Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO

zwischen
dem jeweiligen Kunden, der Leistungen der Lumitra GmbH in Anspruch nimmt
– nachfolgend „**Verantwortlicher**“ –und

Lumitra GmbH, Heisingerstraße 12, 87437 Kempten (Allgäu), vertreten durch die Geschäftsführer Luis Röder und Noah Rues, – nachfolgend **„Auftragsverarbeiter“** –

– **Verantwortlicher** und **Auftragsverarbeiter** nachfolgend gemeinsam auch **„Vertragsparteien“** genannt –

wird der folgende Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (**„Auftragsverarbeitung“**) geschlossen. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Nutzung des Lumitra-Dienstes zur KI-gestützten Mitschrift von Telefonaten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen (Art. 28 DSGVO).

Dieser Vertrag gilt automatisch mit Abschluss des Nutzungsvertrags bzw. der erstmaligen Nutzung von Diensten, bei denen personenbezogene Daten im Auftrag verarbeitet werden, als geschlossen.

1. Gegenstand und Dauer der Auftragsverarbeitung

1.1 Gegenstand: Der Auftragsverarbeiter erbringt für den Verantwortlichen die Dienstleistung der automatisierten Aufzeichnung und Verarbeitung von Telefongesprächen. Dies umfasst insbesondere die **Audioaufzeichnung von Telefonaten**, die **Transkription der Gespräche** in Textform sowie die **KI-gestützte Zusammenfassung** der Gesprächsinhalte. Der genaue Zweck, die Art der Verarbeitung sowie die Art der personenbezogenen Daten und Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag beschrieben. Der Auftragsverarbeiter verarbeitet die vom Verantwortlichen überlassenen personenbezogenen Daten ausschließlich im Rahmen des genannten Leistungsumfangs und **ausschließlich auf dokumentierte Weisung** des Verantwortlichen. Eine Verarbeitung zu anderen, insbesondere eigenen Zwecken des Auftragsverarbeiters, ist ausgeschlossen. Untersagt ist dem Auftragsverarbeiter auch die Erstellung von Kopien oder Duplikaten der Daten ohne Wissen und Zustimmung des Verantwortlichen, sofern sie nicht für die ordnungsgemäße Auftragsdurchführung oder zur Erfüllung gesetzlicher Aufbewahrungspflichten erforderlich sind. Der Auftragsverarbeiter sichert zu, die zur Auftragsdurchführung verarbeiteten Daten **strikt von sonstigen Datenbeständen** zu trennen, die nicht im Auftrag des Verantwortlichen verarbeitet werden.

1.2 Dauer: Die Auftragsverarbeitung beginnt mit Wirksamwerden des zugrundeliegenden Nutzungsvertrags über den Lumitra-Dienst oder mit Unterzeichnung dieses AVV (je nachdem, was früher erfolgt) und läuft **für die Dauer der Nutzung** des genannten Dienstes durch den Verantwortlichen. Die Laufzeit dieses AVV richtet sich somit nach der Laufzeit des Hauptvertrags (Leistungsvertrags) zwischen den Parteien. Eine ordentliche Kündigung dieses AVV ist nicht separat möglich, sondern nur im Zusammenhang mit der Beendigung des Hauptvertrags. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Bestimmungen dieses Vertrages, die ihrer Natur nach über das Vertragsende hinaus Wirkung entfalten (insbesondere Vertraulichkeit, Löschungspflichten), bleiben auch nach Vertragsbeendigung gültig.

2. Art der verarbeiteten Daten, Zweck der Verarbeitung, Kreis der Betroffenen

Der **Zweck und die Art** der Verarbeitung durch den Auftragsverarbeiter ergeben sich aus dem in Abschnitt 1 beschriebenen Leistungsumfang, nämlich der Gesprächsaufzeichnung, Transkription und Zusammenfassung zu Dokumentationszwecken. Einzelheiten hierzu sowie die **Kategorien der personenbezogenen Daten** und **Kategorien der betroffenen Personen** werden in **Anlage 1** konkretisiert. Der Auftragsverarbeiter verarbeitet **ausschließlich solche Daten**, die der Verantwortliche ihm zur Durchführung der beauftragten Dienste übermittelt oder zugänglich macht, oder die durch die Nutzung des Dienstes erhoben werden. Der Verantwortliche bestätigt, dass diese Vereinbarung auf **alle** Verarbeitungen personenbezogener Daten Anwendung findet, bei denen der Auftragsverarbeiter oder ein von ihm beauftragter Subunternehmer mit personenbezogenen Daten des Verantwortlichen in Berührung kommt.

3. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich, bei der Verarbeitung der personenbezogenen Daten die folgenden Pflichten einzuhalten:

- **Einhaltung einschlägiger Gesetze:** Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten in Übereinstimmung mit den anwendbaren Datenschutzvorschriften, insbesondere der DSGVO und dem Bundesdatenschutzgesetz (BDSG), sowie ausschließlich im Rahmen der in diesem Vertrag getroffenen Vereinbarungen und Weisungen des Verantwortlichen. Sofern der Auftragsverarbeiter der Auffassung ist, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, wird er den Verantwortlichen unverzüglich darauf hinweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung einer offensichtlich rechtswidrigen Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder abgeändert wird. Er darf personenbezogene Daten aus dem Auftrag nicht ohne Weisung des Verantwortlichen an Dritte herausgeben; Anfragen von Betroffenen oder Dritten wird er an den Verantwortlichen weiterleiten (siehe auch Ziff. 8). Sollte der Auftragsverarbeiter gesetzlich (z.B. aufgrund einer behördlichen oder gerichtlichen Anordnung) zu einer weitergehenden Verarbeitung oder Herausgabe von Daten verpflichtet sein, wird er – sofern rechtlich zulässig – den Verantwortlichen vorab über diese Pflicht informieren, damit der Verantwortliche dagegen Rechtsmittel einlegen oder sonst über die Herausgabe entscheiden kann.

