



PRIVACY FACT SHEET: AVAYA COMMUNICATIONS APIs

DISCLAIMER: the processing of personal data by Avaya Communications APIs 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 Avaya Communications APIs. This document is an overview of personal data essential processing activities within Avaya Communications APIs, including, but not limiting to, privacy by design built-in tools and controls made available to protect personal data being processed within Avaya Communications APIs.

1. General Description of Avaya Communications APIs

Avaya Communications APIs enables businesses to integrate communications capabilities quickly and easily like voice, video, and messaging into their own applications without needing to build backend infrastructure and interfaces.

Solutions can be personalized and set up in only a few days and can be deployed on top of any existing communications infrastructure which is already in place.

Avaya Communications APIs has the following core features:

- Enable access to SIP Trunking for PSTN telephony services (see [Service Description](#) for more information)
- Provide a full Application Programming Interface (API) platform to create applications that can integrate with existing systems/services (see [Service Description](#) for more information)
- Support third-party SIP Trunking integration (BYOC) with the same capabilities as with Avaya SIP Trunking (see [Service Description](#) for more information)

For offer information on our Avaya Communications APIs, please visit our [website](#).

2. Processing of Personal Data within Avaya Communications APIs

The table below provides an overview of personal data categories processed within Avaya Communications APIs .

| No. | Personal Data Category | General Description and Purpose | Personal Data Examples | Storage Location |
|-----|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| 1. | Account Holder Identifiers | Account Holder Identifiers are bits of information that uniquely identify an account on the system | Email address, phone number, E911 address, employee ID, etc. | Google Cloud Platform |
| 2. | Account Identity | Account Identity data is required by each telco provider to obtain and access numbers | Account Identity data can be, but is not limited to ID card, passport, copy of utility bill, etc. | ServiceNow |
| 3. | CDR | Call detail records of inbound and outbound voice calls and metadata associated with a call | Contains time, duration, completion status, source number, destination number, etc. | Google Cloud Platform |
| 4. | E911 Addresses | Information associated to a number to be sent to upstream carrier when dialing 911 or 112 | User address information | Google Cloud Platform |
| 5. | Logs | Avaya OneCloud CPaaS may generate application-level logs that contain personal data. These logs are securely transmitted to the log destination and stored encrypted. Application logs are used to troubleshoot problems and ensure Avaya OneCloud CPaaS functionality and performance | Application logs may contain customer's identifiers used in sessions, engagements and transcripts | Datadog |
| 6. | Lookups | Data kept for caching purposes | CNAM, BNA, Caller ID | Google Cloud Platform |
| 7. | Call Recordings | The call recording is consolidated into a transcript using Avaya OneCloud CPaaS APIs for customer's consumption | Full call recording transcription | Google Cloud Platform and Amazon Web Services |
| 8. | Traffic | Inbound and outbound | The call signaling traffic, API calls, call logs, SMS/MMS (including source, destination and content) and usage history | Google Cloud Platform and Amazon Web Services |

Avaya Communications APIs enables businesses to integrate communications capabilities quickly and easily like voice, video, and messaging into their own applications without needing to build backend infrastructure and interfaces.



Note: the location of datacenters is based on the geographical location where the Customer is based. For further reference please see the tables below:

| Datacenter Location (ServiceNow) | Provides Avaya OneCloud CPaaS services to Customers in... |
|-----------------------------------------|------------------------------------------------------------------|
| United States of America | Worldwide |

