# Technisch - organisatorische Maßnahmen

## § 1 Technische und organisatorische Sicherheitsmaßnahmen

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass dieVerarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte derbetroffenen Person in angemessener Form gewährleistet ist.

## § 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragsverarbeiters

Der Auftragsverarbeiter wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie denbesonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nachder Art der zu schützenden Daten oder Datenkategorien geeignet sind.

## § 3 Konkretisierung der Einzelmaßnahmen

(1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

| Nr. | Maßnahme | Umsetzung der Maßnahme |
|---|---|---|
| 1. | **Zutrittskontrolle**<br>Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren. | Zutrittskontrollsystem (mit Datenbank mit Protokollierung der Schlüsselbenutzungen), Schlüsselvergabe, Türsicherung |
| 2. | **Zugangskontrolle**<br>Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. | Passwörter mit Mindestanforderungen (8 Zeichen, 1 Nummer, 1 Kleinbuchstaben, 1 Großbuchstaben, 1 Sonderzeichen) organisationsweit und in der Anwendung, Zwei-Faktor-Authentifizierung für die Cloud, Verwendungen von AWS Cognito als Identitätsspeicher mit verschlüsselter Übertragung der Daten (TLS 1.2) und verschlüsselter Speicherung der Zugänge im Ruhezustand bei Nutzerdaten |

| Nr. | Maßnahme | Umsetzung der Maßnahme |
|---|---|---|
| 3. | **Zugriffskontrolle**<br>Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. | Die Zugriffskontrolle wird durch ein zentrales rollenbasiertes Berechtigungsmanagement (RBAC) mit minimalen Zugriffsrechten sichergestellt. Die Verwaltung der Berechtigungen erfolgt ausschließlich durch autorisierte Administratoren nach dem Need-to-Know-Prinzip. Alle administrativen Zugriffe und Änderungen an Berechtigungen werden systemseitig protokolliert. Die Datenübertragung erfolgt durchgehend verschlüsselt, und die Zugriffsberechtigungen werden regelmäßig durch die IT-Administration überprüft und angepasst. |
| 4. | **Weitergabekontrolle**<br>Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. | Die Übertragung aller personenbezogenen Daten erfolgt ausschließlich verschlüsselt über HTTPS mittels TLS 1.2/1.3. Die interne Datenspeicherung und -übertragung ist durch Verschlüsselung nach aktuellem Stand der Technik geschützt. Datenübermittlungen an Dritte werden dokumentiert und erfolgen nur auf Basis einer rechtlichen Grundlage. Die Übermittlungswege werden regelmäßig auf ihre Sicherheit überprüft und bei Bedarf aktualisiert. |
| 5. | **Eingabekontrolle**<br>Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. | Alle Eingaben, Änderungen und Löschungen von personenbezogenen Daten werden im System automatisch protokolliert (Logging). Diese Protokollierung umfasst den Zeitpunkt, die Art der Aktion und den durchführenden Mitarbeiter. Die Protokolldaten sind vor nachträglicher Manipulation geschützt und können nur von autorisierten Administratoren eingesehen werden. Wartungs- und Servicezugriffe durch IT-Dienstleister werden ebenfalls vollständig protokolliert und dokumentiert. |
| 6. | **Auftragskontrolle**<br>Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können. | Abgrenzen der Kompetenz zwischen Verantwortlichem und Auftragsverarbeiter (AVV mit Cloud- und KI-Dienstleistern) |
| 7. | **Verfügbarkeitskontrolle**<br>Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. | AWS/ OVH Cloud stellt mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Von der Datenbank wird 1 Mal täglich ein Backup gemacht. Das Recovery-Konzept wird einmal pro Quartal geübt. Datenbank-Backups werden 3 Tage aufbewahrt und anschließend automatisch gelöscht. |

