM™ PRIVATE CLOUD WITH AVAYA AURA® PRIVATE CLOUD

DISCLAIMER: the processing of Personal Data by Avaya Experience Platform™ (AXP) Private Cloud with Avaya Aura® Private Cloud ("Solution") 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 the Solution. This document is an overview of Personal Data processing activities within the Solution, including, but not limiting to, privacy by design built-in tools and controls made available to protect Personal Data processed within the Solution.

1. General Description of the Solution

AXP Private Cloud with Avaya Aura Private Cloud is a cloud Software-as-a-Service (SaaS) that offers a deployable accessible and flexible business communication solution (UC and CC) capable of accommodating remote and mobile employees delivering collaboration capabilities.

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

2. Processing of Personal Data within the Solution

- The Solution processes the following personal data as part of customer workflows, reporting, maintenance, and troubleshooting:

No.	Personal Data Category	General Description and Purpose	Personal Data Types (i.e., Examples)	Storage Location (Country)
1.	**End-User Identifiers**	End-User Identifiers are configuration items that allow the applications to uniquely identify a user (data subject). This data is required to allow the user to use the service.	Phone number (Extension), first- and last- name, physical location information, IP address, email address.	Microsoft Azure datacenter Verint Cloud in Amazon Web Services datacenter when Recording is used
2.	**Messages**	A data subject's engagement with UC results in the exchange of many messages. A Message is the record of a text or voicemail message sent by a data subject.	• Instant Messaging (IM) • Presence status (online, offline, busy, etc. when manually set by the user) • Voicemail Message. • Callback audio message	Microsoft Azure datacenter
3.	**Call history**	Hard and softphones store call history details in the ´Journal´.	Phone number (Extension), first- and last- name, external phone-numbers.	Microsoft Azure datacenter
4.	**Usage Metering**	Usage Metering reporting for billing purposes.	End User Identifiers (Extension, Agent ID) and usage related data: CC Agent login/-out timestamp, etc.	Amazon Web Services datacenter
5.	**Call Center Reporting**	CC Agent related data that reflects availability and performance.	Agent ID and name, multiple metrics like availability (time), calls received, answered, forwarded, etc.	Microsoft Azure datacenter Verint Cloud in Amazon Web Services datacenter when CC Workforce Management is used
6.	**Emergency location (US only)**	In addition to End-User Identifiers as configuration items that allow the applications to uniquely identify a user (data subject) there is location related information for emergency services support (E911).	MAC-address, location, date and time stamp of a 911 call and location information.	Microsoft Azure datacenter
7.	**Logs**	Operating system and application level logs that may contain personal data. These logs are securely transmitted to the log destination and stored encrypted. Application logs are used to troubleshoot problems and ensure Solution functionality and performance.	Application logs may contain data subject identifiers (see above).	Microsoft Azure datacenter

***Note:** the location of data centers depends on the geographical location where the UC/CC Customer is based. For further reference please see the tables below:

AXP Private Cloud with Avaya Aura Private Cloud services can be contracted in the following countries:

Data Center Location (Microsoft Azure)	Provides AXP Private Cloud with Avaya Aura Private Cloud Services to Customers in…
United States of America	Canada, Colombia, Costa Rica, El Salvador, Guatemala, Jamaica, Mexico, Panama, Peru, Puerto Rico, United States of America.
United Kingdom	United Kingdom, South Africa.
Germany	Austria, Belgium, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Greenland, Hungary, Iceland, Ireland, Italy, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Spain, Sweden, Switzerland, Turkey, United Arab Emirates.
Brazil	Argentina, Brazil, Chile.
Singapore	Australia, India, Japan, Malaysia, New Zealand, Philippines, Singapore, South Korea, Taiwan, Thailand.