- **Vertraulichkeit:** Der Auftragsverarbeiter gewährleistet, dass alle Personen, die von ihm mit der Verarbeitung der personenbezogenen Daten des Verantwortlichen betraut werden, zuvor **auf Vertraulichkeit verpflichtet** wurden oder einer angemessenen gesetzlichen Geheimhaltungspflicht unterliegen (z.B. nach § 53 BDSG oder, sofern einschlägig, **Fernmeldegeheimnis** nach § 88 TKG). Diese Verschwiegenheitspflicht besteht auch nach Beendigung des Vertrags fort. Der Auftragsverarbeiter stellt durch entsprechende interne Regelungen sicher, dass der Zugang zu den personenbezogenen Daten des Verantwortlichen nur solchen Mitarbeitern gewährt wird, die diesen zur Erfüllung der vertraglichen Aufgaben benötigen (Need-to-know-Prinzip). Sofern der Auftragsverarbeiter von weiteren Geheimhaltungspflichten betroffen ist (z.B. Berufsgeheimnisse, besondere Verschwiegenheitspflichten), wird er diese ebenfalls wahren.

- **Technische und organisatorische Maßnahmen:** Der Auftragsverarbeiter hat alle gemäß Art. 32 DSGVO erforderlichen **technischen und organisatorischen Maßnahmen (TOM)** zur angemessenen Sicherung der Verarbeitung getroffen. Diese Maßnahmen sind in **Anlage 3** detailliert beschrieben und bilden einen integralen Bestandteil dieses Vertrags.

Sie umfassen u.a. Maßnahmen zur Sicherung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme. Der Auftragsverarbeiter gewährleistet die laufende Einhaltung und Wirksamkeit der vereinbarten TOM. Maßnahmen können im Laufe der Zeit dem technischen Fortschritt angepasst werden, vorausgesetzt, das Sicherheitsniveau fällt dabei nicht unter das der vereinbarten Maßnahmen. Wesentliche Änderungen der TOM sind dem Verantwortlichen mitzuteilen. Der Auftragsverarbeiter wird dem Verantwortlichen auf Anfrage geeignete Nachweise über die Umsetzung der TOM zur Verfügung stellen (z.B. Zertifizierungen, Auditberichte), sodass sich der Verantwortliche von der Einhaltung der vereinbarten Sicherheitsmaßnahmen überzeugen kann.

- **Mitteilung von Störungen und Pflichtverletzungen:** Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls bei ihm Unregelmäßigkeiten bei der Verarbeitung der Daten auftreten oder er Verstöße gegen diese Vereinbarung oder gegen anwendbare Datenschutzbestimmungen feststellt. Gleiches gilt bei **Kontrollen oder Maßnahmen** einer Datenschutz-Aufsichtsbehörde, die sich auf die Auftragsverarbeitung beziehen; der Auftragsverarbeiter wird den Verantwortlichen hiervon unverzüglich unterrichten.

- **Bestellung eines Datenschutzbeauftragten:** Soweit gesetzlich erforderlich, hat der Auftragsverarbeiter einen Datenschutzbeauftragten gemäß Art. 37 DSGVO bestellt. Die Kontaktdaten des Datenschutzbeauftragten (oder – falls kein Datenschutzbeauftragter bestellt werden muss – einer anderen zuständigen Ansprechperson für Datenschutz beim Auftragsverarbeiter) werden dem Verantwortlichen auf Anfrage mitgeteilt. Der Auftragsverarbeiter stellt sicher, dass der Verantwortliche diesen Ansprechpartner bei allen datenschutzrelevanten Anliegen konsultieren kann.

4. Pflichten des Verantwortlichen

- **Rechtmäßigkeit der Datenverarbeitung:** Der Verantwortliche ist dafür verantwortlich, dass die Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter auf einer **rechtsgültigen Grundlage** im Sinne des Art. 6 DSGVO erfolgt. Er hat insbesondere sicherzustellen, dass etwaige **Einwilligungen** der Telefonteilnehmer zur Aufzeichnung der Gespräche vorliegen oder eine anderweitige Erlaubnis (z.B. auf Grundlage von Art. 6 Abs. 1 lit. b DSGVO bei geschäftlichen Gesprächen zur Vertragserfüllung) gegeben ist, **bevor** er dem Auftragsverarbeiter die Aufnahme und Verarbeitung eines Telefonats gestattet. Der Verantwortliche bleibt alleiniger **Verantwortlicher** für die Verarbeitung im Sinne von Art. 4 Nr. 7 DSGVO und trägt die Verantwortung dafür, dass die **Weitergabe der Daten** an den Auftragsverarbeiter sowie die Nutzung der Ergebnisse (Transkripte, Zusammenfassungen) den gesetzlichen Vorgaben entspricht. Dies umfasst insbesondere die Erfüllung von Informationspflichten gegenüber den betroffenen Personen (Art. 13, 14 DSGVO) und gegebenenfalls die Führung des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO) für den eigenen Verantwortungsbereich.

