GDPR Notice for AudioCodes VoiceAI Connect Enterprise

- Dedicated Environment -

Published: November 14, 2023 | Document #: LTRT-91146

This document describes the VoiceAI Connect Enterprise support for General Data Protection Regulation (GDPR). GDPR aspects that are not listed in this document are considered as not relevant to the VoiceAI Connect Enterprise service operation.

This notice is subject to AudioCodes Privacy Policy.

1 Overview and Definitions

GDPR defines 'personal data' as any information related to an identifiable person. This person may be identified directly (i.e., by name) or indirectly through any other identifier which is unique to that person. In the VoiceAI Connect Enterprise service, individuals can be directly identified by name or indirectly identified through other identifiers such as phone numbers.

Definition:

Provider is the AudioCodes customer that is using the VoiceAI Connect Enterprise to offer a service (or solution) to its Tenants.
Tenant is the end business customer that is subscribing to the Provider's service. For example, the Tenant dials to a voice-bot service that was built by the Provider, using AudioCodes VoiceAI Enterprise.

VoiceAI Connect Enterprise manages, collects, and stores the following information:

a) **CDR Records:**

Call Detail Records (CDR) contain information on calls made from the Provider's Tenants' devices. Information that may be defined as private information in CDR records could include, for example, Provider chatbot or Tenant caller phone number and Tenant called phone number.

CDRs are generated once at the end of the session. CDRs are stored locally and on a central monitoring system operated by AudioCodes support team. CDRs are optionally available to the VoiceAI Connect Enterprise Provider and AudioCodes support team.

b) **Call Transcripts:**

Call transcription is the conversion of a voice call audio track into written words, which is stored as plain text. VoiceAI Connect Enterprise can store chatbot call transcripts (speech-to-text) locally. Tenants' information that may be defined as private information in the transcript may include personal conversation information. Saving the call transcript is up to the Provider. By default, transcription is stored for 24 hours and then automatically deleted. Transcripts are available only to the VoiceAI Connect Enterprise Provider and to the AudioCodes support team, and it can be used by the Provider to verify that call progress is as expected.

c) **VoiceAI Connect Enterprise Syslog Notifications:**

Syslog is an event notification protocol that enables a device to send event notification. Information that may be defined as private information in syslog events may include, for example, the Tenant's caller and called phone numbers. VoiceAI Connect Enterprise saves syslog notifications locally, and it is used for debugging.

Syslog notifications are available only to the VoiceAI Connect Enterprise Provider Administrator and to the AudioCodes support team.

d) **Provider Information:**

Provider data includes contact information which may be used to identify a Provider, for example, the following information is captured:

- First name
- Last name
- Email
- Phone number
- Company name

e) **Provider Settings:**

Provider settings is a collection of Provider configurations, which is stored locally. This configuration includes, as an example, the following:

- Bots' and speech providers' information
- SIP Connection configuration

2 Right of Access (GDPR Art 15)

The Section 'Overview and Definitions' (above) fully outlines what data VoiceAI Connect Enterprise collects and saves as personal data.

Access to CDRs, call transcripts, call recording, syslog notifications, Provider information, Provider settings is limited to privileged users only with required valid credentials. Once appropriate credentials are provided:

- Providers with access to the Web interface or REST API can view and/or download their own CDRs, call transcripts, Provider information, Provider settings.
- Administrators with access to the Web interface or REST API can view and download CDRs, syslog files, Provider information.

Detailed information on how the Provider can retrieve the above can be found in the VoiceAI Connect Enterprise technical documentation.

3 Right to Rectification (GDPR Art 16)

CDRs, call transcripts, call recording, and syslog notifications are treated by VoiceAI Connect Enterprise as 'read-only' information as soon as it's stored in the database/disk. VoiceAI Connect Enterprise does not include a mechanism that allows a user to edit or modify the information once captured and stored, and there are no actions that the application takes based on this information.

4 Data Retention and the Right to be Forgotten (GDPR Art 17)

The information collected by VoiceAI Connect Enterprise as described in the Section Overview and Definitions can be removed to erase personal data.

a) **CDR Records:**

The call information is stored for a 45-day period. This allows AudioCodes to address any questions of the Provider during this period. Once this period elapses, the call information is deleted automatically. In case there is a need to immediately erase CDRs, the VoiceAI Connect Enterprise Administrator can do so.

b) **Call Transcripts:**

Call transcripts are stored for a 24-hour period. This provides sufficient time for the Provider to use call transcripts to track service issues. Once this period elapses, call transcript information is deleted automatically. In case there is a need to immediately erase call transcript records, the Provider can do so by deleting the call transcript record using VoiceAI Connect Enterprise's web interface.

c) **Syslog Notifications:**

Syslog notifications are stored for a 45-day period. This allows the AudioCodes Administrator to address any call history issues. Once this period elapses, the syslog information is deleted automatically. In case there is a need to immediately erase syslog records, the VoiceAI Connect Enterprise Administrator can do so.

d) **Provider Information:**

Provider information retention period is the length of the service contract plus two (2) years. This allows AudioCodes to address any Provider questions even after the two years.

