Vereinbarung

über die

Auftragsverarbeitung nach Art. 28 DSGVO

Datum der Veröffentlichung der aktuellen Version: 06.08.2026

Der Verantwortliche

Für die Verarbeitung Verantwortlicher Kunde

(im Folgenden Auftraggeber)

Der Auftragsverarbeiter
fonio GmbH
Neustiftgasse 73-75/3/7
1070 Wien
Wien
Österreich
(im Folgenden Auftragnehmer)

Falls zwischen Auftraggeber und Auftragnehmer nicht anders vereinbart, ist diese Auftragsverarbeitungsvereinbarung integraler Bestandteil der allgemeinen Geschäftsbedingungen des Auftragnehmers, die unter https://www.fonio.ai/agbs abrufbar sind. Diese AVV gilt zwischen Auftraggeber und Auftragnehmer immer dann, wenn der Auftragnehmer im Rahmen der Bereitstellung seiner Dienste personenbezogene Daten im Auftrag des Auftraggebers verarbeitet.

1. HINTERGRUND UND SPEZIFIKATION DER DATENVERARBEITUNG

1.1 Der Auftragnehmer ist ein Unternehmen, welches folgende Leistungen anbietet:

- Konfigurieren, Verwalten und Bereitstellen eines KI-Telefonie-Assistenten über die B2B fonio.ai Web-App

1.2 Der Auftraggeber ist ein Unternehmen, welches plant, die Dienstleistungen des Auftragnehmers in den genannten Bereichen in Anspruch zu nehmen.

1.3 Diese Auftragsverarbeitungs-Vereinbarung legt die Bedingungen für die Verarbeitung personenbezogener Daten durch den Auftragnehmer unter Billigung des Auftraggebers in Übereinstimmung mit der Datenschutzgrundverordnung (DSGVO) fest. Der Auftragnehmer handelt als Auftragsverarbeiter im Sinne der DSGVO.

2. ART, ZWECK, GEGENSTAND UND RECHTSGRUNDLAGE DER DATENVERARBEITUNG

2.1 Die Leistungen des Auftragnehmers sind in den allgemeinen Geschäftsbedingungen (AGBs) des Auftragnehmers, aufrufbar unter https://www.fonio.ai/agbs beschrieben.

2.2 Im Zuge der Leistungserbringung stellt der Auftraggeber dem Auftragnehmer die für die Leistungserbringung erforderlichen personenbezogenen Daten auf dem jeweils für den konkreten

Fall geeigneten Weg zur Verfügung. Beispielsweise auf elektronischem oder physischem Weg, über Gespräche und Analysen, der Ausübung anderer vertraglich geregelter Tätigkeiten, auf mündlichem Weg oder über Software-Tools.

2.3 Die Verarbeitung personenbezogener Daten kann insbesondere durch Organisation, Ordnen, Speicherung sowie gegebenenfalls Anpassung oder Veränderung, Abfragen, Verknüpfung, Einschränkung, Löschen, Kombination, Kopieren, Ausblenden, Verbindung, Analyse, Lesen, Empfangen, Senden, Aktualisierung erfolgen, soweit dies jeweils für die Erbringung der vereinbarten Leistungen erforderlich ist.

2.4 Der Zweck der Verarbeitung besteht in der vertraglich festgelegten Leistungserbringung gegenüber dem Auftraggeber.

2.5 Der Auftragnehmer ist nicht verpflichtet, die Rechtmäßigkeit der zugrundeliegenden Datenverarbeitungen des Auftraggebers zu prüfen.

3. BETROFFENE PERSONENBEZOGENE DATEN UND KATEGORIE BETROFFENER PERSONEN

3.1 Im Rahmen der vereinbarten Leistungen können die personenbezogenen Daten verarbeitet werden, die für die Leistungserbringung erforderlich sind. Insbesondere können das die folgenden Daten sein:

- Daten im Zusammenhang mit der Servicequalität
- Rechnungsdaten
- Telefonnummern
- Kontaktdaten
- Daten zum Nutzerverhalten und Interaktionen
- Geräte-Informationen
- Browser-Informationen
- Identifikations-Daten
- Technische Zugangsdaten (zum Beispiel API-Keys)
- Telefonkonversationsdaten
- alle Daten, die die Gesprächsteilnehmer im Rahmen des Gesprächs mit der KI selbsttätig einbringen
- Terminbezogene Daten
- Konfigurationsdaten
- Audio-Sprachdaten
- Informationen, welche per E-Mail übermittelt werden
- Kommunikationsdaten
- Technische Informationen
- Informationen, welche als Freitext zur Verfügung gestellt werden
- Zahlungsdaten
- Log-Daten
- Telefonie-Metadaten
- IP-Adressen
- Persönliche Präferenzen
- Cookies und ähnliche Technologien
- KI-Prompts und andere KI-bezogene Informationen
- Fehlerbezogene technische Daten
- Authentifizierungsdaten
- Für Fehleranalyse relevantes Nutzerverhalten
- Abodaten

- Transaktionsdaten

3.2 Von der Verarbeitung sind grundsätzlich alle für die Erbringung der vereinbarten Leistungen notwendigen besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) umfasst. Insbesondere können die folgenden besonderen Kategorien von personenbezogenen Daten im Rahmen der vereinbarten Leistungserbringung (zum Beispiel für Arztpraxen) verarbeitet werden:

- Gesundheitsdaten

3.3 Von der Verarbeitung sind grundsätzlich alle für die Erbringung der vereinbarten Leistungen notwendigen Kategorien von Betroffenen erfasst. Insbesondere fallen darunter die folgenden Kategorien betroffener Personen:

- Kunden
- Unter Vertrag stehende Dritte des Kunden
- Mitarbeiter des Kunden
- Kunden des Kunden
- Partner des Kunden
- Lieferanten des Kunden

3.4 Angesichts der Art der vereinbarten Leistungen erkennt der Auftraggeber an, dass der Auftragnehmer die Liste der Kategorien betroffener Personen weitgehend weder überprüfen noch pflegen kann. Daher verpflichtet sich der Auftraggeber, den Auftragnehmer über alle erforderlichen Änderungen an der Liste der Kategorien betroffener Personen zu informieren.

3.5 Der Auftragnehmer wird die personenbezogenen Daten des Auftraggebers im Hinblick auf alle vorstehend aufgeführten betroffenen Personen in Übereinstimmung mit den vereinbarten Leistungen verarbeiten. Falls aufgrund von Änderungen an der Liste der Kategorien betroffener Personen Änderungen an den vereinbarten Verarbeitungen erforderlich werden, wird der Auftraggeber dem Auftragnehmer dementsprechende zusätzliche Weisungen erteilen.

3.6 Keine Stimmidentifikation oder Stimmverifikation

(a) Der Auftragnehmer führt im Rahmen der vereinbarten Leistungen keine Stimmidentifikation und keine Stimmverifikation durch. Er erstellt, speichert und vergleicht insbesondere keine Stimmprofile („Voiceprints", Stimm-Templates) und setzt keine technischen Verfahren ein, die auf die eindeutige Identifizierung oder auf die gesprächsübergreifende Wiedererkennung einer natürlichen Person anhand ihrer Stimme gerichtet sind. Audio-Sprachdaten werden ausschließlich zur Sprachein- und -ausgabe sowie zur Transkription (Speech-to-Text/Text-to-Speech) verarbeitet. Eine technisch bedingte Unterscheidung von Gesprächsbeiträgen innerhalb eines einzelnen Gesprächs (z. B. Trennung von Anrufer und Assistent) dient nicht der Identifizierung und ermöglicht keine Wiedererkennung über das jeweilige Gespräch hinaus.

