Data Privacy Controls Addendum

This addendum applies to the Avaya Assistant application for Microsoft Teams.

The Avaya Assistant application is built on the Google Compute Engine. Personal Data is stored on the cloud back-end application and accessible by Avaya Assistant user in Microsoft Teams browser, desktop or mobile client.

- Personal Data required by the Cloud application, including access tokens for Avaya Spaces and Avaya Equinox Conferencing, is stored in encrypted storage via Google Compute Engine.
- Personal Data may be captured in application logs.

When Personal Data is being transmitted over a network, it is encrypted with the most up-to-date protocols.

Data Categories Containing Personal Data (PD)

- In Memory of Avaya Assistant server application.
  User Account Information: A Users name, email, authentication token retrieved from Avaya Equinox Conferencing Portal, authentication token retrieved from Avaya Spaces.

- Personal Data on disk
  User Account Information: A Users name, email, authentication token retrieved from Avaya Equinox Conferencing Portal, authentication token retrieved from Avaya Spaces.

- Application Logs generated by Avaya Assistant server application running on Google Cloud Platform.
  User Activities: Steps taken by Users as the interact with the function of the product (login, posting content, etc..) are regularly logged for performance and monitoring. These log files may contain Personal Data.
  User email address: The users email address is commonly used to correlate logs to Account information.
  User IP address: IP Addresses are often logged to correlate session activity

PD Human Access Controls

- Personal data may be displayed in UI.

PD Programmatic/API Access Controls

- None.

Avaya – Proprietary. Use pursuant to the terms of signed agreements or Avaya policy.

PD “at Rest” Encryption Controls

- Encryption controls for data stored on the Google Cloud are provided via Google storage services. All stored data is encrypted

PD “in Transit” Encryption Controls

- Data in transit encrypted via TLS, as negotiated with the server element. TLS 1.2 preferred

PD Retention Period Controls

- Authentication tokens are persisted, until directed by server the token is invalid.

PD Export Controls and Procedures

- Exporting of PD is not a function made available to User’s or Company Administrators. If an export is required for compliance purposes, contact Avaya’s data privacy officer.

PD View, Modify, Delete Controls and Procedures

- Configuration data may be purged with Reset Application action.

PD Pseudonymization Operations Statement

- None

Avaya – Proprietary. Use pursuant to the terms of signed agreements or Avaya policy.