Notice

AudioCodes Voca CIC Solutions

GDPR and HIPAA-Ready Notice for AudioCodes Voca CIC Solution

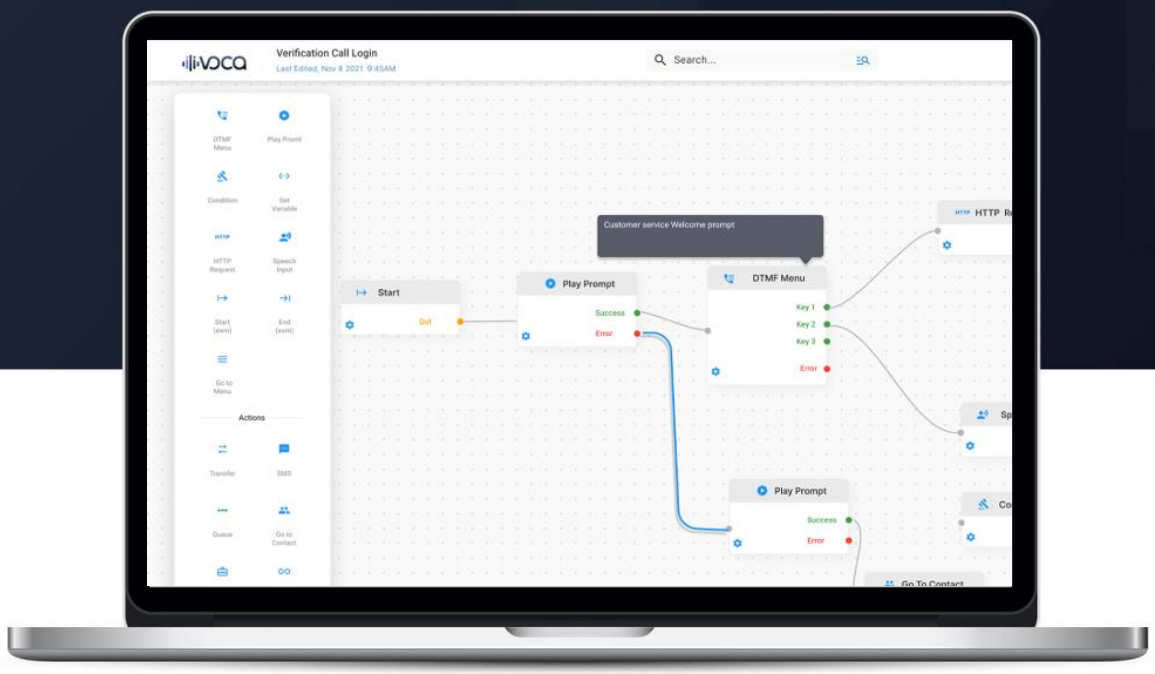

Table of Contents

Notice ii

Security Vulnerabilities ii
Customer Support ii
Stay in the Loop with AudioCodes ii
Abbreviations and Terminology ii
Document Revision Record ii
Documentation Feedback iii

1 Overview and Definitions 2

1.1 Conversation Data 2
1.1.1 Digital Channels 2
1.1.2 Conversation Data Retention Period 3
1.2 User Information 3
1.2.1 User Information Retention Period 3

2 Right of Access (Art 15) 4

3 Right to Rectification (Art 16) 5

4 Right to be Forgotten (Art 17) 6

4.1 Conversation Data 6
4.2 User Information 6

5 Right to Data Portability (Art 20) 7

5.1 Conversation Data 7
5.2 User Information 7

6 Security of Processing (Art 32), Data Protection by Design and by Default (Art 25) and HIPAA Security Rules 8

6.1 Encryption of Personal Data 8
6.2 Access Control to Voca on Premises 8
6.3 Access Control to Database 8
6.4 Backup 9
6.5 Segregation Control 9

7 Disposal Process 10

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: October-5-2025

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Stay in the Loop with AudioCodes

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Document Revision Record

LTRT	Description
28979	GDPR updates
28976	Initial document release

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

1 Overview and Definitions

The AudioCodes Voca solution provides healthcare customers with services that are ready to accept Protected Health Information (PHI), referring to these services as Health Insurance Portability and Accountability Act (HIPAA)-Ready Services.