(b) Nach eigenem Verständnis des Auftragnehmers stellen die verarbeiteten Audio-Sprachdaten daher keine biometrischen Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person iSd Art. 4 Nr. 14, Art. 9 Abs. 1 DSGVO dar. Ziffer 3.6 lit. a enthält eine Tatsachenbeschreibung, lit. b eine Rechtsauffassung des Auftragnehmers; eine Garantie oder Zusicherung im Rechtssinne ist damit nicht verbunden. Die datenschutzrechtliche Einordnung der vom Auftraggeber veranlassten Verarbeitungen im Einzelfall obliegt dem Auftraggeber als Verantwortlichem; Ziffer 2.5 bleibt unberührt.

(c) Unberührt bleibt, dass die Verarbeitung aus anderen Gründen besondere Kategorien personenbezogener Daten iSd Art. 9 DSGVO umfassen kann, insbesondere Gesundheitsdaten (Ziffer 3.2), und dass Gesprächsinhalte Rückschlüsse auf solche Daten zulassen können.

4. BEDINGUNGEN DER DATENVERARBEITUNG

4.1 Der Auftragnehmer verpflichtet sich, während der gesamten Leistungserbringung sämtliche Vorgaben der DSGVO einzuhalten.

4.2 Der Auftragnehmer verpflichtet sich, personenbezogene Daten nur auf schriftliche Anweisung in Form eines Vertrags mit dem Auftraggeber zu verarbeiten. Abweichungen von diesen Weisungen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers.

4.3 Der Auftragnehmer verarbeitet die personenbezogenen Daten nach dem Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit c DSGVO und daher nur so weit, als dies zur Erbringung der vereinbarten Leistungen erforderlich ist.

4.4 Der Zugriff auf personenbezogene Daten des Auftraggebers wird ausschließlich jenen Personen erteilt, welche diesen Zugriff aufgrund vertraglicher oder gesetzlicher Bestimmungen benötigen.

4.5 Alle Personen aufseiten des Auftragnehmers, welche Zugriff auf personenbezogene Daten des Auftraggebers haben, sind zur Verschwiegenheit zu verpflichten. Insbesondere bleibt die Verschwiegenheitspflicht der mit dem Datenverkehr beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

Unterliegt der Auftraggeber einer gesetzlichen berufsrechtlichen Verschwiegenheitspflicht, so gilt ergänzend die in Anhang 4 bezeichnete Verpflichtungserklärung zur Verschwiegenheit und zum Datenschutz in der für den Sitzstaat des Auftraggebers vorgesehenen Fassung; sie ist unter der in Anhang 4 angegebenen Fundstelle fassungsgenau abrufbar. Sie gilt mit Vertragsschluss als vereinbart, ohne dass es einer gesonderten Vereinbarung oder einer Unterzeichnung bedarf; eine Gegenzeichnung erfolgt auf Wunsch des Auftraggebers, ist für die Wirksamkeit jedoch nicht erforderlich. Für Auftraggeber mit Sitz in der Schweiz gilt insoweit das Addendum für Kunden mit Sitz in der Schweiz.

4.6 Der Auftragnehmer ist verpflichtet, alle geeigneten, angemessenen und dem Stand der Technik entsprechenden technischen und organisatorischen Maßnahmen zu ergreifen und aufrechtzuerhalten, um die Verfügbarkeit, Vertraulichkeit und Integrität der personenbezogenen Daten zu gewährleisten. Eine Liste der vereinbarten technischen und organisatorischen Maßnahmen ist dieser Auftragsverarbeitungs-Vereinbarung im Anhang 1 beigefügt.

4.7 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung seiner Verpflichtungen aus der DSGVO, insbesondere in Bezug auf die Rechte der betroffenen Personen.

4.8 Sofern gesetzliche Bestimmungen nicht entgegenstehen, wird der Auftragnehmer den Auftraggeber unverzüglich informieren, wenn er eine Information oder Mitteilung einer betroffenen Person, der Datenschutzaufsichtsbehörde oder einer sonstigen Behörde oder eines Dritten erhält und diese Information oder Mitteilung in unmittelbarem oder mittelbarem Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen dieser Auftragsverarbeitungs-Vereinbarung steht.

4.9 Im Zusammenhang mit der beauftragten Datenverarbeitung wird der Auftragnehmer den Auftraggeber – soweit gesetzlich erforderlich – bei der Erstellung und Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten, bei der Durchführung der Datenschutz-Folgeabschätzung sowie gegebenenfalls bei vorherigen Konsultationen mit der Datenschutzaufsichtsbehörde iSv Art. 36 DSGVO unterstützen und alle dafür notwendigen Angaben machen und Informationen erteilen. Darüber hinaus wird der Auftragnehmer ein eigenes Verzeichnis der Verarbeitungstätigkeiten führen und, sofern erforderlich, Datenschutz-Folgenabschätzungen vornehmen und einen Datenschutzbeauftragten bestellen.

4.10 Der Auftragnehmer hat den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 24 Stunden, zu informieren, wenn die an ihn überlassenen personenbezogenen Daten unrechtmäßig verwendet wurden und/oder den Betroffenen Schaden droht. Er stellt dem Auftraggeber alle notwendigen Informationen zur Verfügung, damit der Auftraggeber seinen Meldepflichten gegenüber den betroffenen Personen gemäß den Datenschutzgesetzen nachkommen kann.

4.11 Jede Übermittlung von personenbezogenen Daten durch den Auftragnehmer an ein Drittland oder eine internationale Organisation erfolgt im Einklang mit dem Unions- oder nationalem Recht und muss insbesondere mit den Bestimmungen der DSGVO im Einklang stehen.

4.12 Die Parteien können in Anhang 2 weitere Klauseln zur Erbringung der Dienstleistung der Verarbeitung personenbezogener Daten vereinbaren, sofern diese weder direkt noch indirekt im Widerspruch zu dieser Auftragsverarbeitungs-Vereinbarung stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Person und den durch die DSGVO gewährten Schutz beeinträchtigen.

4.13 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

5. SUB-AUFTRAGSVERARBEITER

5.1 Je nach vertraglich vereinbarter Leistungserbringung wird eine spezifische Liste zugelassener Subauftragsverarbeiter in die Datenverarbeitung einbezogen.

5.2 Durch die Nutzung von Subauftragsverarbeitern kann eine Datenübertragung in Drittländer erfolgen. Der Auftragnehmer stellt sicher, dass bei einer Übermittlung personenbezogener Daten in Drittländer die Anforderungen der Art. 44–49 DSGVO eingehalten werden und informiert den Auftraggeber über die jeweils eingesetzten Garantien (z. B. Standardvertragsklauseln, Angemessenheitsbeschluss).

5.3 Eine Liste der vom Auftraggeber bei Abschluss der Vereinbarung genehmigten Sub-Auftragsverarbeiter ist in Anhang 3 enthalten.

5.4 Zwischen dem Auftragnehmer und dem Subauftragsverarbeiter muss ein Vertrag gemäß Art. 28 Abs. 4 DSGVO geschlossen werden. Der Subauftrag muss den datenschutzrechtlichen Bestimmungen im selben Umfang Rechnung tragen, wie diese zwischen dem Auftraggeber und dem Auftragnehmer in dieser Vereinbarung vereinbart wurden, und die Datenverarbeitung darf nur zu dem in der jeweils gesondert beauftragten Leistung angegebenen Zweck erfolgen.

5.5 Der Auftragnehmer hat die Subauftragsverarbeiter regelmäßig auf die Einhaltung der nach dieser Auftragsverarbeitungsvereinbarung geltenden Datenschutzpflichten zu prüfen. Sollte dem Auftragnehmer im Rahmen dieser Prüfung zur Kenntnis gelangen, dass der Subauftragsverarbeiter die ihm nach dieser Auftragsverarbeitungsvereinbarung treffenden Datenschutzpflichten nicht oder nicht ausreichend erfüllt, hat er den Auftraggeber unaufgefordert und umgehend darüber zu informieren.

