Technical and Organisational Measures

1. Access Control (Hosting Location)

Physical access control is ensured by our cloud hosting providers within the EU (Microsoft Azure) and in Germany (Hetzner – strongly preferred). These providers are obligated to operate data centers in accordance with high security standards (e.g., ISO 27001) and to protect them against unauthorized access.

2. Access Control (Logical)

Access to the AI application is secured through the following measures:

- **Authentication:** Customers (controllers) integrate the AI into their meetings via registered accounts. Unauthorized access is excluded.
- **Encryption:** All data transmissions are conducted exclusively through encrypted channels (e.g., HTTPS).
- **Access Logging:** All access requests are logged and monitored for potential misuse patterns.
- **Access to Stored Video Recordings:** Access to stored video content is restricted to authorized users based on a defined access control policy.
- **Encrypted Storage:** Stored videos are encrypted and can only be decrypted by authorized entities.
- All workstation computers are centrally managed via Microsoft Intune, ensuring consistent implementation of security policies and device configurations.
- In addition, Microsoft Defender for Endpoint is active on all devices to provide advanced threat detection and response.
- Microsoft Defender Antivirus is installed on all end devices and enabled at all times.

3. Transfer Control

Measures to ensure the secure transmission and storage of data include:

- **Encryption** of data transmissions using TLS/SSL protocols.
- **Logging** of all data transfers to ensure traceability.
- **Transfer of personal data to third parties** only with the prior consent of the controller.
- **Use of VPN connections** for secure remote access.
- **No disclosure of video recordings to third parties** without the controller’s explicit instruction.

- **Processing of video recordings** takes place exclusively within designated systems.

4. Input Control
Measures to ensure the traceability of the processing of personal data:

- Logging of all entries, modifications, and deletions of personal data.
- Documentation of user activities in audit logs.
- Training of employees on proper data processing practices.
- Documentation of access to stored video recordings.
- Transparent labeling of video data processing in system logs.

5. Order Control
Measures to ensure data processing is conducted solely in accordance with instructions:

- Processing activities are carried out exclusively in accordance with the controller's instructions (Art. 28 GDPR).
- Employee training on the controller's instructions and GDPR compliance.
- Regular internal audits to verify compliance.
- Use of video recordings is limited strictly to transcription purposes, with no storage beyond the agreed retention periods.

6. Availability Control
Measures to ensure availability and protection against data loss:

- Regular system backups (at least daily).
- Use of redundant systems (e.g., RAID configurations, failover solutions).
- Contingency plans and regular testing of recovery procedures.
- Ensuring that video and other recordings are no longer accessible in any form after deletion has been requested by the controller.

7. Handling of temporary raw data (audio/video recordings)

- Raw data that is processed exclusively for the purpose of transcription and analysis will be automatically deleted after completion of the respective processing operation.
- Raw data will not be stored beyond the processing time unless the client has expressly requested that the recording be stored.

- Audio and video data stored by the client will only be deleted in accordance with the client's instructions or after the end of the contract in accordance with § 10 AVV.

8. Data Separation Requirement

Measures to ensure separate processing of data for different controllers:

- Logical separation of data through distinct databases or directories.
- Access restrictions based on client-specific (tenant) permissions.
- Strict segregation of development and production environments.
- Video recordings are stored and processed separately for each client.

9. Encryption

Measures to ensure data confidentiality:

- Encryption of stored data using AES-256.
- Use of modern encryption standards for data transmission (e.g., HTTPS).
- Encryption of mobile storage media (e.g., USB sticks, laptops).
- Video recordings are stored in encrypted form (AES-256).
- Access to encrypted data is restricted to designated, authorized entities.

10. Measures in the Event of Disruptions and Data Breaches

- Implementation of an incident management process for reporting and handling data protection incidents.
- Immediate notification of the controller in the event of a data breach, in accordance with Art. 33 GDPR.
- Documentation of security incidents and the corrective actions taken.

11. Awareness and Training of Employees

- Regular training on data protection and information security.
- Confidentiality obligations for all employees with access to personal data.
- Monitoring and enforcement of compliance with security policies by employees.
- Reporting of any incidents, including unauthorized access or unlawful use of video recordings.

These measures are reviewed regularly and adapted to reflect the current state of the art and the requirements of the controller. Any changes or additions to this Annex shall be agreed upon in writing.