GDPR Notice

AudioCodes Meeting Insights™

AudioCodes Meeting Insights solutions provide the customer/administrator with the necessary tools that are required for compliance with the General Data Protection Regulation (GDPR), under the assumption that the customer is a Controller as defined under the GDPR.

The purpose of this document is to provide details for these different tools. GDPR aspects that are not listed in this document are not relevant to the Meeting Insights product operation.

1 Overview and Definitions

GDPR defines 'personal data' as any information related to an identified or identifiable natural person. This person may be identified directly (e.g., name, I.D. number, etc.) or indirectly through any other identifier who is unique to this person ("Data Subject"). For Meeting Insights, individuals can be directly identified by name or indirectly identified through other identifiers such as phone numbers, login IDs and email addresses.

Meeting Insights manages, collects, and stores the following information:

a) **Meeting Recording:** Meeting Insights records and stores meeting-related information and meeting media that it receives from Microsoft Teams. Meeting recordings may include the following information which may be used to identify a person:

   I. Meeting organizer's User Principal Name (UPN)/LoginID, name, and email

   II. Participant's UPN/LoginID name, and email

   III. Meeting recording Viewer's UPN/LoginID, name, and email

   IV. External Participant's name, number, and email

   V. Meeting media (audio, content sharing, pictures)

   VI. Meeting recaps such as summaries, notes, decisions, and action items

b) **Users Information:** Meeting Insights is configured to connect to Microsoft Azure Active Directory to retrieve users' information for the Meeting Insights database. This information is used by Meeting Insights to correlate between the meeting data and the actual usernames and to authenticate users. The users' personal data includes the following information which may be used to identify a person:

   I. First and last names

   II. Account UPN

   III. Email

   IV. Voiceprint – the system creates a digital presentation of the user's voice, which is stored encrypted and separated from the username.

c) **Logs:** Meeting Insights' log messages stored on Meeting Insights servers or Azure Log Monitor may contain CDR private information such as usernames and emails of meeting participants.

d) **AI Technology:** Meeting Insights uses AI technology such as Speech to Text, Speaker Identification, Generative AI to improve productivity, enhance meeting experiences, and foster collaboration by generating automatic and powered by AI insights such as meeting summary, list of action items, meeting outline and more. The process of the AI insights generation includes converting the audio into text, transcription, and then analyzing the transcription to generate the AI insights. Meeting Insights utilizes Microsoft Azure Cognitive services, Speech, and Azure Open AI Services (different than Open AI services). The Microsoft Azure Open AI Service is integrated with enabled abuse monitoring and content filtering. Your data is NOT available to other customers or to OpenAI, it is NOT used to improve OpenAI models or Azure Open AI models or improve any Microsoft or 3rd party products or services.

2 Right of Access (Art 15)

The Meeting Insights administrator can log in to the Web Management Interface using secured and encrypted Web access and look for the personal data upon request of a Data Subject. More information can be found in Section ‘Right to Data Portability (Art 20)’ below.

Detailed information about the Meeting Insights Web Management Interface can be found in the Meeting Insights User Guide.

3 Right to Rectification (Art 16)

In the Meeting Insights system, user information is controlled by the Meeting Insights administrator through the Web Management Interface only. If user information is mapped from an external source, it cannot be changed in Meeting Insights.

Meeting information and media are processed and stored on-the-fly in the Meeting Insights database and storage. The meeting's organizer controls public metadata editing permission of their meetings. The organizer can grant editing permission to another participant in the meeting or delegate permissions globally. The organizer or their delegates can change the metadata of the meeting, including the voice recaps text and meeting transcription, and trim the beginning of the recoding. Each participant can edit their private recaps, highlights, and bookmarks.

The organizer or their delegates can delete a recording. The administrator can delete any recording. The administrator can delete a user from Meeting Insights that was deleted from Azure Active Directory.

There is no mechanism that allows a user to edit or modify audio, video or images once it is captured and stored as part of a normal operation.

Detailed information on how to delete a user or meeting recordings is described in the Meeting Insights Administrator Guide.

4 Right to be Forgotten (Art 17)

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

a) **Meeting Recording:** The meeting recording is stored until it is deleted. The meeting can be deleted by automatic retention policy, the administrator, the meeting's organizer or their delegates. The metadata and media of the meeting is erased immediately from data storage. The backups of metadata and media files can be retained up to 14 days on the cloud and are deleted automatically. These files are not accessible by users as part of normal operations.

b) **Users Information:** The Meeting Insights administrator can locally delete a user defined in Meeting Insights after the user has been removed from Azure Active Directory, including the user voiceprint. However, all the metadata that was collected about the user participation in non-deleted meetings will be retained. The user can still be identified using their User Principal Name (UPN).

5 Right to Data Portability (Art 20)

Personal data that is stored by Meeting Insights as defined in Section 'Overview and Definitions' may be retrieved by the Meeting Insights administrator and sent to a Data Subject.

a) **Meeting Recording:** The Meeting Insights administrator can download a meeting recording through the user interface.

b) **Users Information:** Users' information in Meeting Insights can be retrieved through the Meeting Insights Web interface. The Meeting Insights administrator can select a specific user in Meeting Insights' Users page to view full user details. The specific user's details can be exported to a file. The saved user's details file can then be sent to the Data Subject. Detailed information on how to view a user's information in the Meeting Insights Web interface is described in the Meeting Insights Administrator Guide.

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

Access to personal data stored by Meeting Insights is protected and requires a username and password to view and retrieve any personal data from Meeting Insights.

a) **Meeting Insights Web Access:** Access to the Meeting Insights Web interface either through a Web browser or REST API is performed by administrators who have permission to log in to Meeting Insights and view personal data. Meeting Insights administrators are authenticated and authorized by Microsoft Azure Active Directory, which is controlled and managed by the customer. The customer must select MFA in their Azure Active Directory. The traffic between the Meeting Insights Web client and the Meeting Insights components is secured using the HTTPS protocol.

b) **Meeting Insights Servers Access:** Access to the Meeting Insights servers is protected by username and password. The access transport to the Meeting Insights server is secured over protocols such as SSH for CLI connection to the Meeting Insights server. Meeting Insights server access is under the customer’s responsibility when Meeting Insights is hosted on the customer’s Azure Cloud.

c) **Meeting Insights Data Security at Rest:** Meeting Insights data at rest is inactive data that is stored physically in a digital form such as meeting information and media. It is stored encrypted utilizing disks or storage encryption. Disks and storage encryption are under the customer’s responsibility when Meeting Insights is hosted on the customers’ public cloud or on-premises.

d) **Meeting Insights Data Security in Transit:** Meeting Insight’s data in transit is data flowing through the communications network between the various system elements. Meeting Insight’s data in transit is encrypted using secure protocols such as HTTPS and SRTP.

Detailed information about Meeting Insights access permissions is described in the Meeting Insights Administrator Guide.

7 Disposal Process

The Meeting Insights solution can operate using multiple platforms. If the installation platform is virtual (e.g., VMware), cloud (e.g., Microsoft Azure) or a dedicated bare metal machine, the disposal operation should be performed on the virtual cloud machine platform levels and is beyond the scope of the Meeting Insights product.

This operation erases all data from the Meeting Insights, its database and storage, removing all personal data as defined in this document.

The Meeting Insights server can store the media on multiple platforms such as local disk and cloud storage. The disposal operation is performed by deleting the stored media folders and is beyond the scope of the Meeting Insights product.