GDPR Notice for AudioCodes One Voice Operations Center (OVOC)

This document describes the One Voice Operations Center (OVOC) support for GDPR. GDPR aspects that are not listed in this document are considered as not relevant to the OVOC product operation.

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 OVOC, individuals can be directly identified by name or indirectly identified through other identifiers such as phone numbers. The OVOC manages, collects and stores the following information:

a) **Calls Information:** OVOC collects and stores calls-related information from AudioCodes' SBC and Media gateway, Microsoft on premise Lync or Skype for Business Monitoring SQL Server, and from IP Phones and SIP clients reporting calls-related data using the RFC 6035 protocol.

The calls data includes the following information which may be used to identify a person:

I. Caller name
II. Caller phone number
III. Caller URI
IV. Callee name
V. Callee phone number
VI. Callee URI
VII. Full SIP messages call flow

b) **Users Information:** OVOC can be configured to connect to Active Directory using the LDAPS protocol to retrieve end users' information into the OVOC database. This information is used in OVOC to correlate between the calls data and actual user names. The users' data includes the following information which may be used to identify a person:

I. Full name
II. User name
III. Description
IV. Working department

AudioCodes Inc.
200 Cottontail Lane, Suite A101E, Somerset, NJ 08873
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
1 Hayarden Street, Airport City, Lod 7019900
P.O.Box 255, Ben Gurion Airport, Israel 7019900
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

V. Office phone number
VI. Mobile phone number
VII. Home phone number
VIII. Microsoft Lync or Skype for Business line URI
IX. Email

c) **Personal Device Information:** OVOC can be used to manage devices such as AudioCodes' or Polycom's IP Phones and Jabra headsets and speakers. As part of the device management procedures, the following information is collected and stored and may be used to identify a person:
   I. User name
   II. Phone number
   III. Login name
   IV. Display name

d) **Operator Information:** OVOC can be configured to work with local operators. An operator is a person who can login to the OVOC GUI and use the OVOC. Some of the operators' data is stored in the OVOC and may be used to identify a person:
   I. Operator name
   II. Full name
   III. Phone number
   IV. Email
   V. Description
   VI. List of IP Addresses of the machines the operator can login from

e) **Syslog Information:** OVOC may be used as a syslog server to collect syslog data from AudioCodes' SBCs and Media Gateways. The syslog messages stored in the syslog server may contain CDR private information such as caller and callee phone numbers.

f) **SBC and Media Gateway Debug Recording Information:** The AudioCodes' SBCs and Media gateway can send debug recording packets to the OVOC. The OVOC stores the debug recording data. Information that may be defined as private information in a debug recording data could include, for example, a caller phone number and called phone number.

The remainder of this document describes the compliance of OVOC's handling of 'personal data' per the corresponding GDPR sections. Apart from the above data sets, the OVOC does not collect and retain any other 'personal data'.

2 Right of Access (Art 15)

The section above “Overview and Definition” fully outlines the scope of the data that is retrieved and saved by OVOC and which can be regarded as personal data.

The OVOC operator can login to the OVOC GUI using a web access and look at the private data using specific filters according to specific criteria such as name and phone number. Once the filter is set, the operator can look at the specific subject personal data. A full explanation on how to configure filters using the OVOC GUI can be found in the OVOC User’s Manual.

The OVOC allows tenant and system operators whose Security Level is configured as ‘Monitor’ or ‘Operator’ to conceal from view call details and user information that is exposed in calls:

- The last digits in user’s phone are concealed from view
- Information about callers and called parties in the Call Details page is replaced by ***
- User / URI reports are disabled
- Specific information on any user cannot be retrieved
- User tables and statistics are concealed from view
- SIP ladders and user call information are concealed from view

The OVOC operator can export personal data from OVOC to their network storage device (data will be exported based on filter and privacy mode definition). Detailed explanations are provided in the Section “Right to Data Portability (Art 20)”.

3 Right to Rectification (Art 16)

The calls information, user information, personal device information, syslog information and SBC and Media Gateway Debug Recording information are extracted from external sources and treated as ‘read only’ information once stored in the OVOC database. There is no mechanism that allows a user to edit or modify the information once captured and stored as part of a normal operation.

When the OVOC manages the operators locally, the operator information is controlled by the OVOC administrator. The OVOC administrator can create, delete and edit the personal information of the locally managed operators. Therefore, the OVOC administrator can rectify the operator personal information per request.

4 Right to be Forgotten (Art 17)

The information collected by the OVOC as described in Section 'Overview and Definitions' can be removed in order to erase personal data:

a) **Calls Information:** The calls information is stored for a specific time range. Once this time range elapses, the call information is deleted automatically. The duration of the time a call remains in the OVOC database is configurable by the OVOC administrator.

