

## Data Protection Impact Assessment (DPIA) for the AI Solution

### 1. Introduction

This Data Protection Impact Assessment (DPIA) is conducted in accordance with Article 35 of the GDPR for the AI-powered meeting documentation software of the company. The objective is to systematically analyze the risks to data subjects and to define appropriate protective measures.

### 2. Description of Processing

- **Purpose of Processing:**

Automated transcription, analysis, and summarization of meetings for efficient documentation and follow-up.

- **Personal Data Processed:**

- Spoken language (transcripts)
- Names and contact details of meeting participants (as captured)
- Metadata (date, time, duration, meeting ID)
- Video recordings of meetings to support transcription
- Data Subjects: Participants of meetings (customers, partners, employees).
- Data Sources: Live audio and video recordings from online meetings.
- Processors Involved: Microsoft Azure (hosting), Azure OpenAI (text analysis)

### 3. Assessment of Necessity and Proportionality

- The processing is carried out to provide efficient meeting documentation and to replace manual note-taking.
- Proportionality is ensured, as only relevant data is processed.
- The processing is based on the consent of participants or on legitimate interest pursuant to Article 6(1)(f) GDPR.

### 4. Assessment of Risks to the Rights and Freedoms of Data Subjects

**Potential Risks:**

- Unauthorized access to transcripts, video recordings, and metadata
- Misuse or misinterpretation of the data
- Insufficient transparency for data subjects
- Risks arising from the use of external AI service providers

### 5. Measures to Mitigate Risks

- **Technical and Organizational Measures (TOMs):**
  - Encryption of transcripts, video recordings, and stored data
  - Access restrictions and role-based permissions
  - For users from the European Union (EU), all data traffic remains entirely within the EU data border. No personal data is transferred or processed outside the European Union
  - Pseudonymization of sensitive data
  - Ensuring that video and other recordings are no longer available in any form once deletion has been initiated by the data controller
  - Transparent user information regarding the recording and processing of video content
  - Regular data protection and security audits
  - Further detailed measures can be found in Annex 1: Technical and Organizational Measures
  
- **Specification of deletion periods for raw data:**
  - Temporary raw data required for transcription and analysis will be deleted immediately after processing is complete.
  - Permanent storage of raw data will only take place at the express request of the client.
  - In all other respects, the deletion policy set out in the DPA (§ 10) applies.
  - Contractual safeguards:
    - Conclusion of data processing agreements (DPA) with all subcontractors.
    - Ensuring GDPR compliance of external service providers.
  
- **Contractual Safeguards:**
  - Conclusion of data processing agreements (DPAs) with all subcontractors
  - Ensuring GDPR compliance of external service providers
  
- **Data Subject Rights:**
  - Transparent information on data processing
  - Implementation of deletion periods and rights to object

## 6. Conclusion

After assessing the risks and implemented measures, the processing is deemed



GDPR-compliant and poses an acceptable risk to the data subjects. The Data Protection Impact Assessment is reviewed and updated on a regular basis.