Product Privacy Statement

Avaya Contact Analyzer

(version 1.0, dated 2019-12-07)

DISCLAIMER – the processing of certain Personal Data by Avaya Product does not mean (by default) that Avaya (and/or its sub-processors) may have access to such data. Exact access control and use cases depend on the respective Avaya Product and its specific configuration. This document does not cover the foregoing. The intent of this Product Privacy Statement is to provide overview of built-in tools and controls made available for the protection of Personal Data processed by Avaya Products.

1. General Description of the Product.

Contact centers, by their nature, create vast amounts of customer data – a potential goldmine of intelligence and insights that can be mined to optimize contact center performance while building customer loyalty and creating competitive advantage. Avaya Contact Analyzer provides flexible, customizable reporting at a unique level of granularity that facilitates understanding of any individual transaction as a complement to the summary view of overall performance that is available Avaya's Call Management System (CMS).

Avaya Contact Analyzer uses CMS External Call History (detailed call data) to deliver insights into many aspects of Contact Center performance beyond what can be gained at the summary level. Contact Analyzer can help Contact Center and business managers improve agent performance by providing quantifiable feedback. Knowledge gained, and actions taken can increase customer satisfaction and loyalty by providing insights into common customer complaints, abandon trends and other usage patterns. Furthermore, such insights allow for improvements in business policies and routing processes, a win-win for companies and customers alike.

2. Data Categories Containing Personal Data.

Contact Analyzer is an application that is intended to be used by data analysts to report on External Call History (ECH) call details from the Avaya Call Management System (CMS). This ECH data is transmitted securely from CMS server(s) via Secure File Transfer Protocol (SFTP) to ensure data is encrypted in transit.

Contact Center Agent Information:

- Contact Analyzer stores agent information in the form of temporary ECH files and long-term database storage in the Postgres database.
- The personal data is only for employees of the company utilizing CMS.
- The type of personal data is limited to only that information that will facilitate standard employee work operations (such as name, login ID, extensions, and telephone numbers).
- The ECH files are located on the filesystem in /opt/Avaya/CA/ech/ech_data.
- The Postgres database is in /opt/PostgreSQL

- This information will be stored in the Postgres database in the agendim table.

User to User Information (UUI):

- If configured/modified by the customer, UUI can be stored in an External Call History record.
- By default, there is no UUI in ECH records, but a customer could create a custom application to store any information (limited to 192 characters) in this field. Avaya recommends not storing any PD in this field.
- If UUI is collected, it will be stored in the Postgres database in the callsegmentfact table.

Automatic Number Identification (ANI) and Dialed Number Identification Service (DNIS) Information:

- External Call History could also store ANI and DNIS information depending on how the dial-plan and call routing is configured.
- If ANI or DNIS information is collected, it will be stored in the Postgres database in the callsegmentfact table.

3. Personal Data Human (Manual) Access Controls.

Personal data is accessible through the CA User Console using controlled user logins.

The root and postgres users also have access via a terminal emulator from the UNIX command line interface.

4. Personal Data Programmatic (API) Access Controls.

There are no programmatic or API access controls enabled in Contract Analyzer by default and no remote access to such items.

Postgres can be configured for remote ODBC access. If this is done, Avaya recommends using secure ODBC.

5. Personal Data “at Rest” Encryption Controls.

The PD in Contact Analyzer is not encrypted at rest when stored in the Postgres database. Linux permissions and access controls are enforced, ensuring that only the postgres and root user have access to these filesystems.

Customers provide the Operating System (OS) for Contact Analyzer and it is recommended that the customer encrypt filesystems where Personal Data will be stored if there is concern that a physical compromise of the server or hard drives may occur.

ECH data files are temporarily stored on the OS filesystem with appropriate permissions so only the root and avaya users have access.

Temporary files and permanent Postgres database data are stored in the /opt filesystem.

6. Personal Data “in Transit” Encryption Controls.

The following is the encryption used for PD in transit:

- File transfer

    - SSHv2 and SFTP

- Admin and User Console access
    - TLS 1.2 and HTTPS

7. Personal Data Retention Period Controls.

PD retention is controlled by two methods:

- Long-term database storage.
    - The Postgres database is configured by default to store 365 days of Call Center data.
    - This can be adjusted by editing the /opt/Avaya/CA/biserver-ce/pentaho-solutions/avaya-utils/utilities/variables.xml file and changing the retention_days variable.

- Temporary ECH file storage.
    - By default, ECH data files are stored for 90 days. These transient data files are compressed and archived after the data is successfully imported. Permissions are set so that only the root and avaya user has access to these files.
    - The retention period can be adjusted by editing the /opt/Avaya/CA/biserver-ce/pentaho-solutions/avaya-utils/utilities/load_ech.sh file and changing the DAYS2SAVE variable.

Log files may contain debugging information, only when this is enabled for troubleshooting purposes.

8. Personal Data Export Controls and Procedures.

CA does not have any standard product operations that allow export of personal data.

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

Only the root and avaya users have access to view, modify, and delete any of this temporarily stored data via UNIX terminal emulator.

If necessary, the customer can log in as the root or avaya user and delete logs from the log directories in the /opt/Avaya/CA folder.

ECH data files can also be manually removed from the /opt/Avaya/CA/ech/ech_data folder as the root or avaya user.

Long-term storage of PD data in the Postgres database can be removed using standard Postgres tools (like psql) and SQL queries.

- END OF THE PRODUCT PRIVACY STATEMENT –