Data Privacy Controls Addendum

This addendum applies to Avaya IX Client SDK Communication Services Package (JavaScript), version 4.4, and later. The JavaScript Client SDK is not a standalone application, but a software component that can be used to build a JavaScript browser application that interacts with Avaya network components and services.

Personal Data is not stored on the browser. Session data is retained in browser cookie storage and/or browser storage that is accessible by the current user. Browser storage content is typically encrypted by the browser. Personal data within the Browser is not encrypted. Browser cookie storage is secured by the browser and/or the platform and stored on disk. When Personal Data is being transmitted over a network, it is encrypted with the most up-to-date protocols. Avaya recommends disk encryption using vendor or third-party disk encryption technologies.

Data Categories Containing Personal Data (PD)

User data (in memory)

- Calls: Remote party phone number
- Conference calls: participant display name, roster list, active talker
- AMM messages: participants on conversation(s), messages
- End user preferences information
- Configuration information
- Contacts retrieved from network (and local contacts application on mobile platforms)

User data (on disk)

- No user data is stored on disk.
- No user data is stored in browser storage.

User data (logs)

- Logs are stored in memory. User data is pseudonymized prior to sending to the log stream.

PD Human Access Controls

User data (in memory)

- None.

User data (on disk)

- None.

User data (logs)

- Controlled via JavaScript Client SDK Application, or by direction of network element (remote administrative).

PD Programmatic/API Access Controls

User data (in memory)

- Internal programmatic access.
- Browser debug tools.

User data (on disk)

- Controlled via Browser management operations.

User data (logs)

- None

PD “at Rest” Encryption Controls

User data (in memory)

- Not encrypted

User data (on disk)

- None.

User data (logs)

- None.

PD “in Transit” Encryption Controls

User data (in memory)

- HTTPs/TLS 1.2 to send/receive data with servers

User data (on disk)

- None.

User data (logs)

- None.

PD Retention Period Controls

User data (in memory)

- In-memory data is removed based on use cases. For example, during a call, a call object remains in memory. When the call ends, the object is removed from memory.

User data (on disk)

- None.

User data (logs)

- Responsibility of the JavaScript Application.

PD Export Controls and Procedures

User data (in memory)

- Not applicable.

User data (on disk)

- Not Applicable.

User data (logs)

- Not Applicable.

PD View, Modify, Delete Controls and Procedures

User data (in memory)

- Not applicable.

User data (on disk)

- Not Applicable.

User data (logs)

- Not Applicable.

PD Pseudonymization Operations Statement

User data (in memory)

- None

User data (on disk)

- None

User data (logs)

- User Addresses, phone numbers, and IDs (handles) are removed prior to logging.