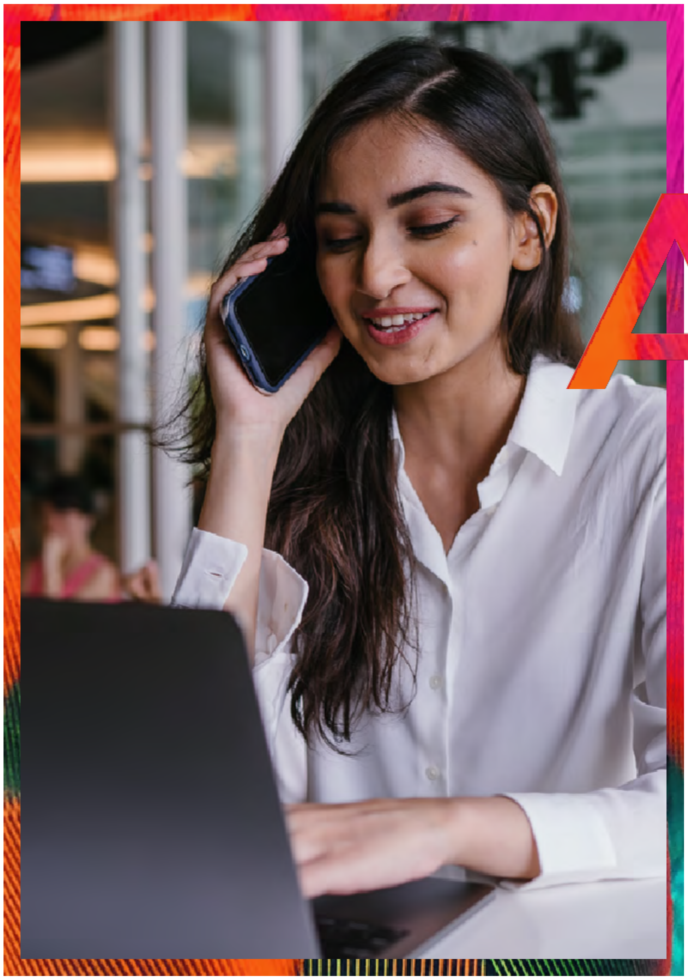

FACT SHEET

PRIVACY FACT SHEET: AXP ON-PREM

DISCLAIMER: the processing of Personal Data by Avaya Experience Platform ("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

Avaya Experience Platform On-Prem is an on-premise flexible business communication solution (UC and CC) which enables a reliable and integrated omnichannel contact center and contributes to rich and compelling customer and employee experiences.

For more information, please visit our website or contact 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.	Customer location
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.	Voicemail Message. Callback audio message	Customer location
3.	**Call history**	Hard and softphones store call history details.	Phone number (Extension), first- and last- name, external phone-numbers.	Customer location
4.	**Call Center Reporting**	Contact Center Agent related data that reflects availability and performance.	Agent ID and name, multiple metrics like availability (time), calls received, answered, forwarded, etc.	Customer location
5.	**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).	Customer location

3. Personal Data Retention Period Controls

It is the customer's responsibility to define and implement a data retention policy.

The product comprises a number of components which support data retention administrative tools for Logging and Call Data Records.

The Data Privacy Administrator may use the Log Storage Retention features to minimize log data storage.

The Log Retention Period time is programmable in units of days of storage. Saved log data would be deleted after this retention period is reached or if the configured storage capacity has been exceeded.

Log retention for Call Data Records (CDRs) within the Communication Manager solution component is configurable from 1 to 20 days.

Log retention within the Session Manager and System Manager solution components is configurable from 1 to 180 days with default 30 days. Please refer to these links for further information: CM GDPR AES GDPR SM GDPR SMGR GDPR

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.
- 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.

5. Personal Data Export Controls and Procedures

- The product will only collect and process data necessary to perform the purpose of the call processing and/or system diagnostics.
- The Data Privacy Administrator shall use the logging feature in a secure and careful fashion. Only those logs that are necessary for the maintenance of the product shall be used and shared with service providers.
- The product provides a special user group "datacontroller" which can only perform the changes related to log, trace retention and clear.

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

- Customers are responsible for processing Personal Data requests. The Data Privacy Administrator may fulfill requests by Data Subjects to review, change, or delete their personal data.

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.