- **Auswahl und Überwachung des Auftragsverarbeiters:** Der Verantwortliche hat den Auftragsverarbeiter sorgfältig ausgewählt und sich von der ausreichenden Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen überzeugt. Er stellt dem Auftragsverarbeiter nur solche personenbezogenen Daten zur Verfügung, die für den **Zweck der Verarbeitung** erforderlich sind (**Datenminimierung**). Der Verantwortliche hat das Recht, vom Auftragsverarbeiter **Nachweise** über die Einhaltung der in diesem Vertrag vereinbarten Pflichten und Maßnahmen zu verlangen (vgl. Ziff. 11).

Sollte der Verantwortliche Kenntnis von Fehlern oder Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter erlangen (z.B. durch Prüfungen, Auskunft der Betroffenen oder Hinweise Dritter), wird er den Auftragsverarbeiter **unverzüglich und vollumfänglich informieren**.

- **Weisungsrecht:** Der Verantwortliche hat das Recht, dem Auftragsverarbeiter jederzeit **Weisungen** über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Weisungen oder Änderungen/Ergänzungen zu bestehenden Weisungen sind in dokumentierter Form (mindestens Textform) an die vom Auftragsverarbeiter benannte Kontaktstelle zu richten. Mündliche Weisungen sind vom Verantwortlichen unverzüglich schriftlich oder in Textform zu bestätigen. Der Verantwortliche wird Weisungen so erteilen, dass dem Auftragsverarbeiter eine angemessene Umsetzungsfrist bleibt. Der Verantwortliche ist verpflichtet, Weisungen, die zu einer Änderung der im Hauptvertrag vereinbarten Leistung führen könnten, nur im Einvernehmen mit dem Auftragsverarbeiter zu erteilen. Der Verantwortliche trägt etwaige Mehrkosten, die durch zusätzliche Weisungen entstehen, sofern diese nicht aufgrund eines dem Auftragsverarbeiter zuzurechnenden Fehlverhaltens erforderlich werden.
- **Anfragen und Rechte Betroffener:** Der Verantwortliche ist für die Wahrung der Rechte der betroffenen Personen verantwortlich. Er entscheidet über Berichtigungen, Löschungen, Herausgabe oder Einschränkungen von Daten und macht diese Ansprüche gegenüber dem Auftragsverarbeiter geltend. Sofern eine betroffene Person sich unmittelbar an den Verantwortlichen wendet, um ihre Rechte (z.B. Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, Widerspruch oder Widerruf) geltend zu machen, wird der Verantwortliche den Auftragsverarbeiter – soweit dessen Mitwirkung erforderlich ist – unverzüglich einbinden.

5. Unterauftragsverhältnisse (Einsatz von Subunternehmern)

5.1 **Einschaltung von Subunternehmern:** Der Auftragsverarbeiter darf **weitere Auftragsverarbeiter (Subunternehmer)** zur Verarbeitung der Daten des Verantwortlichen nur einsetzen, wenn der Verantwortliche dem **vorab** zugestimmt hat (Art. 28 Abs. 2 DSGVO). Der Verantwortliche erteilt mit Unterzeichnung dieses Vertrags seine Zustimmung zur Einschaltung der in **Anlage 2** aufgeführten Subunternehmer. Diese Liste enthält **Name, Anschrift, Leistung und Standort** der Subunternehmer sowie den Umfang der jeweils ausgelagerten Verarbeitungstätigkeiten. Mit deren Beauftragung durch den Auftragsverarbeiter erklärt sich der Verantwortliche ausdrücklich einverstanden. Der Auftragsverarbeiter informiert den Verantwortlichen **rechtzeitig im Voraus** über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, so dass der Verantwortliche die Möglichkeit zum **Einspruch** gegen diese Änderungen hat (Art. 28 Abs. 2 S. 2 DSGVO). Ein Einspruch ist schriftlich innerhalb von [z.B. 14 Tagen] nach Zugang der Information zu erklären und muss wichtige datenschutzrechtliche Gründe darlegen. Im Falle eines berechtigten Einspruchs wird der Auftragsverarbeiter versuchen, eine zumutbare Alternative zur Auslagerung an den neuen Subunternehmer anzubieten. Ist dies dem Auftragsverarbeiter nicht möglich oder ist dem Verantwortlichen die Fortführung des Vertrags ohne Auswechslung des Subunternehmers nicht zumutbar, haben beide Parteien das Recht, den Hauptvertrag und diesen AVV **außerordentlich** zu kündigen.