3. Personal Data Retention Period Controls

No.	Personal Data Category	Default Retention Period
1.	**End-User Identifiers**	Until the earlier of: (i) manually deleted by Administrator or Avaya; or (ii) until the end of the Order Term.
2.	**Messages**	IM: 90 days Presence: 90 days Voicemail: 30 days Callback: 90 days
3.	**Call History (Journal)**	100 records (1 per voice-call).
4.	**Usage Metering**	7 years (financial data retention requirement)
5.	**Call Center Reporting**	1 year
6.	**Emergency location (US only)**	Until the earlier of: (i) manually deleted by Administrator or Avaya; or (ii) until the end of the Order Term.
7	**Logs**	Local logs on servers: 4 weeks Centralized security logs (audit logs and events): 2 years. Application and metrics logs: 60 days.

Any modifications to retention periods defaults must be mutually agreed to by the parties in writing.

4. Security Overview within the Solution

- **Security Controls:** Security and privacy are of primary importance. Avaya has adopted a combination of security technologies, technical measures, and organizational controls to protect personal data. Solution enforces strict security groups, identity access management policies, logging, and more:
  - Edge security to protect Solution's external interfaces from DoS/DDoS attacks, bots, and other malware.
  - Web application firewall with rules sets to protect against existing and new web vulnerabilities.
  - Solution uses cloud service provider's recommended tools to manage the security posture and perform a regular threat analysis against its infrastructure.
- **Encryption Controls:** Avaya uses industry-standard encryption to secure personal data "at rest" and "in transit."
  - "In-transit" (i.e., transmission) connections are encrypted via Transport Layer Security ("TLS"), an encryption protocol at version 1.2 or higher, designed to provide confidentiality and integrity for data transferred 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, chat, logs are encrypted at rest.
- Additionally, Avaya has security services (e.g. auditing, hardening, and integration) built into the Solution. 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 Solution. 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 applications connect to the cloud services via a 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 Corporate Customer environment has a set of dedicated subnets:
    - Core: core application services.
    - Services: 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.
  - **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 security safeguards. Additionally, Avaya has implemented appropriate policies, procedures, and operational controls to maintain this level of security in UC and CC instantiations.
  - **Contingency Plans** for emergency operations and testing support high availability cloud services 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 training, detailed termination procedures and employee policies are just some of the personnel security safeguards in the Solution.

5. Personal Data Human (Manual) Access Controls

- Administrative personnel access to the Solution components is strictly controlled and managed. A virtual desktop environment (VDI) is the only central entry point, requiring two-factor authentication. It serves as the administration gate to the customer environment. Centralized logging and screen recording ensure auditability of every action performed by administrators.
- Data subject access to their individual sensitive data depends on the data category:
  - Call history/Journal: Access to the journal is through either a hard phone or a softphone clients. Both clients require authentication. Personal journal data can be deleted by the end-user individually.
  - Instant Messaging content can be deleted by the user by closing the IM conversation. Presence status can be manually changed at any time.
  - Voicemail: Access to voicemails is by calling the voicemail service from either a hard phone or a softphone. Authentication is required on the voicemail system based on a PIN entered through DTMF digits. Voicemails can be individually deleted by the end-user.

6. Personal Data Export Controls and Procedures

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

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

- Customers can create a service request via Avaya OneCare portal to delete personal data.
- Depending on the category of personal data, it will be either deleted or anonymized. Messages and Logs are deleted/purged.
  - User data is not automatically anonymized or pseudonymized. If pseudonymization is desired, customers can request this via Avaya OneCare portal.

About Avaya

Businesses are built by the experiences they provide, and every day, millions of those experiences are delivered by Avaya. Organizations trust Avaya to provide innovative solutions for some of their most important ambitions and challenges, giving them the freedom to engage their customers and employees in ways that deliver the greatest business benefits.

Avaya contact center and communications solutions power immersive, personalized, and unforgettable customer experiences that drive business momentum. With the freedom to choose their journey, there's no limit to the experiences Avaya customers can create.

08/24 • UC15896EN-06