5.6 Die Weitervergabe an Subauftragsverarbeiter oder die Änderung der bestehenden Subauftragsverarbeiter sind zulässig, sofern:

- der Auftragnehmer eine solche Weitervergabe an Subauftragsverarbeiter mindestens zwei Wochen im Voraus schriftlich oder in Textform ankündigt und
- der Auftraggeber nicht binnen zwei Wochen ab Zugang der Ankündigung, bei erstmaliger Datenübermittlung an den Auftragnehmer spätestens bis zu deren Zeitpunkt, schriftlich oder in Textform Einwände gegen die geplante Auslagerung oder Änderung erhebt. Im Falle eines

Widerspruchs gegen die geplante Einbindung oder Änderung eines Subauftragsverarbeiters darf dieser insoweit nicht eingesetzt werden, solange keine Einigung erzielt wurde. Als Änderung im Sinne dieser Ziffer gilt auch die Erweiterung des Einsatzumfangs eines bereits benannten Subauftragsverarbeiters, insbesondere die Aufnahme eines zusätzlichen Verarbeitungsorts in einem Drittland.

6. PRÜFUNG UND EINHALTUNG

6.1 Der Auftragnehmer gestattet dem Auftraggeber oder den von ihm benannten Vertretern die Durchführung von Audits und Inspektionen, um die Einhaltung der Bestimmungen dieser Auftragsverarbeitungsvereinbarung zu überprüfen. Solche Audits sind mit angemessener Vorankündigung durchzuführen und dürfen den Betrieb des Auftragnehmers nicht unangemessen beeinträchtigen. Es ist dem Auftraggeber bekannt, dass allfällige Inspektionen bei Sub-Auftragsverarbeitern direkt mit diesen abzustimmen sind und der Auftragnehmer keinen Einfluss auf die dabei angewendeten Bestimmungen hat.

Die Kosten der Durchführung des Audits trägt der Auftraggeber, es sei denn, das Audit deckt einen schwerwiegenden Verstoß des Auftragnehmers gegen diese AVV auf.

6.2 Alle externen Prüfer unterliegen einer Vertraulichkeitsvereinbarung.

6.3 Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zur Verfügung und arbeitet mit ihm zusammen, um die Einhaltung der DSGVO nachzuweisen.

7. LAUFZEIT UND VERTRAGSENDE

7.1 Diese Auftragsverarbeitungs-Vereinbarung bleibt für die Dauer der Datenverarbeitungstätigkeiten in Kraft und endet mit dem Abschluss der Leistungserbringung oder wie von den Parteien anderweitig vereinbart.

7.2 Bei Beendigung der Auftragsverarbeitungs-Vereinbarung (oder auch jederzeit vorher über entsprechendes Verlangen des Auftraggebers) wird der Auftragnehmer die verarbeiteten personenbezogenen Daten (einschließlich allfälliger Kopien) nach freier Wahl des Auftraggebers entweder selbst vernichten oder zur Gänze an den Auftraggeber übergeben, sofern dem keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung aller Vorgaben. Sollte sich der Auftraggeber hinsichtlich der Vorgehensweise nicht äußern, wird der Auftragnehmer die Daten, vorbehaltlich gesetzlicher Aufbewahrungsauflagen, 30 Tage nach Beendigung der Vereinbarung vernichten.

7.3 Der Auftragnehmer ist gleichermaßen verpflichtet, die Vernichtung oder Übergabe durch allfällige Sub-Auftragsverarbeiter herbeizuführen.

8. SCHLUSSBESTIMMUNGEN

8.1 Änderungen und Ergänzungen dieser Auftragsverarbeitungs-Vereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung, die auch in elektronischer Form (Textform) erfolgen kann, sowie der ausdrücklichen Angabe, dass es sich um eine Änderung oder Ergänzung dieser Auftragsverarbeitungs-Vereinbarung handelt. Dies gilt auch für den Verzicht auf diese Formvorschrift.

Ziffer 2.3 der AGB (Änderung durch Zustimmungsfiktion) findet auf diese Vereinbarung und ihre Anhänge keine Anwendung.

8.2 Diese Auftragsverarbeitungs-Vereinbarung unterliegt dem geltenden Recht in Österreich und ist nach diesem auszulegen. Gerichtsstand ist Wien.

8.3 Sollten einzelne Bestimmungen dieser Auftragsverarbeitungs-Vereinbarung ungültig oder undurchsetzbar sein oder werden, so bleibt der Rest der Auftragsverarbeitungs-Vereinbarung davon unberührt. Diese Bestimmungen gelten als durch gültige und durchsetzbare Regelungen ersetzt, die den von den Vertragsparteien beabsichtigten, wirtschaftlichen Zweck am ehesten erreichen.

Anhang

Anhang 1: Technische und organisatorische Maßnahmen (TOMs)

Technische Maßnahmen

- Betrieb in einem ISO27001-zertifizierten Rechenzentrum: Die fonio-App wird in einem ISO27001-zertifizierten Rechenzentrum betrieben.
  Sicherheitszertifizierungen von Drittanbietern, wie z. B. ISO 27001, belegen, dass eine Organisation einen bestimmten Standard für das Informationssicherheitsmanagement erfüllt. Sie sind ein wichtiges Element, um Vertrauen bei Kunden und Partnern aufzubauen.
- Physische Sicherheit / Zutrittskontrolle zu Büroräumen: Büroräume sind angemessen gegen unbefugten Zutritt geschützt, außerhalb der Geschäftszeiten geschlossen und Besucher dürfen diese nur in ständiger Begleitung betreten.
  Der Schutz von Büroräumen vor unbefugtem Zutritt und die Sicherstellung, dass externe Personen ständig begleitet werden, tragen zum Schutz personenbezogener Daten in Büroräumen bei.
- Strikte Trennung von Produktions- und Testumgebungen: Produktions- und Testumgebungen sind sowohl logisch als auch infrastrukturell strikt voneinander getrennt. Die Verarbeitung tatsächlicher Produktionsdaten (echte personenbezogene Daten) in Staging-Umgebungen ist strengstens untersagt. Sofern Daten für Testzwecke benötigt werden, müssen sie vollständig anonymisiert oder synthetische Daten verwendet werden.
  Strikte Trennung von Produktions- und Testumgebungen: Produktions- und Testumgebungen sind sowohl logisch als auch infrastrukturell strikt voneinander getrennt.
- Firewalls: Firewalls überwachen und kontrollieren den ein- und ausgehenden Netzwerkverkehr und erlauben nur notwendige, explizit autorisierte Verbindungen.
  Firewalls sind Netzwerksicherheitssysteme, die den eingehenden und ausgehenden Netzwerkverkehr auf der Grundlage vordefinierter Sicherheitsregeln überwachen und steuern. Sie bilden eine Barriere zwischen vertrauenswürdigen internen Netzwerksegmenten und nicht vertrauenswürdigen externen Netzwerken, wie dem Internet.
- Netzwerkprotokolle und -konfigurationen nach dem Stand der Technik: Sichere, dem Stand der Technik entsprechende, Netzwerkprotokolle und -konfigurationen werden als Härtungsmaßnahmen eingesetzt, um Daten während der Übertragung zu schützen.
  Sichere Netzwerkprotokolle, wie z. B. Korrekt konfiguriertes, TLS-basiertes HTTPS trägt zum Schutz von Daten während der Übertragung (Data in Transit) bei.
- Netzwerküberwachung: Netzwerkaktivitäten werden kontinuierlich überwacht, um Sicherheitsbedrohungen zu erkennen und darauf zu reagieren.
  Die Netzwerküberwachung ist ein kritischer IT-Prozess, bei dem alle Netzwerkkomponenten wie Router, Switches, Firewalls, Server und VMs kontinuierlich auf Fehler, Sicherheitsvorfälle und Performance-Probleme überwacht und ausgewertet werden, um die Verfügbarkeit der

Systeme aufrechtzuerhalten und zu optimieren. Die frühzeitige Erkennung von Problemen oder Sicherheitsvorfällen kann unerwartete Ausfallzeiten verhindern.