5.2 **Pflichten bei Subauftrag:** Der Auftragsverarbeiter ist verpflichtet, mit allen von ihm eingeschalteten Subunternehmern einen der DSGVO und diesem Vertrag **vergleichbaren Auftragsverarbeitungsvertrag** abzuschließen (Art. 28 Abs. 4 DSGVO). Insbesondere muss der

dortige Verarbeitungsumfang, die Weisungsbindung sowie geeignete technische und organisatorische Maßnahmen dem in dieser Vereinbarung für den Auftragsverarbeiter festgelegten Niveau entsprechen. Der Auftragsverarbeiter stellt sicher, dass die **Verpflichtungen aus diesem AVV** – insbesondere die Vorgaben aus Abschnitt 3 (Pflichten des Auftragsverarbeiters) und Abschnitt 7 (TOM) – auch dem Subunternehmer auferlegt werden. Der Auftragsverarbeiter hat die Einhaltung der Pflichten des Subunternehmers regelmäßig zu überwachen. Eine **Weiterleitung von personenbezogenen Daten** an den Subunternehmer darf erst erfolgen, nachdem der Auftragsverarbeiter sich vergewissert hat, dass der Subunternehmer seine Pflichten im Einklang mit Art. 28 Abs. 4 DSGVO erfüllt hat (z.B. durch Nachweise/Zertifikate). Der Auftragsverarbeiter bleibt dem Verantwortlichen gegenüber **voll verantwortlich** für die ordnungsgemäße Datenverarbeitung auch durch die eingesetzten Subunternehmer (Art. 28 Abs. 4 S. 2 DSGVO).

5.3 **Liste der Subunternehmer:** Derzeit setzt der Auftragsverarbeiter die in **Anlage 2** genannten Subunternehmer ein. Eine Verarbeitung durch andere als die in Anlage 2 aufgeführten Subunternehmer ist dem Auftragsverarbeiter – vorbehaltlich der vertraglichen Zustimmung nach Ziff. 5.1 – nicht gestattet. Der Auftragsverarbeiter wird die Anlage 2 bei Änderungen aktualisieren und dem Verantwortlichen zur Verfügung stellen.

6. Ort der Datenverarbeitung und Drittlandübermittlungen

6.1 **Verarbeitungsstandorte:** Die Datenverarbeitung findet grundsätzlich in **Mitgliedstaaten der Europäischen Union (EU)** oder des Europäischen Wirtschaftsraums (EWR) statt. Der Auftragsverarbeiter oder dessen Subunternehmer verarbeiten die Daten nach Möglichkeit innerhalb von EU/EWR-Rechenzentren. So werden die Dienste der Lumitra GmbH derzeit in einem **Microsoft Azure** Rechenzentrum in **Irland** (EU) betrieben, und der Telekommunikationsdienst zur Gesprächsvermittlung (sipgate) befindet sich in **Deutschland**. Eine Verlagerung von Verarbeitungstätigkeiten in ein **Drittland** (außerhalb EU/EWR) erfolgt nur, soweit die besonderen Voraussetzungen der **Art. 44 ff. DSGVO** erfüllt sind (z.B. Vorliegen eines Angemessenheitsbeschlusses der EU-Kommission oder Abschluss von **Standarddatenschutzklauseln**).

6.2 **Drittstaatentransfer in die USA (OpenAI):** Der Verantwortliche nimmt zur Kenntnis, dass der Auftragsverarbeiter zur Erfüllung der vertraglichen Leistung einen Subunternehmer in einem Drittstaat einsetzt, nämlich **OpenAI, Inc. (USA)**, für die KI-gestützte Verarbeitung der Gesprächsdaten. Hierdurch findet eine **Übermittlung personenbezogener Daten in die USA** statt, ein Land, für das kein Angemessenheitsbeschluss der EU gemäß Art. 45 DSGVO besteht. Der Auftragsverarbeiter hat daher **geeignete Garantien** gemäß Art. 46 DSGVO getroffen, um beim Einsatz von OpenAI ein den EU-Standards vergleichbares Datenschutzniveau sicherzustellen. Insbesondere wurden mit OpenAI die **EU-Standardvertragsklauseln** (SCC) abgeschlossen und vertragliche Zusicherungen eingeholt, dass OpenAI die übermittelten Daten ausschließlich im Rahmen des Auftrags verarbeitet und **nicht** für eigene Zwecke (insbesondere nicht zum Training von KI-Modellen) nutzt. Zudem nutzt der Auftragsverarbeiter die OpenAI-Dienste im **Enterprise/API-Modus**, bei dem eine Speicherung der eingegebenen Daten zu Trainingszwecken durch OpenAI deaktiviert ist. Die Übermittlung an OpenAI erfolgt **verschlüsselt** über gesicherte Verbindungen (TLS). Der Auftragsverarbeiter hat eine **Risikoabschätzung** im Sinne des Schrems-II-Urteils durchgeführt und – gemäß den Empfehlungen des Europäischen Datenschutzausschusses und der deutschen Datenschutzkonferenz – zusätzliche technische Schutzmaßnahmen implementiert (siehe **Anlage 3**, z.B. Verschlüsselung und Datenminimierung), um die Daten vor unbefugtem Zugriff zu schützen. Sofern OpenAI oder andere US-Behörden dem Auftragsverarbeiter gegenüber

Anfragen zum Zugriff auf die Daten des Verantwortlichen stellen, wird der Auftragsverarbeiter den Verantwortlichen hierüber nach Maßgabe von Ziff. 8.3 umgehend informieren.