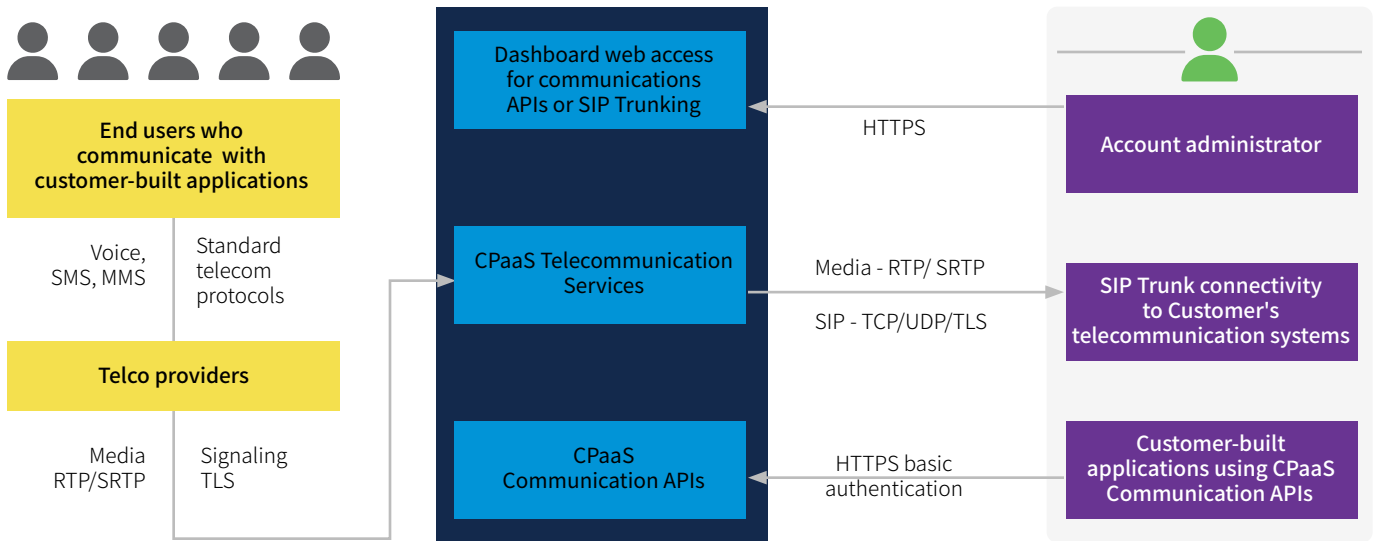
| Datacenter Location (Amazon Web Services) | Provides Avaya OneCloud CPaaS services to Customers in... |
|--------------------------------------------------|------------------------------------------------------------------|
| United States of America | USA, Canada, Puerto Rico |

| Datacenter Location (Google Cloud Platform) | Provides Avaya OneCloud CPaaS services to Customers in... |
|----------------------------------------------------|------------------------------------------------------------------|
| United States of America | USA, Canada, Puerto Rico |
| Germany | UK, Ireland, France, Netherlands, Portugal, Belgium, Italy |
| Singapore | Singapore, Australia |
| Brazil | Brazil |

| Datacenter Location (Datadog) | Provides Avaya OneCloud CPaaS services to Customers in... |
|--------------------------------------|------------------------------------------------------------------|
| United States of America | Worldwide |

3. Security Overview within Avaya Communications APIs

The visual diagram below identifies the interfaces in which authorized users and external applications communicate with Avaya Communications APIs. The sub-sections following this chart provide more details of the control measures used to safeguard customers' data.



Encryption Controls

- All personal data at rest uses RDS encryption by default and is stored on Amazon's S3 cloud. It uses AES 256-bit encryption.
- Confidential data such as passwords and secrets at rest is additionally encrypted using envelope encryption that employs a combination of AES 256-bit encryption and 2048-bit RSA asymmetric encryption.
- All data in transit over external and internal interfaces is secured using TLS protocol (version 1.2+). This applies to common protocols like HTTPS, WSS, POP3, IMAP and SMTP.
- For services consumed by dialing from the PSTN, Avaya Communications APIs can offer TLS encryption, however it is depending on the primary carrier and Avaya cannot guarantee end-to-end encryption of the voice / signaling path across all global service provider networks.

- Voice media encryption using RTP and SRTP with DTLS.
- X509 certificates issued by well-known Public CAs secure Avaya Communications APIs, external interfaces and storage resources hosted by the cloud service provider.

Security Controls

- Edge security to protect Avaya Communications APIs external interfaces from DDoS attacks, bots, and other malware.
- Web application firewall with OWASP and managed rules sets to protect against existing and new web vulnerabilities.
- All storage services are inaccessible from the external network. Restrictive network access control policies further limit access between applications and storage services.

Avaya will not access Avaya Communications APIs customers' content data without permission from the customer and only for the purposes set out in the underlying customer agreement.

4. Personal Data Human (Manual) Access Controls

- Avaya Communications APIs leverages industry best practices to host and manage its resources. Access to these resources is restricted to a small number of Avaya cloud operations engineers. Our processes are designed to achieve security and compliance certifications.
- Avaya will not access Avaya Communications APIs customers' content data without permission from the customer and only for the purposes set out in the underlying customer agreement.
- Access control measures in place include integration with Avaya MFA, when configured, for account holder authentication.
 - The Account Holder has access to the Avaya Communications APIs web-based dashboard containing access to CDRs, the account's SMS messages, platform notifications, recordings, transcriptions and usage history.

5. Personal Data Programmatic (API) Access Controls

- Avaya Communications APIs uses REST APIs to exchange data with its web-based portals and other authorized external applications. Avaya Communications APIs provides access to account data using a combination of Account ID and token pair to access account data using the API.
- Please refer to the [developer website](#) to learn more about Avaya Communications APIs.