AudioCodes Voca solutions provide customers with services that are ready to accept Personal Identifiable Information (PII), referring to these services as General Data Protection Regulation (GDPR)-Ready Services.

AudioCodes provides all the necessary tools for the customer/administrator to be GDPR and HIPAA compliant. The purpose of this document is to detail the different tools that help the customer remain compliant. GDPR/HIPAA aspects that are not listed in this document are not relevant to the Voca product operation.

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 that is unique to that person.

The HIPAA privacy rule defines all individually identifiable health information that is held or transmitted as Protected Health Information (PHI).

1.1 Conversation Data

Voca optionally collects and stores call-related information.

Call data includes the following information that may be used to identify a person:

- Caller phone number
- Called phone number
- Call start time
- Call end time
- Duration of the call
- Audio recordings of the caller's interaction with Voca

1.1.1 Digital Channels

- SMS
- Webchat

The information collected may be:

- First Name
- Last Name
- Phone number
- Email
- Customer custom fields

1.1.2 Conversation Data Retention Period

If the customer decides to store the conversation data, the retention period needs to be configured. The conversation data retention period will be configured during the setup phase. Options are 3, 6 or 12 months.

1.2 User Information

The Voca system can be configured to connect to the Active Directory using the LDAPs protocol to retrieve the organization's contacts information into the Voca database. This information is collected in accordance with the service and may vary depending on the activity. The organization contacts' data may include the following information:

- First and last name
- Job title
- Phone number
- Mobile phone number
- Email addresses
- Department

1.2.1 User Information Retention Period

The user information retention period will be as long as the customer uses the system; it is the customer's responsibility to destroy or delete the data when the system is no longer in use.

2 Right of Access (Art 15)

The Overview and Definitions section above fully outlines what data the Voca system collects and saves as personal data.

The Voca administrator can log in to the Web Management Interface using secured and encrypted web access and view the 'personal data'. Detailed information on the Voca Web Management Interface can be found in the *Voca Administrator's Guide*.

The Voca administrator can export personal data outside of the Voca system. More information can be found in the Right to Data Portability (Art 20) section below.

3 Right to Rectification (Art 16)

The user's information is taken from external sources but can be modified locally if needed.

The conversation data is processed and stored on-the-fly in the Voca database. There is no mechanism that allows a user to edit or modify the information once captured and stored as part of normal operation.

In the Voca system, the information is controlled by the Voca administrator through the Web Management Interface only. The Voca administrator can create, delete, and edit the personal information and can rectify personal information per request.

4 Right to be Forgotten (Art 17)

The information collected by the Voca system as described in Section 1 can be removed to erase personal data.

4.1 Conversation Data

Conversation data is stored for a specific time range. Once this time range elapses, conversation data is deleted automatically. The retention period for conversation data in the Voca database is configurable by the Voca administrator, to adhere to and facilitate the relevant Data Protection policy required by the organization.

If there is a need to immediately erase personal conversation data, the Voca administrator should approach AudioCodes for immediate support.

4.2 User Information

User information can be imported from the Active Directory server using the LDAPS protocol, uploaded through a file to the Web Management Interface, or created manually. User information is actively retrieved by Voca.

To erase the imported personal user information, the Voca administrator can terminate the connection with the Active Directory and manually delete all the users and their personal data from the Voca Web Management Interface on demand.

Detailed information on how to delete a contact from the Voca system can be found in the *Voca Administrator's Guide*.

5 Right to Data Portability (Art 20)

Personal data which is stored in the customer's OVOC as defined in Conversation Data above, may be retrieved by the Voca administrator and sent to a data subject.