6.3 **Weitere Drittstaatentransfers:** Abgesehen von OpenAI findet derzeit keine Übermittlung personenbezogener Daten in Drittstaaten außerhalb des EU/EWR-Raums statt. Sollte der Auftragsverarbeiter beabsichtigen, weitere Verarbeitungen in einem Drittland durchzuführen oder neue Subunternehmer in Drittstaaten einzusetzen, wird er zuvor das Einverständnis des Verantwortlichen einholen (vgl. Ziff. 5.1) und sicherstellen, dass **jede** Datenübermittlung in ein Drittland nur unter **Einhaltung der Voraussetzungen der Art. 44 ff. DSGVO** erfolgt. Hierzu zählen insbesondere der Abschluss der jeweils gültigen **Standardvertragsklauseln** der EU-Kommission sowie – falls erforderlich – ergänzende Maßnahmen zum Schutz der Daten.

7. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Der Auftragsverarbeiter verpflichtet sich, **angemessene technische und organisatorische Maßnahmen** zum Schutz der personenbezogenen Daten zu implementieren und aufrechtzuerhalten. Die konkreten zum Einsatz kommenden Maßnahmen sind in **Anlage 3** beschrieben und von den Vertragsparteien als angemessen vereinbart. Der Auftragsverarbeiter stellt sicher, dass die in Anlage 3 aufgeführten Sicherheitsmaßnahmen vor Beginn der Verarbeitung umgesetzt wurden und während der gesamten Dauer der Verarbeitung eingehalten werden. Er überprüft die Wirksamkeit dieser Maßnahmen regelmäßig und nimmt erforderlichenfalls Anpassungen vor, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1 lit. d DSGVO). Wesentliche Änderungen sind vom Auftragsverarbeiter zu dokumentieren und dem Verantwortlichen auf Anfrage mitzuteilen.

Sollten die vom Verantwortlichen vorgegebenen oder vereinbarten Maßnahmen im Laufe der Zeit den **Stand der Technik** nicht mehr entsprechen oder sich als unzureichend erweisen, wird der Auftragsverarbeiter den Verantwortlichen hierüber informieren und Vorschläge für notwendige Änderungen unterbreiten. Maßnahmen, die nur mit Zustimmung des Verantwortlichen effektiv umgesetzt werden können (z.B. Pseudonymisierung von Daten durch den Verantwortlichen selbst), wird der Verantwortliche nach besten Kräften unterstützen.

8. Unterstützungspflichten des Auftragsverarbeiters

8.1 **Unterstützung bei Betroffenenrechten:** Der Auftragsverarbeiter wird den Verantwortlichen – unter Berücksichtigung von Art und Umfang der Verarbeitung – nach besten Möglichkeiten dabei unterstützen, die **Rechte betroffener Personen** nach Kapitel III DSGVO (Art. 12–22 DSGVO) zu gewährleisten. Insbesondere wird er dem Verantwortlichen alle erforderlichen Auskünfte und Informationen bereitstellen, damit dieser seinen Auskunfts- oder Informationspflichten nachkommen kann. Der Auftragsverarbeiter ermöglicht dem Verantwortlichen die Berichtigung, Einschränkung oder Löschung von Daten direkt vorzunehmen oder führt solche Maßnahmen auf Weisung des Verantwortlichen unverzüglich selbst durch. Sofern sich ein Betroffener unmittelbar an den Auftragsverarbeiter wendet (etwa mit einem Auskunfts- oder Löschungsverlangen), wird der Auftragsverarbeiter dieses Anliegen **ohne schuldhaftes Zögern an den Verantwortlichen weiterleiten**. Eine eigenständige Bearbeitung entsprechender Anfragen durch den Auftragsverarbeiter erfolgt nur auf Weisung des Verantwortlichen. Ohne Weisung erteilt der Auftragsverarbeiter **keinerlei Auskünfte** über Daten aus der Auftragsverarbeitung weder an die betroffene Person selbst noch an Dritte.

8.2 **Unterstützung bei der Sicherheit der Verarbeitung und Folgenabschätzungen:** Der Auftragsverarbeiter wird den Verantwortlichen bei der Einhaltung der in Art. 32 bis 36 DSGVO

genannten Pflichten unterstützen, soweit dies möglich und erforderlich ist (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Dazu zählen:

- **Meldung von Datenschutzverletzungen:** Unterstützung bei der Abwicklung und Dokumentation von Meldungen an Aufsichtsbehörden und ggf. an betroffene Personen gemäß Art. 33, 34 DSGVO, indem der Auftragsverarbeiter dem Verantwortlichen unverzüglich alle relevanten Informationen über den Vorfall zukommen lässt (siehe Ziff. 9).
- **Datenschutz-Folgenabschätzung (DSFA):** Sofern der Verantwortliche eine DSFA nach Art. 35 DSGVO durchführt, wird der Auftragsverarbeiter die hierfür benötigten Informationen über die vom ihm durchgeführten Verarbeitungen bereitstellen und auf Anfrage an der DSFA mitwirken (z.B. durch technische Einschätzungen).
- **Vorherige Konsultation:** Im Falle einer notwendigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO unterstützt der Auftragsverarbeiter den Verantwortlichen mit Informationen über die Auftragsverarbeitung.