6. Personal Data Retention Period Controls

The table below provides personal data retention periods within Avaya Communications APIs.

| No. | Personal Data Category | Default Retention Period* |
|-----|----------------------------|---------------------------------------------------------------------------------------------------------------------|
| 1. | Account Holder Identifiers | Per subscription term |
| 2. | Account Identity | Until the account is active on Avaya OneCloud CPaaS platform or needed for regulatory purposes, whichever is longer |
| 3. | CDR | 18 months |
| 4. | E911 Addresses | Per subscription term |
| 5. | Logs | 30 days |
| 6. | Lookups | 30 days |
| 7. | Call Recordings | 30 days |
| 8. | Traffic | 30 days |

* The Account Holder can reach out to Avaya by creating a service request via the Avaya OneCare portal to request a change of the default retention period.

7. Personal Data Export Controls and Procedures

Account holders can download .csv files of traffic data and/or data generated from API requests from the Avaya Communications APIs dashboard.

Account holders can also create a request to Avaya via Avaya OneCare portal if additional exports are needed.

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

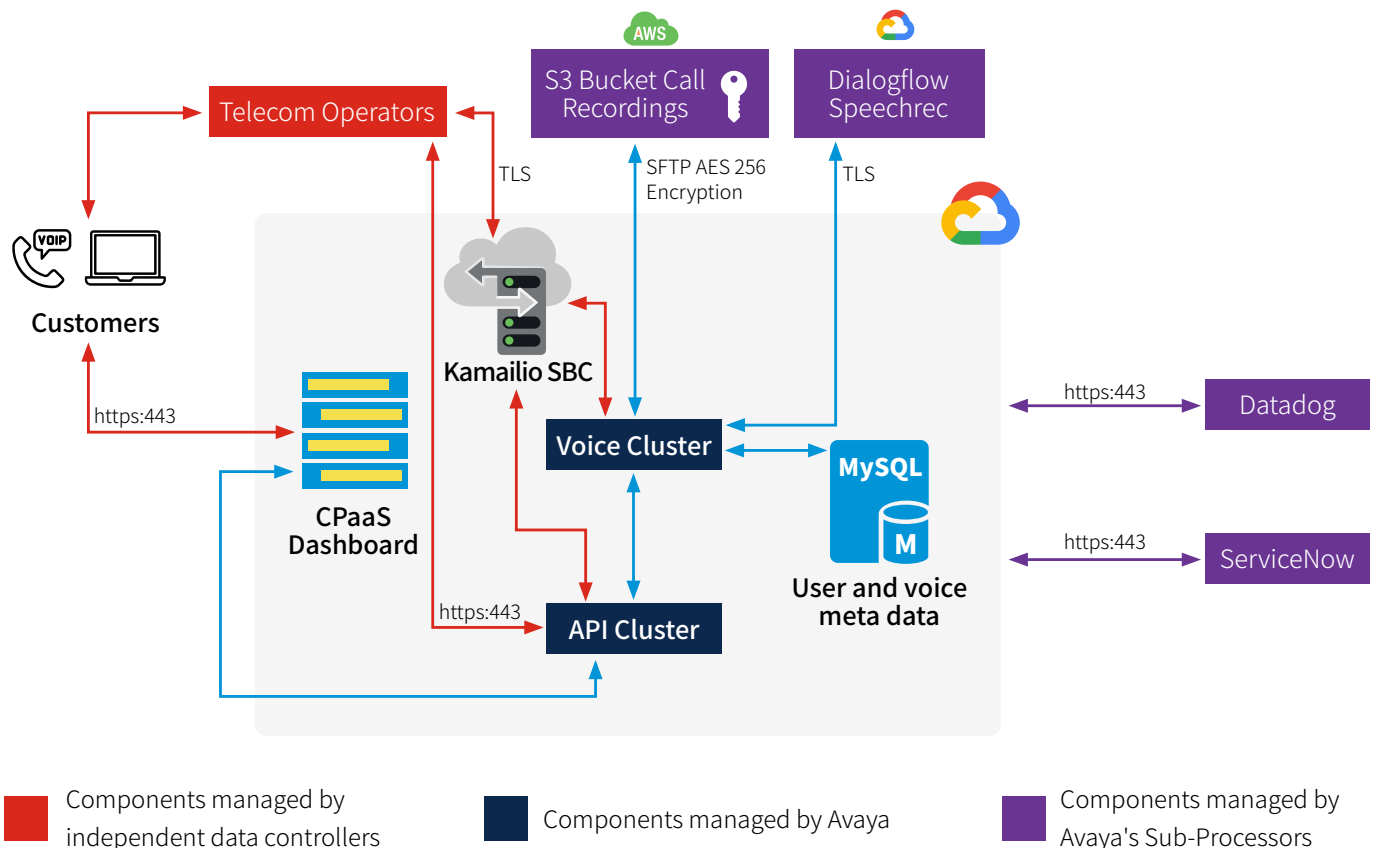
- Account holders have (view and/or modify) access to the personal data described in Section 2. Access control for

these users is implemented through the measures set out in Sections 4 and 5.