   In case there is a need to immediately erase personal call information, the OVOC administrator can do so by deleting the device from OVOC that retrieved the calls information and sent it to OVOC. By deleting the device from the OVOC, the entire history of the calls collected and sent by this device will become non-accessible. Therefore, by deleting a device in the OVOC, all related personal data call information will become non-accessible.

   Detailed information on how to delete a device in the OVOC can be found in the OVOC User's Manual.

   Calls information is also used for Top Users Scheduled reports. It might be the case that personal data for a specific data subject is seen in the Top Users reports. In order to delete the personal data, the OVOC operator should delete the historical Top Users reports created by the Scheduled reports mechanism. Refer to the OVOC User's Manual for more information regarding how to delete a scheduled report.

b) **Users Information:** The Users information is retrieved from the Active Directory server using the LDAPS protocol. The users' information is correlated to the configured instance of the Active Directory in the OVOC. In order to erase personal user information, the OVOC administrator can delete the Active Directory instance from the OVOC. Once the OVOC Active Directory instance is deleted, all the attached users and their personal data are also erased from the OVOC.

   Detailed information on how to delete an Active Directory instance from OVOC is described in the OVOC User's Manual.

c) **Personal Device Information:** Personal device information is stored whenever a device such as IP Phone or Jabra device is managed by the OVOC. To erase the private device information from the OVOC, the OVOC administrator can delete a specific user and all their managed devices from the OVOC Device Manager. Once the user and their managed devices are erased from the OVOC, all the related personal device information is erased.

   Detailed information on how to delete a user and their devices from the OVOC is described in the OVOC Device Manager Pro Administrator's Manual.

d) **Operator Information:** When the OVOC manages the OVOC operators locally on the OVOC server, the OVOC administrator can delete a specific operator. Once the OVOC administrator deletes the operator, all the operator's personal data is erased. Detailed information on how to delete an operator from the OVOC is described in the OVOC User's Manual.

e) **Syslog Information:** The OVOC may be used to collect syslog information from AudioCodes' SBCs and gateways. The OVOC collects syslog information using a syslog server embedded inside the OVOC server. The syslog information may contain personal data as part of CDRs sent to the syslog server by the SBCs and the gateways. The syslog information is stored in a file located in the OVOC NBIF folder in the OVOC file system. The OVOC administrator using a specific username and password can delete the syslog file using a secured protocol such as SFTP. Once the syslog file is deleted, all the related personal syslog information is also erased.

   Detailed information on how to access the OVOC NBIF folder and delete the syslog file from the OVOC server is described in the OVOC IOM Manual.

f) **SBC and Media Gateway Debug Recording Information:** The OVOC may be used to collect debug recording information from AudioCodes' SBCs and gateways. The OVOC collects the debug recording information using a Wireshark network sniffer embedded inside the OVOC server. The debug recording information may contain personal data. The debug recording information is stored in a file located in the OVOC NBIF folder in the OVOC file system. The OVOC administrator using a specific username and password can delete the debug recording file using a secured protocol such as SFTP. Once the debug recording file is deleted, all the related personal debug recording information is also erased.

   Detailed information on how to access the OVOC NBIF folder and delete the debug recording file from the OVOC server is described in the OVOC IOM Manual.

5 Right to Data Portability (Art 20)

Personal data which is stored in OVOC as defined in Section 'Overview and Definitions' of this document may be retrieved by the OVOC administrator and sent to a data subject.

a) **Calls Information:** The OVOC administrator can save calls information to a CSV file which can then be sent to the data subject. The calls are saved to a CSV file according to the filter defined by the OVOC administrator. The OVOC administrator may use the OVOC filter to filter only the calls related to the data subject prior to saving the calls to the CSV file.

   The calls recorded 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 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 OVOC customer to make sure that other personal data is not exposed to the data subject. It is beyond the OVOC product's scope to erase other personal data that is not related to the data subject's personal data from the CSV file. Detailed information on how to filter calls information and save them to a CSV file in the OVOC is described in the OVOC User's Manual.

b) **Users Information:** Users information in the OVOC can be retrieved via the OVOC GUI interface. The OVOC administrator can select a specific user in the OVOC Users tab and click the "Show" button to view the full details of the user. The specific user's page can then be saved as a text file or any other method such as a screen capture and alike. The saved user's details file can then be sent to the data subject.