- Systemhärtung: Härtungsmaßnahmen werden für alle relevanten Systeme durch eine sichere Konfiguration auf Grundlage von CIS-Benchmarks und/oder den Empfehlungen des Anbieters umgesetzt.
  Eine sichere Systemkonfiguration bedeutet, Systeme und Software so einzurichten, dass das Risiko einer Ausnutzung durch böswillige Akteure verringert wird. Dies umfasst Maßnahmen wie das Deaktivieren nicht benötigter Dienste, das Einrichten angemessener Benutzerberechtigungen sowie das regelmäßige Aktualisieren der Systeme.
- Malwareschutz: Es wurden Anti-Malware-Maßnahmen implementiert, um Systeme und Daten vor bösartiger Software zu schützen. Dies umfasst die Installation und den Betrieb von Software zur Erkennung von Schadsoftware auf den relevanten Systemen sowie die Überwachung und Bearbeitung von Warnmeldungen, die durch potenziell erkannte Bedrohungen ausgelöst werden.
  Anti-Malware-Maßnahmen umfassen den Einsatz von Software-Tools zur Erkennung und Entfernung von Schadsoftware, die die Systemsicherheit und Datenintegrität gefährden könnte.
- Patch-Management-Prozess: Alle Software- und Hardwarekomponenten werden regelmäßig über einen dedizierten Patch-Management-Prozess aktualisiert, um sie vor bekannten Schwachstellen zu schützen. Patches werden je nach Systemtyp in unterschiedlichen Intervallen eingespielt, mindestens jedoch einmal pro Quartal sowie unverzüglich, wenn ein Patch eine kritische Schwachstelle behebt.
  Regelmäßige Aktualisierungen von Software und Hardware gewährleisten den Schutz vor bekannten Schwachstellen. Updates enthalten häufig Patches für Sicherheitslücken, die seit der letzten Version der Software oder Hardware entdeckt wurden.
- Identity & Access Management (IAM) und Lifecycle-Prozesse: Ein zentralisiertes Identity- und Access-Management-System (IAM) ist zusammen mit einem strukturierten „Joiner-Mover-Leaver“-Prozess (JML) implementiert.
  Ein integrierter IAM- und JML-Prozess stellt sicher, dass Benutzeridentitäten, Zugriffsrechte und Berechtigungen während des gesamten Beschäftigungslebenszyklus systematisch verwaltet werden – vom Onboarding (Joiner) über interne Rollenwechsel (Mover) bis hin zum Offboarding (Leaver). Bei Beendigung des Arbeits- oder Vertragsverhältnisses werden alle Zugriffsberechtigungen auf personenbezogene Daten und interne Systeme automatisch und unverzüglich entzogen. Dies mindert effektiv das Risiko von „Privilege Creep“ (schleichende Rechteausweitung) und verhindert unbefugten Zugriff durch ehemalige Mitarbeiter oder externe Dienstleister.
- Berechtigungskonzept: Es wurden strenge Zugriffskontrollen auf der Grundlage der Prinzipien „Need-to-Know“ (Kenntnis nur bei Bedarf) und „Least Privilege“ (Minimale Rechtevergabe) für den Zugriff auf personenbezogene Daten implementiert. Wo möglich und sinnvoll, wird eine Multi-Faktor-Authentifizierung (MFA) umgesetzt, und die obligatorische Nutzung von Passwortmanagern sowie die Verwendung von zufällig generierten Passwörtern mit einer Mindestlänge von 20 Zeichen werden eingefordert. Administrative Rechte werden nach dem Vier-Augen-Prinzip vergeben und dürfen nur zu berechtigten Zwecken genutzt werden. Die Nutzung administrativer Rechte wird überwacht.
  Zugriffskontrollen sind Maßnahmen, die definieren, wer auf bestimmte Ressourcen zugreifen darf, wie z. B. personenbezogene Daten, zugreifen darf. Sie sind entscheidend, um unbefugten Zugriff zu verhindern und sicherzustellen, dass nur autorisierte Personen auf Daten zugreifen.
- Beschränkung administrativer Tätigkeiten auf qualifiziertes Personal: Nur speziell geschultes, qualifiziertes und autorisiertes Personal darf administrative Aufgaben an Infrastrukturkomponenten durchführen. Die Autorisierung erfolgt streng auf Basis nachgewiesener fachlicher Kompetenz, und administrative Benutzer sind verpflichtet,

regelmäßige, dokumentierte sicherheitsrelevante Schulungen für administrative Tätigkeiten zu absolvieren.
Die Beschränkung des administrativen Zugriffs auf verifizierte Experten stellt sicher, dass kritische Systemänderungen nur von kompetenten Personen durchgeführt werden. Dies minimiert das Risiko von Sicherheitslücken, Fehlkonfigurationen oder versehentlichem Datenverlust infolge menschlichen Versagens oder mangelnden technischen Fachwissens.

- Sessionmanagement und automatisches Timeout: Benutzer- und Administratorsitzungen in Anwendungen und internen administrativen Systemen werden nach einer vordefinierten Inaktivitätsdauer automatisch beendet.
  Automatische Session-Timeouts mindern das Risiko unbefugten Datenzugriffs, wenn ein Arbeitsplatz oder ein mobiles Gerät in einer unsicheren Umgebung unbeaufsichtigt gelassen wird.
- Umgang mit Anmeldedaten und anderen sensiblen Informationen: Zur Absicherung des Zugriffs auf personenbezogene Daten wird eine Zwei-Faktor-Authentifizierung (2FA) eingesetzt. Anmeldedaten und andere sensible Informationen werden in einem Passwortmanager gespeichert. Alle Zugriffspunkte auf den Passwortmanager sind verschlüsselt.
  Die Zwei-Faktor-Authentifizierung bietet eine zusätzliche Sicherheitsebene, da Benutzer zwei Identitätsnachweise erbringen müssen, bevor sie auf Daten zugreifen können. Dies macht es für unbefugte Personen erheblich schwieriger, Zugriff auf Daten und Systeme zu erlangen.
- Passwort-Management-Tools: Passwort-Management-Tools werden verwendet, um sichere Passwörter für Systeme und Anwendungen gemäß den internen Passwortrichtlinien zu erstellen, zu speichern und zu verwalten.
  Passwort-Management-Tools helfen Benutzern dabei, einzigartige, komplexe Passwörter für verschiedene Konten zu generieren, zu speichern und zu verwalten, wodurch das Risiko der Wiederverwendung von Passwörtern verringert und die allgemeine Passwortsicherheit verbessert wird.
- Datenverschlüsselung: Gespeicherte Daten (Data at Rest) und Daten während der Übertragung (Data in Transit) werden gemäß bewährten Industriepraktiken verschlüsselt, um sie vor unbefugtem Zugriff zu schützen.
  Die Datenverschlüsselung stellt sicher, dass sensible Daten in nicht lesbarer Form auf dem Speichermedium gespeichert und übertragen werden, was sie vor unbefugtem Zugriff schützt, insbesondere im Falle von Diebstahl oder Verlust des Mediums.
- Pseudonymisierung von Daten: Techniken zur Pseudonymisierung personenbezogener Daten werden eingesetzt, um das Risiko von Datenschutzverletzungen zu verringern.
  Die Pseudonymisierung ist ein Verfahren zur De-Identifizierung, bei dem persönliche Identifikationsfelder innerhalb eines Datensatzes durch einen oder mehrere künstliche Identifikatoren oder Pseudonyme ersetzt werden.
- Protokollierung (Audit Logs): Es werden Audit-Logs geführt, um aufzuzeichnen, wer wann auf welche personenbezogenen Daten zugegriffen hat. Darüber hinaus werden sicherheitsrelevante Protokolle unveränderlich gespeichert.
  Audit-Logs zeichnen auf, wann Benutzer auf Systeme und Daten zugreifen. Dies kann im Falle eines Sicherheitsvorfalls von entscheidender Bedeutung sein, da es dabei hilft, die Aktionen nachzuvollziehen und potenzielle Verursacher zu identifizieren.
- Regelmäßige Backups: Daten werden regelmäßig gesichert, wo dies notwendig und angemessen ist, um Datenverlust zu verhindern.
  Regelmäßige Datensicherungen sind von entscheidender Bedeutung, um Datenverlust bei Vorfällen wie Datenschutzverletzungen oder technischen Ausfällen zu verhindern. Sie stellen sicher, dass die Organisation selbst im schlimmsten Fall Daten wiederherstellen und den Geschäftsbetrieb aufrechterhalten kann.
- Automatisiertes Scannen auf Schwachstellen: Automatisierte interne und externe Schwachstellenscans werden regelmäßig über alle Infrastrukturkomponenten, Anwendungen

und Netzwerksegmente hinweg durchgeführt.
Das automatisierte Scannen ergänzt regelmäßige Penetrationstests, indem es neu entdeckte Sicherheitslücken und Fehlkonfigurationen in Echtzeit erkennt und so eine schnelle Behebung durch Patches ermöglicht.

