Anlage 1: Technische und organisatorische Maßnahmen

1. Zugangskontrolle (Hosting-Standort)
Die physische Zugangskontrolle wird durch unseren Cloud-Hosting-Dienstleister in Deutschland (Hetzner Online GmbH) sichergestellt. Der Standort der eingesetzten Rechenzentren ist Falkenstein, Deutschland. Dieser ist verpflichtet, Rechenzentren mit hohen Sicherheitsstandards zu betreiben (z. B. ISO 27001) und vor unbefugtem Zugang zu schützen.

2. Zugriffskontrolle (logisch)
Der Zugang zur KI-Anwendung wird durch folgende Maßnahmen gesichert:

- Authentifizierung: Kunden (Auftraggeber) laden die KI in ihre Meetings über registrierte Konten ein. Unautorisierte Zugriffe sind ausgeschlossen.
- Verschlüsselung: Die Übertragung aller Daten erfolgt ausschließlich über verschlüsselte Kanäle (z. B. HTTPS).
- Zugriffsprotokollierung: Alle Anfragen werden protokolliert und auf mögliche Missbrauchsmuster hin überwacht.
- Zugriff auf gespeicherte Videoaufnahmen erfolgt nur durch berechtigte Nutzer gemäß Berechtigungskonzept.
- Gespeicherte Videos sind verschlüsselt und können nur durch autorisierte Instanzen entschlüsselt werden.
- Alle Arbeitsplatzrechner sind zentral über Microsoft Intune verwaltet, wodurch Sicherheitsrichtlinien und Gerätekonfigurationen einheitlich umgesetzt werden.
- Zusätzlich ist Microsoft Defender for Endpoint auf allen Geräten aktiv, um erweiterte Bedrohungserkennung und -abwehr zu gewährleisten.
- Microsoft Defender Antivirus ist auf allen Endgeräten installiert und durchgehend aktiviert.

3. Weitergabekontrolle
Maßnahmen zur Sicherstellung der geschützten Übertragung und Speicherung von Daten:

- Verschlüsselung von Datenübertragungen mit TLS 1.3/SSL.
- Sicherstellung der Protokollierung bei Datenweitergaben.
- Übermittlung personenbezogener Daten an Dritte nur mit vorheriger Zustimmung des Auftraggebers.
- Einsatz von VPNs für sichere Remote-Verbindungen.

- Keine Weitergabe von Videoaufzeichnungen an Dritte ohne explizite Anweisung des Auftraggebers.
- Verarbeitung der Videoaufnahmen erfolgt ausschließlich innerhalb der vorgesehenen Systeme.

4. Eingabekontrolle
Maßnahmen zur Nachvollziehbarkeit der Verarbeitung personenbezogener Daten:

- Protokollierung aller Eingaben, Änderungen und Löschungen von personenbezogenen Daten.
- Dokumentation von Nutzeraktivitäten in Audit-Logs.
- Schulung der Mitarbeiter zur ordnungsgemäßen Datenverarbeitung.
- Dokumentation von Zugriffen auf gespeicherte Videoaufnahmen.
- Transparente Kennzeichnung der Verarbeitung von Videodaten in Systemprotokollen.

5. Auftragskontrolle
Maßnahmen zur Sicherstellung der weisungsgemäßen Datenverarbeitung:

- Verarbeitungen erfolgen ausschließlich gemäß den Weisungen des Auftraggebers (Art. 28 DSGVO).
- Schulung der Mitarbeiter zu den Weisungen und der DSGVO.
- Regelmäßige Überprüfung der Einhaltung durch interne Audits.
- Nutzung der Videoaufnahmen ausschließlich für die Transkription, keine Speicherung über die vereinbarten Fristen hinaus.

6. Verfügbarkeitskontrolle
Maßnahmen zur Sicherung der Verfügbarkeit und des Schutzes vor Datenverlust:

- Mindestens tägliches Voll-Backup der Systeme, ergänzt um ein fortlaufendes Transaktionslog-Archiv, das eine Wiederherstellung auf nahezu jeden Zeitpunkt ermöglicht. Die Sicherungen erfolgen auf eine räumlich getrennte Storage-Instanz in Deutschland und sind mit AES-256 verschlüsselt.
- Einsatz redundanter Systeme: Hardware-Redundanz am Datenbankserver (RAID, ECC-Arbeitsspeicher), Datenbank-Cluster mit Replikation und automatischem Failover sowie ein lastverteilter, redundanter Anwendungs-Tier mit unterbrechungsfreiem rollierendem Deployment.
- Notfallpläne und regelmäßige Tests von Wiederherstellungsmaßnahmen.
- Sicherstellung, dass Video- und sonstige Aufnahmen in keiner Form verfügbar sind, nachdem der Auftraggeber die Löschung dieser Daten veranlasst hat

7. Umgang mit temporären Rohdaten (Audio-/Videoaufnahmen):

- Rohdaten, die ausschließlich zur Durchführung der Transkription und Analyse verarbeitet werden, werden nach Abschluss des jeweiligen Verarbeitungsvorgangs automatisch gelöscht.
- Eine Speicherung von Rohdaten über den Verarbeitungszeitpunkt hinaus erfolgt nicht, es sei denn, der Auftraggeber hat die Speicherung der Aufnahme ausdrücklich gewünscht.
- Kundenseitig gespeicherte Audio- und Videodaten werden ausschließlich nach Weisung des Auftraggebers gelöscht oder nach Vertragsende gemäß § 10 AVV.