   As is the case for the Call information, the user's web page in the OVOC GUI may also include other personal information. It is up to the OVOC customer to make sure that other personal data is not exposed to the data subject.
   Detailed information on how to view user's information in the OVOC GUI can be found in the OVOC User Manual.

c) **Personal Device Information:** By using the Export Users and Devices option on the OVOC's Device Manager, the OVOC administrator can export personal device information to a CSV file which then can be sent to the data subject.

   The personal device information in the CSV file may contain other personal data which is not related to the data subject. It is up to the OVOC customer to make sure that other personal data is not exposed to the data subject.
   Detailed information on how to Export Users and Devices from the OVOC Device Manager can be found in the OVOC Device Manager Pro Administrator's Manual.

d) **Operator Information:** Operators information in the OVOC can be retrieved via the OVOC GUI interface. The OVOC administrator can select a specific operator in the OVOC Operators tab and view the full details of the operator on the left side summary pane view in the OVOC GUI. The specific operator's details can then be saved as a text file or by other methods such as screen capture and alike. The saved operator's details file can then be sent to the data subject. The operators web page in the OVOC GUI may include others personal information. It is up to the OVOC customer to make sure that other personal data is not exposed to the data subject. Detailed information on how to view operator's information in the OVOC GUI is described in the OVOC User's Manual.

e) **Syslog Information:** The syslog information is stored in a file located in the OVOC NBIF folder in the OVOC file system. The OVOC administrator using a specific username and password can access and copy the syslog file using a secured protocol such as SFTP.

The syslog file may include other personal information. It is up to the OVOC customer to make sure that other personal data is not exposed to the data subject.
Detailed information on how to access the OVOC NBIF folder and copy the syslog file from the OVOC server can be found in the OVOC IOM Manual.

f) **SBC and Media Gateway Debug Recording Information:** The Debug Recording information is stored in a file located in the OVOC NBIF folder in the OVOC file system. The OVOC administrator using specific username and password can access and copy the Debug Recording file using secured protocol such as SFTP. The Debug Recording file may include other personal information. It is up to the OVOC customer to make sure that other personal data is not exposed to the data subject. Detailed information on how to access the OVOC NBIF folder and copy the Debug Recording file from the OVOC server can be found in the OVOC IOM Manual.

g) **"Privacy" mode** can be enabled by System operators to hide OVOC data from Tenant and System operators. This includes the masking of phone numbers, URIs and all the call related data, hiding of User/URI reports or schedulers, user tables and statistics and Calls/SIP Ladder.

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

Access to personal data stored in the OVOC is protected and requires a username and password in order to look and retrieve any personal data from the OVOC.

a) **OVOC Web Access:** Access to the OVOC web interface either via a browser or REST API is performed by administrators and operators who have rights to login to the OVOC.

   OVOC administrators and operators can be authenticated and authorized either locally on the OVOC server or by using a centralized third- party authentication server such as Active Directory or RADIUS servers. In case of Active Directory usage, the access protocol used to secure the traffic between the OVOC and the Active Directory is Secured LDAP (LDAPS). The operator's access rights are defined by the OVOC System Administrator. The HTTPS protocol is used to secure traffic between the OVOC web client and the OVOC server.

b) **OVOC Server Access:** Access to the OVOC server is protected by username and password. The access transport to the OVOC server is over secured protocols such as SSH for CLI connection to the OVOC server, and SFTP for file access and retrieval.

c) **OVOC Database Access:** The OVOC uses databases as part of its operation. The databases are embedded inside the OVOC and cannot be accessed directly. They are used only by the OVOC application. The OVOC database access is protected in two layers. Only a root user on the OVOC machine can access the OVOC database. Once a user is a root user on the OVOC machine, the database access requires a specific database administrator login and password to access the database content.

   Detailed information about OVOC access rights and OVOC access secured protocols is described in the OVOC Security Guidelines.

d) **OVOC Server Data Encryption:** In order to make best data protection for the entire data stored in the databases and on disk, it is recommended to encrypt storage used by the OVOC application. For exact instructions for encryption methodology and possible performance impact, please consult with your IT department experts / storage vendors. There were no performance implications experienced on the OVOC application during the test cycle.

7 Disposal Process

The OVOC system can run on multiple platforms. If the platform is virtual (e.g. VMware or HyperV) or cloud (e.g. AWS or Azure), the disposal operation should be performed on the virtual or cloud platforms level and is beyond the scope of the OVOC product.

If the OVOC server runs on a hardware server provided by AudioCodes, to remove any personal information from the system before disposal, an admin level user can perform a clean installation operation on the OVOC server. This operation erases all data from the OVOC server and restores it to its initial state, removing all 'personal data' as defined in this document.

Detailed information on how to perform a clean install of the OVOC server is described in the OVOC IOM Manual.