8.3 **Unterstützung bei behördlichen Anfragen und Verfahren:** Der Auftragsverarbeiter teilt dem Verantwortlichen unverzüglich mit, wenn **Aufsichtsbehörden** im Rahmen ihrer Zuständigkeit beim Auftragsverarbeiter handeln (z.B. Anfragen, Prüfungen), soweit sie die Auftragsverarbeitung betreffen. Er wird den Verantwortlichen – im Rahmen seiner Möglichkeiten – bei allen behördlichen Verfahren, die die im Auftrag verarbeiteten Daten betreffen, unterstützen. Gleiches gilt, wenn der Auftragsverarbeiter von anderen staatlichen Stellen oder Dritten eine Anfrage oder Anordnung zur Herausgabe von beim Auftragsverarbeiter gespeicherten personenbezogenen Daten des Verantwortlichen erhält. Der Auftragsverarbeiter wird, soweit rechtlich zulässig, den Verantwortlichen unverzüglich darüber informieren und weitere Schritte abstimmen.

9. Meldung von Verletzungen des Schutzes personenbezogener Daten

Stellt der Auftragsverarbeiter **Verletzungen des Schutzes personenbezogener Daten** im Sinne des Art. 4 Nr. 12 DSGVO (z.B. Sicherheitsvorfälle, Datenpannen) in Bezug auf die vom Verantwortlichen überlassenen Daten fest, so hat er den Verantwortlichen **unverzüglich**, spätestens innerhalb von 24 Stunden nach Bekanntwerden, darüber zu informieren. Die Meldung an den Verantwortlichen hat alle nach Art. 33 Abs. 3 DSGVO relevanten Informationen zu enthalten, insbesondere:

- eine **Beschreibung der Art der Datenschutzverletzung**, einschließlich (soweit möglich) der Kategorien und ungefähren Anzahl der betroffenen Personen sowie der betroffenen Datensätze;
- eine **Beschreibung der vom Auftragsverarbeiter bereits ergriffenen oder vorgeschlagenen Maßnahmen** zur Behebung der Datenschutzverletzung und ggf. zur Minderung ihrer möglichen nachteiligen Auswirkungen;
- eine **Beschreibung der wahrscheinlichen Folgen** der Verletzung für die betroffenen Personen (soweit möglich und einschätzbar);
- die Nennung eines Ansprechpartners beim Auftragsverarbeiter für Rückfragen.

Der Auftragsverarbeiter wird zudem alle ihm zur Verfügung stehenden Maßnahmen ergreifen, um die Verletzung einzudämmen und – in Abstimmung mit dem Verantwortlichen – möglichst schnell zu beheben sowie Folgeschäden zu minimieren. **Folgemeldungen** mit neuen

Erkenntnissen erfolgen ebenfalls in Abstimmung mit dem Verantwortlichen. Der Auftragsverarbeiter unterstützt den Verantwortlichen ferner bei der Erfüllung etwaiger Melde- und Benachrichtigungspflichten nach Art. 33, 34 DSGVO (siehe Ziff. 8.2).

Keine Meldungspflicht besteht, wenn sich der Vorfall nachweislich **nicht auf vom Verantwortlichen bereitgestellte oder im Auftrag verarbeitete personenbezogene Daten** bezieht oder wenn ein Meldekriterium nach Art. 33 DSGVO objektiv nicht gegeben ist. Gleichwohl informiert der Auftragsverarbeiter den Verantwortlichen auch über sicherheitsrelevante Vorfälle, die **keine** meldepflichtigen Datenschutzverletzungen darstellen, wenn ein Bezug zum Auftragsverhältnis besteht, damit der Verantwortliche ein eigenes Bild der Sachlage gewinnen kann.

10. Beendigung der Auftragsverarbeitung, Rückgabe und Löschung von Daten

Nach Beendigung der vertraglichen Leistungen und auf Wunsch des Verantwortlichen auch **jederzeit zuvor** wird der Auftragsverarbeiter sämtliche personenbezogenen Daten, die er im Auftrag verarbeitet hat – einschließlich etwaiger Kopien – **entweder** an den Verantwortlichen (bzw. an einen vom Verantwortlichen benannten neuen Dienstleister) **herausgeben oder** nach Weisung des Verantwortlichen **datenschutzgerecht löschen**. Dies umfasst auch die Löschung in allen Backups und bei Subunternehmern. Sofern der Verantwortliche keine konkrete Weisung erteilt, wird der Auftragsverarbeiter die personenbezogenen Daten nach Ende des Auftrags unverzüglich löschen. Eine Herausgabe oder Rückübermittlung der Daten erfolgt in einem gängigen strukturierten Format, sofern nichts anderes vereinbart ist. Über die erfolgte Löschung beim Auftragsverarbeiter und den Subunternehmern hat der Auftragsverarbeiter dem Verantwortlichen **auf Verlangen eine Bestätigung** in Textform zukommen zu lassen.

Vom Löschen ausgenommen sind Daten, deren weitere Aufbewahrung für den Auftragsverarbeiter **pflichtig** ist (z.B. zur Erfüllung gesetzlicher Aufbewahrungsvorschriften nach Handels- oder Steuerrecht) oder die für die Bereitstellung von abrechnungsrelevanten Unterlagen erforderlich sind. Diese Daten darf der Auftragsverarbeiter maximal so lange speichern, wie es die jeweiligen Aufbewahrungsfristen vorsehen. Für diese Zeit ist die Verarbeitung der betreffenden Daten auf die zulässigen Zwecke der Archivierung beschränkt; anschließend sind auch diese Daten unverzüglich zu löschen. Ebenfalls darf der Auftragsverarbeiter Daten aus dem Auftrag zurückbehalten, wenn und solange er ein **zurückbehaltungsrechtliches Interesse** geltend machen kann (etwa bis zur vollständigen Begleichung offener Vergütungsansprüche); in diesem Fall dürfen die Daten nur für die Dauer und Zwecke der Durchsetzung des Rechts zurückbehalten und danach gelöscht werden.