- Penetrationstests: Es werden regelmäßig Penetrationstests durchgeführt, um potenzielle Schwachstellen in Systemen zu identifizieren.
  Penetrationstests, auch bekannt als Pentests, sind simulierte Cyberangriffe auf Informationssysteme und IT-Umgebungen, um ausnutzbare Schwachstellen aufzudecken. Der Prozess umfasst das Sammeln von Informationen über das Ziel vor dem Test, das Identifizieren potenzieller Einstiegspunkte, den Versuch, diese zu durchbrechen, und das Berichten der Ergebnisse.

Organisatorische Maßnahmen

- Informationssicherheitsrichtlinien: Informationssicherheitsrichtlinien sind ausgerollt und werden regelmäßig überprüft und aktualisiert.
  Informationssicherheitsrichtlinien bilden den Rahmen dafür, was von Mitarbeitern und Systemen im Hinblick auf die Informationssicherheit erwartet wird. Die regelmäßige Überprüfung und Aktualisierung dieser Richtlinien stellen sicher, dass sie angesichts der sich wandelnden Bedrohungslage effektiv und relevant bleiben.
- Datenschutzbeauftragter (DSB): Ein Datenschutzbeauftragter (DSB) wurde bestellt, um die Einhaltung der DSGVO zu überwachen.
  Ein Datenschutzbeauftragter ist dafür verantwortlich, die Datenschutzstrategie eines Unternehmens sowie deren Umsetzung zu überwachen, um die Einhaltung der DSGVO-Anforderungen sicherzustellen. Der DSB dient als Ansprechpartner für das Unternehmen, betroffene Personen und Aufsichtsbehörden.
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Privacy by Design und Privacy by Default): Die Grundsätze des Datenschutzes durch Technikgestaltung (Privacy by Design) und durch datenschutzfreundliche Voreinstellungen (Privacy by Default) werden eingehalten.
  Diese Prinzipien beziehen sich auf die Integration des Datenschutzes in Verarbeitungstätigkeiten und Geschäftspraktiken, von der Entwicklungsphase bis hin über den gesamten Lebenszyklus. Dies trägt dazu bei, dass Datenschutz kein nachträglicher Gedanke ist, sondern fest in das Design und die Architektur von IT-Systemen und Geschäftspraktiken eingebettet wird.
- Grundsatz der Datenminimierung: Der Grundsatz der Datenminimierung wird beachtet; es werden nur die personenbezogenen Daten erhoben, die zur Erbringung des Dienstes erforderlich sind.
  Die Datenminimierung ist ein Kernprinzip der DSGVO. Sie besagt, dass eine Organisation nur die personenbezogenen Daten erheben und verarbeiten sollte, die sie für ihren spezifischen Zweck benötigt.
- Verzeichnis von Verarbeitungstätigkeiten (VVT): Wir führen ein DSGVO-konformes Verzeichnis von Verarbeitungstätigkeiten, das alle relevanten Verarbeitungsvorgänge, die damit verbundenen Datenflüsse, beteiligte Dritte und die jeweilige Rechtsgrundlage für die Verarbeitung dokumentiert.
  Ein Verzeichnis der Verarbeitungstätigkeiten schafft Transparenz über Datenflüsse und hilft dabei, potenzielle Risiken bei der Verarbeitung zu identifizieren. Zudem stellt es sicher, dass jede Verarbeitungstätigkeit und Übermittlung personenbezogener Daten auf einer gültigen Rechtsgrundlage beruht.
- Datenschutz-Folgenabschätzungen (DSFA) & Transfer Impact Assessments (TIA): Es werden regelmäßige Datenschutz-Folgenabschätzungen sowie Transfer Impact Assessments (TIAs) durchgeführt, um Risiken sowohl bei der Verarbeitung als auch bei der Übermittlung

personenbezogener Daten über Unternehmens- und Landesgrenzen hinweg zu identifizieren und zu mindern.
Datenschutz-Folgenabschätzungen (DSFAs) und Transfer Impact Assessments (TIAs) identifizieren, bewerten und mindern oder minimieren Datenschutzrisiken bei der Datenverarbeitung. DSFAs und TIAs sind wichtig, da sie Organisationen dabei helfen, Probleme frühzeitig zu erkennen und zu beheben, wodurch die damit verbundenen Kosten und potenzielle Reputationsschäden, die andernfalls entstehen könnten, reduziert werden.

- Risikomanagement für Dienstleister / Auftragsverarbeitungsverträge (AVV): Es werden Überprüfungen der Informationssicherheit von Auftragsverarbeitern durchgeführt und Auftragsverarbeitungsverträge (AVV) abgeschlossen, um die Einhaltung von Sicherheitsstandards zu gewährleisten und vertraglich abzusichern.
  Überprüfungen der Informationssicherheit von Auftragsverarbeitern sind entscheidend, um zu verifizieren, ob Drittdienstleister oder Anbieter dieselben Datenschutz- und Sicherheitsstandards einhalten wie die eigene Organisation. Dies trägt dazu bei, das Risiko von Datenschutzverletzungen oder Datenlecks durch Dritte zu minimieren. Gemäß der DSGVO muss dies formal durch einen Auftragsverarbeitungsvertrag (AVV) geregelt werden.
- Verfahren zum Umgang mit Betroffenenrechten: Es ist ein standardisierter Workflow eingerichtet, um sicherzustellen, dass Anfragen von betroffenen Personen – wie das Recht auf Auskunft, Berichtigung oder Datenübertragbarkeit – überprüft, bearbeitet und innerhalb der gesetzlichen Fristen erfüllt werden.
  Die Einrichtung eines klaren internen Verfahrens für Betroffenenrechte gewährleistet die Einhaltung der Transparenzpflichten nach der DSGVO und verhindert rechtliche Eskalationen sowie Beschwerden bei den Aufsichtsbehörden.
- Mitarbeiterschulungen: Mitarbeiter erhalten regelmäßige Schulungen zum Datenschutz und zur Einhaltung der DSGVO.
  Regelmäßige Schulungen stellen sicher, dass die Mitarbeiter über die Datenschutzgrundsätze sowie ihre Pflichten im Rahmen der DSGVO informiert sind. Dies kann dazu beitragen, durch menschliches Versagen verursachte Datenschutzverletzungen zu verhindern und sicherzustellen, dass Probleme korrekt gemeldet und gelöst werden.
- Kampagnen zur Sensibilisierung für Informationssicherheit: Es werden regelmäßige Kampagnen (Awareness-Schulungen) zur Sensibilisierung der Nutzer für die Informationssicherheit durchgeführt, um die Mitarbeiter über potenzielle Cyberbedrohungen aufzuklären.
  Kampagnen zur Sensibilisierung für Informationssicherheit (Awareness-Schulungen) sind von entscheidender Bedeutung, um Mitarbeiter über Cyberbedrohungen wie Phishing, Social Engineering und Malware aufzuklären und Best Practices im Datenschutz zu fördern.
- Secure-Coding-Schulungen für Entwickler: Softwareentwicklern werden regelmäßig Sicherheitsschulungen angeboten, um sichere Programmierpraktiken zu gewährleisten.
  Regelmäßige Sicherheitsschulungen für Entwickler sind unerlässlich, um das Bewusstsein für die neuesten Sicherheitsbedrohungen und Best Practices für sicher Entwicklung zu schärfen und so die Wahrscheinlichkeit , Schwachstellen in die Software gelangen,zu verringern.
- Löschverfahren (Datenaufbewahrung und -löschung): Auf der Grundlage eines Datenlöschkonzepts werden personenbezogene Daten automatisch gelöscht – sofern gesetzlich zulässig –, sobald der Zweck der Leistungserbringung erfüllt ist oder die betroffene Person dies ausdrücklich verlangt (Recht auf Löschung / Recht auf Vergessenwerden).
  Die regelmäßige Löschung von Daten, die keinen Zweck mehr erfüllen, ist ein wichtiger Bestandteil des Datenmanagements und der DSGVO-Konformität. Sie trägt dazu bei, das Risiko von Datenschutzverletzungen zu verringern, und stellt sicher, dass die Organisation personenbezogene Daten nicht länger als nötig aufbewahrt.
- Reaktionsplan für Sicherheitsvorfälle (Incident Response Plan): Es wurde ein detaillierter Reaktionsplan erstellt, um potenzielle Datenschutzverletzungen oder