- The account holder can create a service request via the Avaya OneCare portal to delete personal data within Logs, Call Recordings, and Usage Metrics.
 - The request must contain one or more identifiers of the data subject whose personal data needs to be deleted.
 - Depending on the category of personal data, it will be either deleted or anonymized. Call Recordings, Messages and Logs are deleted/purged. End-User Identifiers and personal data within Engagements and metrics collected in the analytics application are anonymized.

9. Avaya Communications APIs Components and Data Flow

The visual below provides a high-level overview of the data flows in Avaya Communications APIs.



Solutions can be personalized and set up in only a few days and can be deployed on top of any existing communications infrastructure which is already in place.



Avaya Communications APIs Components managed by Avaya:

Avaya Communications APIs: Customers can connect to the Avaya Communications APIs dashboard through a web browser and navigate to add funds, purchase numbers and access APIs

Voice Cluster: SIP media server that facilitates IVR and API functionality for all traffic (calls, SMS, MMS)

API Cluster: Rest API services and functional microservices housing all business logic and recordings

SBC Cluster: Session border control (SBC) layer is the interface for calls into Avaya Communications APIs

Please refer to the [Avaya Trust Center](#) for information on the sub-processors used to provide Avaya Communications APIs.

10. Usage Metering

Avaya Communications APIs customers are billed for the numbers used for calling, messaging and services such as recording and transcription. The quantity of the services consumed depend on the application created using Avaya Communications APIs. Usage Data contains data such as the user's ID (generated when the user's account is created), login time, logout time. Avaya will process such data for billing purposes.

11. Definitions

| No. | Term | Description |
|-----|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Account Holder | An Administrator using the Avaya Communications APIs web-based portal to manage accounts, order numbers, download data and access APIs |
| 2 | CNAM | Caller Name Delivery |
| 3 | BNA | Backbone Network Architecture |
| 4 | Avaya Communications APIs Dashboard | Web-based application for account holder to manage number and services |
| 5 | AES | Advanced Encryption Standard is a symmetric block cipher used to encrypt sensitive data |
| 6 | DDoS | Distributed Denial of Service is a malicious attempt to disable a service's normal operation |
| 7 | DTLS | Datagram Transport Layer Security is a communications protocol that provides security for datagram-based applications by allowing them to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery |
| 8 | E911 | A system used to provide the caller's location to PSAP dispatchers. |
| 9 | HTTPS | Hypertext Transfer Protocol Secure used for secure communication over a computer network |
| 10 | IMAP | Internet Message Access Protocol (IMAP) is a protocol used by email clients to retrieve email messages from a mail server |
| 11 | MFA | Multi Factor Authentication is an authentication process that requires the user to provide two or more verification factors |
| 12 | MMS | Multimedia messaging service |
| 13 | OWASP | Open Web Application Security Project is an online community that produces freely available articles, methodologies, documentation, tools, and technologies in the field of web application security |
| 14 | POP3 | Post Office Protocol 3 is a protocol used by email clients to retrieve email messages from a mail server |
| 15 | Public CA | Public Certificate Authority is a well-known and trusted organization that issues digital certificates |
| 16 | RDS | RDS encryption uses the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your Amazon RDS instance |
| 17 | REST API | A REST API is an application programming interface (API) conforming to RESTful architecture style |

| No. | Term | Description |
|-----|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 18 | RSA | Rivest, Shamir, and Adleman (RSA) is a public-key cryptosystem that is widely used for secure data transmission |
| 19 | SIP | The Session Initiation Protocol (SIP) is a signaling protocol used for initiating, maintaining, and terminating real-time voice calls in CCaaS |
| 20 | SMS | Short message service |
| 21 | SMTP | Simple Mail Transfer Protocol is a standard protocol for sending emails |
| 22 | SRTP | Secure Real-time Transport Protocol is a profile for Real-time Transport Protocol intended to provide encryption, message authentication and integrity, and replay attack protection |
| 23 | TLS | Transport Layer Security is a cryptographic protocol designed to provide communications security over a computer network |
| 24 | X509 | X509 is a standard defining the format of public key certificates |
| 25 | WSS | WebSocket Secure is a computer communications protocol designed over the HTTP protocol, to provide full duplex communication channels |

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.