Der Auftragsverarbeiter hat nach Vertragsende auf Anforderung des Verantwortlichen die im Zusammenhang mit der Auftragsverarbeitung ggf. genutzten **Träger medien** (z.B. mobile Datenträger) herauszugeben oder – nach Wahl des Verantwortlichen – zu vernichten. Die Vernichtung ist dem Verantwortlichen auf Wunsch nachzuweisen.

Die Dokumentationen über die Auftragsverarbeitung (Protokolle, Berichte, Nachweisdokumente), die dem Auftragsverarbeiter zur Einhaltung der Auftrags- und gesetzlicher Pflichten dienen, sind vom Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungspflichten über das Vertragsende hinaus aufzubewahren. Der Auftragsverarbeiter darf sie danach erst nach Freigabe durch den Verantwortlichen löschen.

11. Kontrollrechte des Verantwortlichen (Audit)

Der Verantwortliche hat das Recht, die Einhaltung der datenschutzrechtlichen Vorschriften und der vertraglichen Vereinbarungen beim Auftragsverarbeiter im erforderlichen Umfang zu **kontrollieren**. Der Auftragsverarbeiter sagt zu, dem Verantwortlichen auf Anfrage **alle Auskünfte** zu erteilen, die zur Durchführung einer solchen Kontrolle erforderlich sind, und erforderliche Nachweise bereitzustellen. Der Verantwortliche kann insbesondere **Prüfungen** durchführen oder durch einen im Einzelfall zu benennenden **externen Prüfer** (z.B. Wirtschaftsprüfer, Datenschutzauditor) durchführen lassen. Das Prüfungsrecht erstreckt sich auch auf Subunternehmer, soweit diese im Rahmen der Auftragsverarbeitung tätig werden; der Auftragsverarbeiter wird entsprechende Zugangs- und Prüfungsrechte bei den Subunternehmern vertraglich sicherstellen.

Kontrollen beim Auftragsverarbeiter sollen – soweit kein konkreter Anlass vorliegt – mit angemessener **Voranmeldung** (mindestens 2 Wochen vorher) und während der üblichen Geschäftszeiten erfolgen, und sie dürfen den Betriebsablauf des Auftragsverarbeiters nicht unverhältnismäßig stören. Der Auftragsverarbeiter ist berechtigt, diese Kontrollen aus **Geheimhaltungs- und Sicherheitsgründen** von der Unterzeichnung einer branchenüblichen Vertraulichkeitserklärung abhängig zu machen. Sollte eine Aufsichtsbehörde des Verantwortlichen eine Prüfung bei dem Auftragsverarbeiter durchführen (oder eine solche anordnen), gilt dies ebenfalls als Kontrolle, die der Auftragsverarbeiter ermöglicht.

Anstatt einer Vor-Ort-Inspektion kann der Auftragsverarbeiter dem Verantwortlichen **Nachweise** über die Einhaltung der Pflichten aus diesem Vertrag auch durch aktuelle **Zertifikate, Prüfungsberichte oder Berichte einer unabhängigen Instanz** (z.B. externer Datenschutzbeauftragter, IT-Revision, externer Auditor) oder durch geeignete **Eigen-Audits** zur Verfügung stellen. Diese Nachweise müssen dem Verantwortlichen eine angemessene Überzeugungsbildung von der Einhaltung der vertraglichen Pflichten ermöglichen. Die Entscheidung, ob ein eigener Audit durchgeführt wird oder die vorgelegten Nachweise ausreichen, trifft der Verantwortliche nach pflichtgemäßem Ermessen.

Eventuelle Kosten einer vom Verantwortlichen initiierten Vor-Ort-Kontrolle (bei dem Auftragsverarbeiter oder Subunternehmer) trägt der Verantwortliche, sofern die Kontrolle nicht aufgrund eines konkreten Verdachts einer Pflichtverletzung durch den Auftragsverarbeiter erforderlich wurde. Die Aufwendungen des Auftragsverarbeiters für die Mitwirkung an Kontrollen sind vom Verantwortlichen in dem Umfang zu tragen, wie dies im Hauptvertrag ggf. vereinbart ist.

12. Schlussbestimmungen

12.1 Schriftform und Änderungen: Für alle in diesem Vertrag genannten Mitteilungen zwischen den Parteien (z.B. Weisungen, Anzeigen, Genehmigungen) ist zumindest die Textform (z.B. E-Mail) erforderlich; sofern eine strengere Form (Schriftform) gesetzlich vorgeschrieben ist, bleibt diese unberührt. Änderungen und Ergänzungen dieses Auftragsverarbeitungsvertrags einschließlich dieser Klausel bedürfen der **Schriftform** (im Sinne von Art. 28 Abs. 9 DSGVO kann dies auch in einem elektronischen Format erfolgen). Einseitige Änderungen – mit Ausnahme der Aktualisierung der Anlagen im vereinbarten Rahmen – sind ausgeschlossen. Im Falle von Widersprüchen zwischen diesem AVV und anderen Vereinbarungen zwischen den Parteien (insbesondere dem Hauptvertrag) gehen die Bestimmungen dieses AVV den übrigen Vereinbarungen vor, **insbesondere** hat im Zweifel die Regelung den Vorrang, welche die **datenschutzrechtlich strengeren Pflichten** enthält.