Explicit Deletion: A Provider can request to delete its VoiceAI Connect Enterprise deployment. This explicit deletion deletes call transcripts, call recordings and the Provider's settings. CDRs are kept for 30 days and Provider information is kept for an additional two (2) years.

e) **Provider Setting:**

Provider setting retention period is the length of the service contract. The Provider can delete its own settings using the VoiceAI Enterprise web interface. This explicit deletion deletes all Provider setting information.

5 Right to Data Portability (GDPR Art 20)

Personal data that is stored in VoiceAI Connect Enterprise, as defined in Section Overview and Definitions of this document, may be retrieved by the Provider and/or by the Administrator and sent to a data subject.

It is the Provider's responsibility to comply with the applicable Privacy laws after downloading any personal information.

a) **CDR Records:**

Providers can save their own call information to a CSV file. The calls are saved to a CSV file according to the procedure defined by the VoiceAI Connect Enterprise technical documentation.

The calls saved in the CSV file may contain Tenant personal data which is not related to the data subject. For example, if the data subject is the caller of the call, the callee personal data of the same call may also be part of the call record in the CSV file. It is up to the VoiceAI Connect Enterprise Provider to make sure that Tenant personal data is not exposed to the data subject. It is beyond the VoiceAI Connect Enterprise product’s scope to erase other personal data that is not related to the data subject’s personal data from the CSV file.

b) **Call Transcript:**

Providers can save their own call transcript file, which can then be sent to the data subject. The calls are saved to a file according to the procedure defined by the VoiceAI

Connect Enterprise technical documentation. The call transcript file may contain Tenant personal data which is not related to the data subject. It is up to the VoiceAI Connect Enterprise Provider to make sure that other personal data is not exposed to the data subject. It is beyond the VoiceAI Connect Enterprise product's scope to erase other personal data that is not related to the data subject's personal data from the transcript file.

c) **Syslog Information:**

Only the VoiceAI Connect Enterprise Administrator can access and copy the syslog file. The syslog file may include other personal information. The syslog file is not shared with any Provider and is used only by the Administrator for debugging purposes.

d) **Provider Information:**

Providers can view their own account information in the VoiceAI Connect Enterprise through the VoiceAI Connect Enterprise 's web interface. The Provider page can then be saved as a text file or any other method such as a screen capture and alike.

e) **Provider Setting:**

Providers can view their own account setting information in VoiceAI Connect Enterprise through the VoiceAI Connect Enterprise web interface (e.g., Bot, SIP Connections). Provider settings can then be saved as a text file or any other method such as a screen capture and alike.

6 Responsibility of the Controller and Data Protection by Design and by Default (GDPR Art 24 and 25)

The service provides security measures that only allow authorized users to have access to the VoiceAI Connect Enterprise portal information and settings. Access to personal data stored in the VoiceAI Connect Enterprise is protected and requires a username and password to view and retrieve any personal data from VoiceAI Connect Enterprise.

a) **VoiceAI Connect Enterprise Web Access:**

Access to VoiceAI Connect Enterprise's web interface is only performed by Providers and Administrators who have rights to log in to VoiceAI Connect Enterprise. VoiceAI Connect Enterprise users are authenticated and authorized using a username and password. Provider can access only the following information: Provider CDRs, Provider transcript, Provider recording, Provider information, and Provider settings.

The AudioCodes Administrator can access only the following information: Provider CDRs, Provider information, syslog notification, and Provider settings.

b) **VoiceAI Connect Database Access:**

VoiceAI Connect Enterprise uses databases as part of its operation. The databases are embedded inside the VoiceAI Connect Enterprise and cannot be accessed directly. They are used only by the VoiceAI Connect Enterprise application. To offer data protection at rest, databases and file systems are encrypted using industry-standard encryption.

c) **Data in Transit:**

VoiceAI Connect Enterprise implements encrypted communication for signaling, media and syslog information (secure SIP and SRTP) and uses HTTPS for bot-frameworks and cognitive services.

7 End of Contract

The Provider can ask to delete its own account. Delete requests are sent to the VoiceAI Connect Administrator, and the Administrator then initiates the following:

- Deletes all Provider call transcripts, call recordings, and Provider settings.
- Provider CDR records and Provider information are kept for two (2) more years to address Provider queries. Once this retention time elapses, all Provider information is deleted, except for the Provider's email, account deletion date, account balance at time of deletion, and plan used.

Detailed information on how to perform an end of contract (Delete Provider) is described in the VoiceAI Connect Enterprise technical documentation.