| Nr. | Maßnahme | Umsetzung der Maßnahme |
|---|---|---|
| 8. | **Trennungskontrolle**<br>Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. | Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden getrennt verarbeitet, Mandantenfähigkeit, Funktionstrennung zwischen<br>Produktions- /Testumgebung durch Staging Server. |
| 9. | **Regelmäßige Untersuchung zur Wirksamkeit der Maßnahmen** | Die Wirksamkeit der Technischen und Organisatorischen Maßnahmen wird mindestens einmal jährlich überprüft. Diese Überprüfung erfolgt durch interne Audits und Penetrationstests, die durchgeführt werden.<br>Alle Feststellungen aus den Prüfungen werden dokumentiert, bewertet und führen bei Bedarf zu Maßnahmen zur kontinuierlichen Verbesserung. |
| 10. | **Incident-Response-Management** | Ein Incident-Response-Management-Prozess ist etabliert, der folgende Punkte umfasst:<br>● Meldung und Dokumentation: Sicherheitsvorfälle werden über ein<br>zentralisiertes System (Ticketing-System) erfasst.<br>● Untersuchung: Vorfälle werden von dem Entwicklungsteam analysiert, und entsprechende Gegenmaßnahmen werden eingeleitet.<br>● Eskalation: Kritische Vorfälle werden unverzüglich an die Geschäftsführung und den Datenschutzbeauftragten gemeldet. Betrifft ein Vorfall Daten des Verantwortlichen, wird dieser gemäß § 6 Abs. 2 AVV informiert. Meldungen an Aufsichtsbehörden für den Verantwortlichen erfolgen nur auf dessen Weisung (§ 6 Abs. 3 AVV).<br>● Lessons Learned: Nach jedem Vorfall werden Analysen durchgeführt und Präventivmaßnahmen implementiert.<br>● Schulungen: Alle notwendigen Mitarbeiter werden regelmäßig geschult, um potenzielle Sicherheitsvorfälle frühzeitig zu erkennen und korrekt zu melden. |
| 11. | **Privacy by Design / Privacy by Default** | Privacy by Design:<br>Datenschutzanforderungen werden bereits in der Konzeptions- und Entwicklungsphase aller Produkte und Systeme berücksichtigt. Es erfolgt<br>eine systematische Risikoanalyse, und technische Schutzmaßnahmen (z. B. Pseudonymisierung, Verschlüsselung) werden direkt implementiert.<br>Privacy by Default:<br>Alle Systeme und Anwendungen sind standardmäßig so konfiguriert, dass<br>sie nur die für den jeweiligen Zweck erforderlichen personenbezogenen<br>Daten verarbeiten. Es werden keine unnötigen Daten erhoben oder gespeichert. Benutzer können Datenschutzpräferenzen einfach und intuitiv einstellen. |

| Nr. | Maßnahme | Umsetzung der Maßnahme |
|---|---|---|
| 12. | **Schutz besonderer Kategorien personenbezogener Daten**<br>Biometrische Daten nach Art. 9 Abs. 1 DSGVO sind besonders zu schützen. | Die Funktion „Sprecherwiedererkennung“ ist standardmäßig deaktiviert und wird nur auf Weisung des Verantwortlichen aktiviert (§ 2 Abs. 5 AVV). Erzeugung und Abgleich der Stimmschlüssel erfolgen mit einem selbst betriebenen Modell in einer eigenen Azure-Umgebung. Stimmschlüssel werden innerhalb der OVH Cloud in Frankfurt verschlüsselt (AES-256) gespeichert. Der Zugriff ist auf Administratoren beschränkt. Stimmschlüssel werden ausschließlich zur Wiedererkennung der Sprecher verwendet, nicht zum Training von KI-Modellen. Sie werden gelöscht, sobald der Verantwortliche sie löscht oder die Funktion deaktiviert, spätestens mit Beendigung der Leistungsvereinbarung. |
| 13. | **Mobiles Arbeiten / Homeoffice**<br>Auch außerhalb der Betriebsräume ist ein gleichwertiges Schutzniveau sicherzustellen. | Mobiles Arbeiten erfolgt ausschließlich innerhalb der EU/ des EWR (§ 3 Abs. 9 AVV) und ausschließlich auf dienstlichen Endgeräten. Diese sind vollständig verschlüsselt und zentral über ein MDM verwaltet. Der Zugriff auf Systeme erfolgt über verschlüsselte Verbindungen / VPN mit Zwei-Faktor-Authentifizierung. Es gelten automatische Bildschirmsperren sowie keine Ausdrucke oder lokale Speicherung von Kundendaten. Beschäftigte sind zu Vertraulichkeit gegenüber Dritten im häuslichen Umfeld verpflichtet. |

(2) Änderungen, die den Datenschutz betreffen, werden dem Vertragspartner per E-Mail mitgeteilt. Wenn gewünscht,
kann gemeinsam eine erneute Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden
technischen und organisatorischen Maßnahmen durch die Vertragsparteien in dem Fall vorgenommen werden.