5.1 Conversation Data

The Voca administrator can save conversation data to a CSV file, which then can be sent to the data subject. The calls saved to the CSV file, are based on the filters defined by the Voca administrator, who may use the Voca filter feature to filter only the calls related to the data subject prior to saving the calls to a CSV file.

The interaction records in the CSV file may contain other personal data which is not related to the data subject. For example, if the data subject is the caller of the interaction, the callee's personal data of the same call may also be part of the interaction record in the CSV file. It is up to the Voca customer to make sure that other personal data is not being exposed to the data subject. It is out of the Voca product's scope to erase other information from the CSV file that is not related to the data subject personal data.

Detailed information on how to filter conversation data and save it to a CSV file in the Voca system can be found in the *Voca Administrator's Guide*.

5.2 User Information

User information in the Voca system can be retrieved using the Voca Web Management Interface. The Voca administrator can select a specific user and see their full user details. The specific user's page can then be copied to a text file or captured via screenshot. The saved user details file can then be sent to the data subject.

As with conversation data, also the Contacts section in the Voca Web Management Interface may include other personal information. It is up to the Voca customer to make sure that other people's personal data is not being exposed to the data subject.

Detailed information on how to view contact information can be found in the *Voca Administrator's Guide*.

6 Security of Processing (Art 32), Data Protection by Design and by Default (Art 25) and HIPAA Security Rules

6.1 Encryption of Personal Data

- Voca is configured by default: caller speech inputs, caller number.
- This data is saved encrypted on disk.
- Configuration can be changed to NOT save any caller data.
- Voca can also be configured to mask the caller number to show only the last 4 digits.
- Data in Transit is encrypted:
  - AudioCodes SBC creates a TLS and an SRTP session between caller and Voca.
  - Traffic from Voca to any 3rd party system runs over the HTTPS sessions.

6.2 Access Control to Voca on Premises

- Voca has two connectivity options: RDP or Web UI
- Access by RDP is relevant for customer support by AudioCodes only as needed.
- The customer is responsible to provide a secure connection and authentication method.
- Voca Web access is for customers' operational usage. The preferred way is to synchronize Voca to the customers' Azure AD and use the MFA and credentials as defined in the customer's policy.
- Voca also provides the ability to use local users. This method is not recommended.

6.3 Access Control to Database

- The database is based on MySQL and might contain PII or PHI in case the customer chooses to do so.
- Access to the database is pre-configured during the installation phase to a default password but can be replaced by another one known to the customer only. In that case, it is the customer's responsibility to save the credentials and retrieve them when database support is needed.

6.4 Backup

Voca can set up backups for all server configurations. The data is backed up at scheduled intervals to the external storage. It is the customer's responsibility to provide secure, encrypted storage.

6.5 Segregation Control

The Voca system has several Web UI levels of users:

- **Super Admin:** This user is used ONLY by AudioCodes to set licensing and features.
- **Provider Admin:** This user is used to configure and maintain, on behalf of a tenant admin, the Voca server and Tenants (optional).
- **Tenant Admin:** This user is used to configure and maintain specific tenants.
- **Analytic User:** This user is used to view and generate reports globally or per tenant.

7 Disposal Process

The Voca system can run on multiple platforms. If the platform is virtual (for example, VMware) or cloud (for example, AWS), the disposal operation should be done on the virtual or cloud platform level and is out of the Voca product's scope.

If the Voca server runs on a hardware server provided by AudioCodes, an administrator-level user can perform a clean installation process on the Voca server to remove any personal information from the system before disposal.

This operation erases all data from the Voca server and returns it to its initial state, removing all 'personal data' as defined in this document. Detailed information on how to clean install the Voca server can be found in the *Voca Installation Manual*.

International Headquarters
Naimi Park
6 Ofra Haza Street
Or Yehuda, 6032303, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com

©2025 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-28979