Data Privacy Controls Addendum

This addendum applies to Avaya Aura Messaging, Version 7.x

Personal Data is stored in the database that is accessible only as a privileged system user.

Data Categories Containing Personal Data (PD)

Primary Category: User data (Name, Phone Number, preferred Messaging configuration options, etc) – Location: Database (OpenLDAP 2.4.40).

User media content (Voicemail messages and greetings) – Location: IMAP.

Secondary Category: Software Log files located in var/log/avaya directory

PD Human Access Controls

Human access to AAM product is role based via login/password. Login configuration is through the Administrator Accounts SMI Web page (HTTPS://<AAM_server>/cgi-bin/cm/secAdminAccnt/w_adminAccnt).

Documentation of the access levels can be found in “Administering Avaya Aura Messaging” guide located in https://downloads.avaya.com/css/P8/documents/101033961

Log files are located in the /var/log/avaya/mango(messaging) directories and accessible by administrators and privileged users as read only. Human access to these logs is via SSH, port 22.

PD Programmatic/API Access Controls

Programmatic access to PD is via TLS (encrypted) internal communication links to trusted sources only. Examples are Avaya clients such as the Avaya Web Client or 3rd Party clients like Mutare and Unimax and Starfish.

Programmatic access to log files is internal through an encrypted communication link.

PD “at Rest” Encryption Controls

If the AAM 7.x software is running on an Avaya provided HP DL360 G9 server with hard drive encryption enabled, then the entire hard drive and all its data is encrypted. If not using this server with encryption enabled, then:

User data: Only passwords are encrypted using 3DES algorithm.
Log files and User media content are not encrypted.

PD “in Transit” Encryption Controls

User data in transit occurs over a TLS encrypted link, so is always encrypted while “in transit”.

Port Matrix available at:

7.0 document:
https://downloads.avaya.com/css/appmanager/css/P8Secure/documents/101047408

7.1 document:
https://downloads.avaya.com/css/appmanager/css/P8Secure/documents/101047410

PD Retention Period Controls

AAM has no retention policy thus no automatic deletion of PD. Refer to ‘PD View, Modify, Delete Procedures’ below for manual delete procedure.
Log retention period cannot be configured. Only the Log size can be configured via the “log_size” CLI command.

PD Export Controls and Procedures

AAM does not provide an export capability for a single User’s contact data.
There’s no single-user export from the debug or application log files.

PD View, Modify, Delete Controls and Procedures

View, Modify and Deletion of PD is a manual task. User data can be modified through Admin web pages (SMI). This can also be done through the SMGR Messaging Admin Web page SMGR Messaging Element Manager administration Web page

PD Pseudonymization Operations Statement

NA