Cybersicherheitsvorfälle zu bewältigen, die personenbezogene Daten betreffen.
Ein Incident Response Plan ist ein Regelwerk aus Anweisungen, das dabei hilft, Sicherheitsvorfälle zu identifizieren, darauf zu reagieren und sich davon zu erholen. Ein robuster Plan ist von entscheidender Bedeutung, um die Auswirkungen einer Datenschutzverletzung zu minimieren und eine schnelle Wiederherstellung zu ermöglichen.

- Meldeverfahren für Datenschutzverletzungen: Ein Verfahren zur Meldung von Datenschutzverletzungen ist eingerichtet, um betroffene Personen, Aufsichtsbehörden sowie andere relevante Parteien zu informieren.
  Im Falle einer Datenschutzverletzung verpflichtet die DSGVO Organisationen, die betroffenen Personen und die zuständigen Aufsichtsbehörden zu benachrichtigen. Dieses Verfahren ermöglicht eine rechtzeitige Benachrichtigung und kann dazu beitragen, die Folgen einer Datenschutzverletzung abzumildern.
- Regelmäßige Überprüfung der Datenschutzpraktiken: Die Datenschutzmanagementpraktiken werden in regelmäßigen Abständen überprüft, um die Aktualität und ordnungsgemäße Umsetzung sicherzustellen, und etwaige Abweichungen werden bewertet und behoben.
  Regelmäßige Überprüfungen der Datenschutzpraktiken stellen sicher, dass Änderungen in der Verarbeitung oder Lücken in den Maßnahmen identifiziert und angemessen adressiert werden, um Abweichungen von den DSGVO-Anforderungen zu vermeiden oder gegebenenfalls frühzeitig zu erkennen und zu beheben.

Anhang 2: Ergänzende Bestimmungen

Versionsstand dieses Anhangs: 28.10.2026

- Personenbezogene Daten werden weder vom Auftragnehmer noch von dessen Subprozessoren zum Training, zur Verbesserung oder zur Evaluierung von KI-Modellen verwendet.
- Folgende Standard-Löschfristen werden angewandt:
  - Audio-Aufnahmen: 30 Tage ab Anruf-Ende
  - Transkripte und Zusammenfassungen des Gesprächsverlaufs: 90 Tage ab Anrufende
  - Webchats: 90 Tage je Nachricht ab Nachrichtenerstellung
  - Webchat-Traces: 14 Tage
  - Dialog-Logs und technische Protokolle: 30 Tage ab Anruf-Ende
  - Telefonie-Metadaten: 6 Monate ab Anruf-Ende
  - Buchhaltungsrelevante Belege: 7 Jahre gesetzliche Aufbewahrungsfrist ab Ausstellung
  - Backups: 90 Tage
  - Für etwaige andere Datenkategorien gilt Punkt 7.2 dieser AVV
- Regelungen mit Bezug zu Reseller-Partner
  - Falls diese Auftragsverarbeitungsvereinbarung mit einem Reseller-Partner geschlossen wird, übernimmt fonio die Rolle eines Sub-Verarbeiters für diesen Partner.
  - Bezieht der Auftraggeber die Leistungen über einen Reseller-Partner und verweist der Vertrag zwischen Auftraggeber und Reseller-Partner für die Verarbeitung durch den Auftragnehmer auf diese Auftragsverarbeitungsvereinbarung, gilt diese unmittelbar zwischen Auftraggeber und Auftragnehmer; der vorstehende Punkt findet insoweit keine Anwendung.
  - Erbringt der Reseller-Partner gegenüber dem Auftraggeber eigene Leistungen mit Zugriff auf personenbezogene Daten im Konto des Auftraggebers (insbesondere Support und Implementierung), wird er hierbei unmittelbar für den Auftraggeber tätig. Die hierfür erforderliche Vereinbarung gemäß Art. 28 DSGVO schließt der Auftraggeber mit dem Reseller-Partner ab.

Anhang 3: Sub-Auftragsverarbeiter

Versionsstand dieses Anhangs: 28.10.2026

Klarstellung für Auftraggeber mit Sitz in der Schweiz: Die in diesem Anhang für Übermittlungen in die USA angegebenen Garantien beziehen sich auf das EU-US Data Privacy Framework und die EU-Standardvertragsklauseln. Für Auftraggeber mit Sitz in der Schweiz treten insoweit die schweizerischen Übermittlungsinstrumente an deren Stelle bzw. hinzu, namentlich das Swiss-U.S. Data Privacy Framework (für entsprechend zertifizierte Empfänger; Aufnahme der USA in Anhang 1 der Datenschutzverordnung durch den Bundesrat am 14.08.2024) sowie – für nicht zertifizierte Empfänger und andere Drittländer – die vom EDÖB anerkannten Standardvertragsklauseln (EU-SCC in der Fassung vom 04.06.2021 mit dem sog. „Swiss Finish“). Einzelheiten regelt das Addendum für Kunden mit Sitz in der Schweiz.

Hauptanbieter für die Service-Erbringung

Die folgenden Anbieter werden immer verwendet. Für den Fall, dass ein Fallback-Anbieter auf ausdrücklichen Kundenwunsch als Hauptanbieter gewählt wurde, besteht die Möglichkeit, den vorherigen Anbieter aus der nachfolgenden Hauptanbieterliste ebenfalls auf ausdrücklichen Kundenwunsch nicht zu verwenden.

- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland
  - Bezeichnung der Dienstleistung: System-Hosting
  - Rechtsgrundlage für allfällige Übermittlung in ein Drittland: n/a
  - Serverstandort: Rechenzentren in Nürnberg, Falkenstein und Helsinki werden genutzt.
  - Weiterführende Informationen: https://docs.hetzner.com/cloud/general/locations/
  - BSI C5:2020 Testat vom 02.03.2026: https://files.hetzner.com/docs/BSI-C52020Typ2_Testat_2026.pdf
- OVH GmbH, Christophstraße 19, 50670 Köln, Deutschland (Gesellschaft der OVHcloud-Gruppe; Muttergesellschaft: OVH SAS, 2 rue Kellermann, 59100 Roubaix, Frankreich)
  - Bezeichnung der Dienstleistung: System-Hosting
  - Rechtsgrundlage für allfällige Übermittlung in ein Drittland: n/a
  - Serverstandort: Rechenzentren in Deutschland und Frankreich werden genutzt.
  - Infos zu Zertifizierungen der OVH-Dienste (inkl. BSI:C5 Testat und ISO27001): https://www.ovhcloud.com/de/compliance/
- Twilio Ireland Limited, 25-28 North Wall Quay, D01 H104 Dublin, Ireland
  - Bezeichnung der Dienstleistung: Telefonie
  - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
    - EU-US Data Privacy Framework - https://www.dataprivacyframework.gov/list
    - Swiss-U.S. Data Privacy Framework - https://www.dataprivacyframework.gov/list
    - Binding Corporate Rules sind als nachrangige vertragliche Sicherheitsmaßnahme (Fallback) für den internationalen Datentransfer vereinbart https://www.twilio.com/en-us/legal/bcr/processor
    - Standardvertragsklauseln (Modul 3) inkl. "Swiss Finish" wird zusätzlich vertraglich vereinbart, um den Schutz personenbezogener Daten bei internationalen Datentransfers lückenlos sicherzustellen.
    - Information zur Datenaufbewahrung: Für Audiodaten erfolgt keine Speicherung (Zero-Data-Retention).
  - Serverstandort: EU - Region Irland
  - Weiterführende Informationen: https://www.twilio.com/docs/global-infrastructure/edge-locations