8. Trennungsgebot

Maßnahmen zur getrennten Verarbeitung von Daten für unterschiedliche Auftraggeber:

- Logische Trennung der Daten durch unterschiedliche Datenbanken oder Verzeichnisse.
- Zugriffsbeschränkungen basierend auf den Mandantenrechten.
- Strikte Trennung von Entwicklungs- und Produktionssystemen.
- Videoaufnahmen werden mandantengetrennt gespeichert und verarbeitet.

9. Verschlüsselung

Maßnahmen zur Sicherstellung der Vertraulichkeit der Daten:

- Verschlüsselung gespeicherter Daten mit AES-256.
- Nutzung moderner Verschlüsselungsstandards für Datenübertragungen (z. B. HTTPS).
- Verschlüsselung mobiler Datenträger (z. B. USB-Sticks, Laptops).
- Videoaufzeichnungen werden verschlüsselt gespeichert (AES-256).
- Zugriff auf verschlüsselte Daten erfolgt nur durch dedizierte, autorisierte Instanzen.
- Die Schlüssel für die Verschlüsselung im Ruhezustand werden vom Auftragsverarbeiter erzeugt und ausschließlich von diesem verwahrt. Sie werden nicht an den Infrastrukturanbieter weitergegeben und liegen dort nicht im Klartext vor; der Infrastrukturanbieter hat weder Zugriff auf die Schlüssel noch auf entschlüsselte Daten im Ruhezustand. Der Schlüsselwechsel erfolgt nach einem definierten Intervall, jährlich sowie anlassbezogen, in einem dokumentierten Verfahren.

10. Maßnahmen bei Störungen und Datenschutzverletzungen

- Einrichtung eines Prozesses zur Meldung und Bearbeitung von Datenschutzvorfällen (Incident Management).
- Unverzügliche Benachrichtigung des Auftraggebers im Fall von Datenpannen gemäß Art. 33 DSGVO.
- Dokumentation von Sicherheitsvorfällen und ergriffenen Maßnahmen.

11. Sensibilisierung und Schulung von Mitarbeitern

- Regelmäßige Schulungen zum Datenschutz und zur Informationssicherheit.
- Vertraulichkeitsverpflichtung aller Mitarbeiter, die Zugriff auf personenbezogene Daten haben.
- Prüfung und Überwachung der Einhaltung von Sicherheitsrichtlinien durch die Mitarbeiter.
- Meldung eines Vorfalls auch, wenn es sich um unbefugten Zugriff oder eine unrechtmäßige Nutzung von Videoaufnahmen handelt.

Diese Maßnahmen werden regelmäßig überprüft und an den Stand der Technik sowie an die Anforderungen des Auftraggebers angepasst. Änderungen oder Ergänzungen dieser Anlage werden schriftlich vereinbart.

12. Bezug zu besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO)

Die in dieser Anlage beschriebenen technischen und organisatorischen Maßnahmen sind auch mit Blick auf die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO gestaltet und werden im Hinblick auf das erhöhte Schutzbedürfnis dieser Datenkategorien als angemessen bewertet. Dies gilt insbesondere für folgende Maßnahmen:

- Verschlüsselung gespeicherter Daten mit AES-256 sowie Transportverschlüsselung mit TLS 1.3
- Rollenbasierte Zugriffskontrolle (RBAC) und strikte Mandantentrennung
- Verarbeitung ausschließlich durch ein selbst betriebenes Sprachmodell auf eigener Infrastruktur in Deutschland; eine Übermittlung an externe Anbieter von Sprachmodellen findet nicht statt
- Umfassende Zugriffsprotokollierung und revisionssichere Nachvollziehbarkeit
- Vertraglich abgesicherte Vertraulichkeitsverpflichtung aller Mitarbeitenden mit Zugriff auf Kundendaten

Die Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 2 DSGVO liegt beim Verantwortlichen und ist von diesem im

Einzelfall zu prüfen und sicherzustellen. Der Auftragsverarbeiter nimmt keine eigene inhaltliche Bewertung der bereitgestellten Daten hinsichtlich ihrer Zugehörigkeit zu besonderen Kategorien vor.