(3) Weiter Vorkehrungen:

- Die von SpeechMind genutzten Cloud Anbieter AWS, OVH und Azure sind nach den folgenden Normen zertifiziert:
  o ISO 27001 für technische Maßnahmen
  o ISO 27017 für Cloud-Sicherheit
  o ISO 27018 für Cloud-Datenschutz
  o SOC 1, SOC 2 und SOC 3, PCI DSS Level 1,
  o BSIs Cloud Computing Compliance Controls Catalogue (C5)
  o ENS Hoch
- Alle Sprachdaten werden mittels Server-side encryption mit 256-bit Advanced Encryption Standard (AES-256) verschlüsselt abgespeichert
- Es besteht die Möglichkeit der Überwachung von Berechtigungen und auch die Möglichkeit, als Administrator Rechte zu entziehen.
- Einem Benutzer, der nicht mehr der Organisation angehört, kann der Zugriff auf die Daten entzogen werden.

- Die Datenübertragbarkeit nach DSGVO wird mittels Exports von JSON Dateien gewährleistet (Exportfunktion). Der Auskunftsanspruch aus der DSGVO ist damit bei entsprechendem Wunsch erfüllbar.
- Die Löschfrist für Aufzeichnungen ist durch den Verantwortlichen in der Software-Anwendung einstellbar (tagesgenau von einem Tag bis max zwei Jahre). Zudem ist eine manuelle Löschung jederzeit möglich. Nach Ablauf der eingestellten Frist werden die Daten automatisch gelöscht. Spätestens mit Beendigung der Leistungsvereinbarung werden sämtliche Daten gemäß § 7 Abs. 2 AVV gelöscht.
- Es werden keine Kundendaten zum Training des KI-Modells verwendet.

# § 4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

(1) Datenschutzschulungen und Geheimhaltung
Jährliche Datenschutzschulungen werden für alle Mitarbeitenden durchgeführt, um das Bewusstsein und Verständnis für den Umgang mit personenbezogenen Daten gemäß den aktuellen Datenschutzgesetzen zu fördern. Alle Mitarbeiter sind vertraglich zur Geheimhaltung und zum vertraulichen Umgang mit allen sensiblen und personenbezogenen Daten verpflichtet.

(2) Benennung und Rolle des Datenschutzbeauftragten (DSB)
Der Auftragsverarbeiter hat einen Datenschutzbeauftragten benannt (§ 4 Abs. 3 AVV), der die Einhaltung der Datenschutzvorschriften überwacht. Diese Maßnahme ist sowohl im Vertrag fixiert als auch in den TOMs dokumentiert, um die aktive Rolle des DSB in unseren Datenschutzpraktiken zu unterstreichen.

(3) Evaluierung und Implementierung einer Datenschutzmanagement Software
Die Evaluierung zur Auswahl einer geeigneten Datenschutzmanagement-Software wird durchgeführt, um unsere Datenschutzverfahren zu unterstützen und zu optimieren. Die Entscheidung und Implementierung werden dokumentiert und in die laufenden Prozesse integriert.

(4) Zentrale Dokumentation
Ein zentrales Verfahrensverzeichnis sowie umfassende Regelungen zum Datenschutz werden stetig geführt und aktualisiert. Diese Dokumentation ist zugänglich für den Datenschutzbeauftragten und autorisierte Personen, um eine konsistente Handhabung personenbezogener Daten zu gewährleisten.

(5) Datenschutzfolgenabschätzung (DSFA)
Die DSFA kann als Grundlage für die interne Abschätzung des Unternehmens von SpeechMind erfragt werden.

(6) Etablierung von Prozessen bei Datenschutzvorfällen und Auskunftsersuchen
Es sind klare Prozesse für den Umgang mit Datenschutzverletzungen und Auskunftsersuchen etabliert. Verletzungen des Schutzes personenbezogener Daten werden unverzüglich intern an den Datenschutzbeauftragten gemeldet und dem Verantwortlichen gemäß § 6 Abs. 2 AVV unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung, mitgeteilt, damit dieser seine Meldefrist nach Art. 33 Abs. 1 DSGVO einhalten kann.

(7) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und

Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.