- Voxbone SA, Avenue Louise 489, 1050 Brüssel, Belgien (Gesellschaft der Bandwidth-Unternehmensgruppe; Muttergesellschaft: Bandwidth Inc., 900 Main Campus Drive, Raleigh, NC 27606, USA)
    - Bezeichnung der Dienstleistung: Telefonie / PBX-Telefonie
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - Der Vertrag über die Auftragsverarbeitung wird mit der Voxbone SA (Belgien) geschlossen; die Leistungserbringung für Auftraggeber im EWR erfolgt durch diese Gesellschaft.
        - EU-US Data Privacy Framework - https://www.dataprivacyframework.gov/list
        - Standardvertragsklauseln (Modul 3) inkl. "Swiss Finish" ist zusätzlich vertraglich vereinbart, um den Schutz personenbezogener Daten bei internationalen Datentransfers lückenlos sicherzustellen.
    - Information zur Datenaufbewahrung: Für Audiodaten erfolgt keine Speicherung (Zero-Data-Retention).
    - Serverstandort: Deutschland, Belgien, Irland
- LiveKit Inc., 4285 Payne Avenue, Suite 9154, CA 95157 San Jose, California, Vereinigte Staaten
    - Bezeichnung der Dienstleistung: Virtuelle Gesprächsräume
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - EU-US Data Privacy Framework https://www.dataprivacyframework.gov/list
        - Swiss-U.S. Data Privacy Framework - https://www.dataprivacyframework.gov/list
        - Standardvertragsklauseln (Modul 3) inkl. "Swiss Finish" sind als nachrangige vertragliche Sicherheitsmaßnahme (Fallback) für den internationalen Datentransfer vereinbart.
    - Serverstandort: Durch die Konfiguration von Region Pinning verlassen die Daten nicht die europäische Region. Weiterführende Informationen: https://docs.livekit.io/deploy/admin/regions/region-pinning/
    - Information zur Datenaufbewahrung: Für Audiodaten erfolgt keine persistente Speicherung (Echtzeit-Streaming / ZDR).
- Soniox, Inc. 1045 Helm Ln Foster City, CA 94404 United States
    - Bezeichnung der Dienstleistung: Speech-To-Text
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - Standardvertragsklauseln (Modul 3), vertraglich in der AVV mit Soniox festgelegt.
    - Serverstandort: Verarbeitung im Rahmen des Enterprise Agreements in Europa. Weiterführende Informationen: https://soniox.com/europe
    - Information zur Datenaufbewahrung: Für Audiodaten erfolgt keine Speicherung (Zero-Data-Retention).
- OpenAI Ireland Ltd. 1st Floor, The Liffey Trust Centre 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland
    - Bezeichnung der Dienstleistung: LLM
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - EU-Standardvertragsklauseln (SCC - Modul 3) inkl. "Swiss Finish" , vertraglich in der AVV mit OpenAI festgelegt.
    - Serverstandort: Verarbeitung im Rahmen des Enterprise Agreements in Europa. Weiterführende Informationen: https://openai.com/index/introducing-data-residency-in-europe/.
    - Weitere Informationen: Es wird "Zero Data Retention" angewendet.
- Theai, Inc. dba Inworld AI, 1975 W El Camino Real #300, Mountain View, CA 94040, USA
    - Bezeichnung der Dienstleistung: Text-to-Speech
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - Standardvertragsklauseln (Modul 3) sind für den internationalen Datentransfer vereinbart.

    - Serverstandort: EU-Datenresidenz vereinbart über Enterprise-Vertrag
    - Datenaufbewahrung: Für Audiodaten erfolgt keine Speicherung (Zero-Data-Retention). Weitere Informationen: https://docs.inworld.ai/portal/zero-data-retention
    - Weiterführende Informationen zu Sicherheit und Zertifizierungen: https://trust.inworld.ai/
- Sinch AB (Mailgun), Lindhagensgatan 112, 112 51 Stockholm Schweden
    - Bezeichnung der Dienstleistung: E-Mail-Versand
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - Der DPA wurde mit der Sinch AB in Stockholm geschlossen, welche die Mutter des US-Unternehmens Mailgun Technologies, Inc., 112 E Pecan St #113 San Antonio, TX 78205, United States, ist. Die Mailgun Technologies, Inc. ist Teil des EU-US Data Privacy Frameworks https://sinch.com/legal/terms-and-conditions/other-sinch-terms-conditions/data-processing-agreement/
        - Standardvertragsklauseln (Modul 3) sind als nachrangige vertragliche Sicherheitsmaßnahme (Fallback) für den internationalen Datentransfer vereinbart.
    - Serverstandort: Region "EU". Weiterführende Informationen: https://www.mailgun.com/about/regions/
- New Relic, Inc., 188 Spear Street, Suite 1200, CA94105 San Francisco, California, Vereinigte Staaten
    - Bezeichnung der Dienstleistung: Logging und Monitoring
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - EU-US Data Privacy Framework - https://www.dataprivacyframework.gov/list
        - Swiss-U.S. Data Privacy Framework - https://www.dataprivacyframework.gov/list
        - Standardvertragsklauseln (Modul 3) inkl. "Swiss Finish" sind als nachrangige vertragliche Sicherheitsmaßnahme (Fallback) für den internationalen Datentransfer vereinbart.
    - Serverstandort: Fonio nutzt den europäischen Standort. Weiterführende Informationen: https://docs.newrelic.com/docs/accounts/accounts-billing/account-setup/choose-yourdata-center/

Fallback-Anbieter zur Erhöhung der Verfügbarkeit

Die folgenden Anbieter dienen als Fallback, falls ein Hauptanbieter ausfällt oder die benötigte Servicequalität nicht erbringen kann. Dies dient der Erhöhung der Verfügbarkeit und der Qualität des Services. Der Einsatz von Fallback-Anbietern ist für Berufsgeheimnisträger standardmäßig deaktiviert und kann auf Kundenwunsch aktiviert werden. Für alle anderen Kunden, die keiner Berufsgeheimnispflicht unterliegen, sind Fallback-Anbieter standardmäßig aktiviert, können jedoch auf Kundenwunsch deaktiviert werden. Es besteht die Möglichkeit die genannten Anbieter auf ausdrücklichen Kundenwunsch auch als Hauptanbieter zu verwenden.

- Deepgram, Inc., 548 Market St, Suite 25104, CA 94104-5401 San Francisco, California, Vereinigte Staaten
    - Bezeichnung der Dienstleistung: Speech-to-Text
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - EU-Standardvertragsklauseln (SCC - Modul 3), vertraglich in der AVV mit Deepgram festgelegt.
    - Serverstandort: Verarbeitung durch Enterprise Agreement rein in Europa über eigenen EU-Endpunkt
    - Information zur Datenaufbewahrung: Für Audiodaten erfolgt keine Speicherung (Zero-Data-Retention).

- Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, D04 E5W5, Irland
    - Bezeichnung der Dienstleistung: LLM
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - EU-US Data Privacy Framework - https://www.dataprivacyframework.gov/list
        - Swiss-U.S. Data Privacy Framework - https://www.dataprivacyframework.gov/list
        - Standardvertragsklauseln (Modul 3) inkl. "Swiss Finish" sind als nachrangige vertragliche Sicherheitsmaßnahme (Fallback) für den internationalen Datentransfer vereinbart.
    - Serverstandort: Europa Region
    - Information zur Datenaufbewahrung: Für Audiodaten erfolgt keine Speicherung (Zero-Data-Retention)
- Eleven Labs Inc., 169 Madison Ave #2484, NY 10016 New York, New York, Vereinigte Staaten
    - Bezeichnung der Dienstleistung: Text-to-Speech
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - EU-US Data Privacy Framework https://elevenlabs.io/privacy-policy
        - Standardvertragsklauseln (Modul 3) sind als nachrangige vertragliche Sicherheitsmaßnahme (Fallback) für den internationalen Datentransfer vereinbart.
    - Serverstandort: Im Rahmen eines Enterprise-Vertrags bleiben sämtliche Daten ausschließlich innerhalb Europas. Weiterführende Informationen: https://elevenlabs.io/docs/overview/administration/data-residency
    - Information zur Datenaufbewahrung: Für Audiodaten erfolgt keine Speicherung (Zero-Data-Retention).

Optionale Anbieter

Die folgenden Anbieter werden optional bei der Nutzung von zusätzlichen Serviceangeboten und nur auf ausdrücklichem Kundenwunsch eingesetzt.

- Nylas, Inc., 2100 Geng Rd. #2100, Palo Alto, CA 94303
    - Bezeichnung der Dienstleistung: Kalender-Integration zur Anbindung von Kalenderkonten (Google Calendar, Microsoft Outlook) über OAuth zur Verfügbarkeitsprüfung, Terminbuchung und bidirektionalen Synchronisation von Kalenderereignissen.
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - EU-US Data Privacy Framework - https://www.dataprivacyframework.gov/list
        - Swiss-U.S. Data Privacy Framework - https://www.dataprivacyframework.gov/list
        - Standardvertragsklauseln (Modul 3) sind als nachrangige vertragliche Sicherheitsmaßnahme (Fallback) für den internationalen Datentransfer vereinbart.
    - Serverstandort: Die Data-Residency-Region ist Europa (Irland). Weiterführende Informationen: https://developer.nylas.com/docs/dev-guide/platform/data-residency/
- Meta Platforms Ireland Ltd., Merrion Road, Dublin 4, D04 X2K5, Ireland
    - Bezeichnung der Dienstleistung: WhatsApp-Integration
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - EU-US Data Privacy Framework - https://www.dataprivacyframework.gov/list
        - Swiss-U.S. Data Privacy Framework - https://www.dataprivacyframework.gov/list
        - Standardvertragsklauseln (Modul 3) sind als nachrangige vertragliche Sicherheitsmaßnahme (Fallback) für den internationalen Datentransfer vereinbart.

- SideGuide Technologies, Inc. (Firecrawl), 2261 Market Street STE 85367, CA 94114 San Francisco, United States
    - Bezeichnung der Dienstleistung: Suchmaschine
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - Standardvertragsklauseln (Modul 3) inkl. "Swiss Finish"
- LangChain, Inc., 501 2nd Street, Suite 120, CA 94107 San Francisco, United States
    - Bezeichnung der Dienstleistung: Web-Chat-Integration und Tracing
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - Standardvertragsklauseln (Modul 3)
    - Serverstandort: Es wird der EU-Endpunkt von Langchain verwendet
- Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, D04 E5W5, Irland
    - Bezeichnung der Dienstleistung: Zustellung von Push-Benachrichtigungen an Endgeräte mit Android über Firebase Cloud Messaging (FCM)
    - Einsatz nur falls die fonio Telefon-App verwendet wird und Push-Notifications aktiviert sind
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland:
        - EU-US Data Privacy Framework – https://www.dataprivacyframework.gov/list
        - Swiss-U.S. Data Privacy Framework – https://www.dataprivacyframework.gov/list
        - Standardvertragsklauseln (Modul 3) inkl. „Swiss Finish“ sind als nachrangige vertragliche Sicherheitsmaßnahme (Fallback) für den internationalen Datentransfer vereinbart.
    - Serverstandort: Für Firebase Cloud Messaging steht keine europäische Datenresidenz zur Verfügung; die Zustellung erfolgt über die globale Infrastruktur von Google, einschließlich der Standorte in den Vereinigten Staaten.
    - Weitere Informationen:
        - Bei der Verwendung der Push-Notifications in der fonio-App werden zusätzlich folgende Daten verarbeitet: FCM-Registrierungstoken bzw. Firebase Installation ID, Zustellmetadaten sowie die technischen Verbindungsdaten des Endgeräts (insbesondere die IP-Adresse). Die Benachrichtigungen können zudem Rufnummern, Anrufzusammenfassungen oder Namen enthalten.
        - Information zur Datenaufbewahrung: Push-Benachrichtigungen werden nur für den zur Zustellung erforderlichen Zeitraum vorgehalten.
        - Weiterführende Informationen: https://firebase.google.com/support/privacy
    - Ergänzung zu Push Notifications für iOS-Geräte:
        - Für Endgeräte mit iOS erfolgt die Zustellung über den Apple Push Notification Service. Apple tritt nach unserer Auffassung als eigener Verantwortlicher auf; eine Auftragsverarbeitung liegt insoweit nicht vor, weshalb Apple in diesem Anhang nicht als Subauftragsverarbeiter geführt wird.
- T-Systems International GmbH, Hahnstraße 43d, 60528 Frankfurt am Main, Deutschland
    - Bezeichnung der Dienstleistung: System-Hosting auf der "T Cloud Public"
    - Hinweis: Dieser Anbieter wird exklusiv für Kunden der Deutschen Telekom AG und ihrer Konzerntöchter als alternativer Hosting-Dienst anstelle von Hetzner und OVH bereitgestellt.
    - Rechtsgrundlage für allfällige Übermittlung in ein Drittland: n/a
    - Serverstandort: Niederlande
    - Infos zu Zertifizierungen der T Cloud Public (inkl. ISO/IEC 27001, BSI C5 Typ II Testat, SOC 2...): https://www.t-cloud-public.com/de/produkte-services/core-services/zertifikate

Ergänzungen zu Failover-Mechanismen

Um die Verfügbarkeit unseres Dienstes und dessen Servicequalität sicherzustellen, setzen wir für folgende Anbieter im Falle einer Nichtverfügbarkeit oder unzureichenden Verfügbarkeit der EU-Standorte – und nur dann – ein US-Failover (temporäre Umleitung des Datenflusses des betroffenen Anbieters auf US-Server-Standorte) ein:

- Soniox, Inc
- OpenAI Ireland Ltd.
- Theai, Inc. dba Inworld AI

Failover-Mechanismen werden nur für die minimal notwendige Zeit eingesetzt. Eine Deaktivierung des US-Failovers ist auf Kundenwunsch jederzeit möglich.

Für Berufsgeheimnisträger ist ein US-Failover standardmäßig deaktiviert.

Anhang 4: Verpflichtungserklärung zur Verschwiegenheit und zum Datenschutz

Dieser Vereinbarung werden als Anhang 4 die folgenden Verpflichtungserklärungen zur Verschwiegenheit beigefügt. Der Auftraggeber kann die für ihn einschlägige Fassung ohne inhaltliche Änderung in Anspruch nehmen:

- Verpflichtungserklärung zur Verschwiegenheit und zum Datenschutz – Deutschland (§§ 203, 204 StGB, § 62a StBerG, § 43e BRAO);
- Verpflichtungserklärung zur Verschwiegenheit und zum Datenschutz – Österreich (§ 121 StGB, § 54 ÄrzteG, § 9 RAO, § 80 WTBG 2017, § 6 DSG).

Für Auftraggeber mit Sitz in der Schweiz wird keine gesonderte Erklärung geführt; die entsprechende Regelung (Art. 321 chStGB, Art. 62 revDSG) ist in Ziffer 4 des Addendums für Kunden mit Sitz in der Schweiz enthalten.

Diese Auftragsverarbeitungsvereinbarung wurde mit dem Metasoul AVV-Generator erstellt.