12.2 Rechtswahl: Es gilt – vorbehaltlich etwaiger zwingender Vorschriften des internationalen Datenschutzrechts – das Recht der Bundesrepublik Deutschland. Bei internationalen Sachverhalten werden die **Standardvertragsklauseln** gemäß Durchführungsbeschluss

(EU) 2021/914 der EU-Kommission vom 4. Juni 2021 und ggf. Zusatzvereinbarungen (TCF, o. ä.) in diesen Vertrag einbezogen, soweit dies zur rechtmäßigen Drittlandübermittlung erforderlich ist. Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist, soweit rechtlich zulässig, [Sitz des Verantwortlichen]/[Sitz des Auftragsverarbeiters].

12.3 Salvatorische Klausel: Sollten einzelne Bestimmungen dieses Vertrags unwirksam oder nicht durchsetzbar sein oder werden, so bleibt die Gültigkeit der übrigen Bestimmungen hiervon unberührt. Die Parteien werden in einem solchen Fall die unwirksame Bestimmung durch eine Regelung ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung und den Anforderungen der DSGVO so weit wie möglich gerecht wird. Entsprechendes gilt für etwaige Vertragslücken.

12.4 Vorrang der DSGVO und ergänzende Vereinbarungen: Soweit in diesem Vertrag oder in Weisungen des Verantwortlichen nicht ausdrücklich etwas anderes geregelt ist, gelten die gesetzlichen Vorschriften der DSGVO und des BDSG. Dieser Vertrag entfaltet Wirkung ab dem Datum seiner Unterzeichnung durch beide Parteien. Er stellt zusammen mit dem Hauptvertrag die **vollständige Vereinbarung** der Parteien über die Auftragsverarbeitung dar. Etwaige frühere Vereinbarungen zum gleichen Gegenstand (insbesondere ältere Auftragsverarbeitungsverträge) treten mit Wirksamwerden dieses Vertrags außer Kraft.

Anlage 1 – Beschreibung der Verarbeitung (Datenarten und betroffene Personen)

Zweck der Verarbeitung: Durchführung des Mitschriften-Dienstes der Lumitra GmbH – insbesondere Aufzeichnung von Telefongesprächen, automatische Spracherkennung und Transkription der Gespräche sowie KI-gestützte Zusammenfassung der Inhalte – zum Zweck der Dokumentation, Protokollierung und Auswertung von Telefonaten des Verantwortlichen. Die Verarbeitung dient der Unterstützung des Verantwortlichen bei der nachvollziehbaren **Dokumentation von Gesprächsinhalten** (z. B. zur Qualitätssicherung, Kundenbetreuung, Beweissicherung oder Protokollerstellung geschäftlicher Telefonate).

Art der Verarbeitung: Erhebung von Audio-Daten (Mitschnitt von Telefongesprächen über eine VoIP/Telekommunikationsschnittstelle), automatisierte Auswertung dieser Audio-Daten durch Spracherkennungs- und KI-Systeme, Speicherung der daraus generierten **Transkriptionen** (Text) und **Zusammenfassungen** auf Cloud-Servern des Auftragsverarbeiters sowie Bereitstellung dieser Ergebnisse für den Verantwortlichen (z.B. über eine Web-Oberfläche oder API). Gegebenenfalls erfolgen hierbei Zwischenschritte wie die Konvertierung von Audioformaten, Zwischenspeicherung in Arbeitsspeichern, und Versenden der Daten an einen KI-Dienst (OpenAI) zur Verarbeitung. Es findet auch eine **Speicherung** der Ergebnisse und eventuell der Originalaufzeichnungen für begrenzte Zeiträume statt, um dem Verantwortlichen Zugriff und Nachnutzung (z.B. Download der Transkripte) zu ermöglichen. Nach Ablauf definierter Aufbewahrungsfristen oder auf Weisung des Verantwortlichen werden die Daten gelöscht (siehe Hauptvertrag bzw. Löschkonzept).

Kategorien personenbezogener Daten:

- **Audio-Daten des Gesprächs:** Sprachaufzeichnungen der beteiligten Personen (die Telefongesprächsmitschnitte enthalten Stimmen und gesprochenen Inhalt). Daraus resultierend **Textdaten** (Transkription des gesprochenen Wortlauts) sowie **analysierte Inhalte** (automatisch erstellte Zusammenfassungen, Gesprächsnotizen, Schlagworte). Diese Daten können **personenbezogene Informationen** beinhalten, die von den

Gesprächsteilnehmern genannt werden – z.B. Namen, Kontaktdaten (Adresse, Telefonnummer, E-Mail), Kundennummern, geschäftliche Vorgänge, vereinbarte Termine, Vertrags- oder Bestelldetails, u. U. auch sensible Informationen je nach Gesprächsthema.

- **Metadaten des Telefonats:** Zeitpunkt und Dauer des Anrufs, Rufnummer des Anrufers und Angerufenen (falls nicht anonymisiert), ggf. interne Kennungen (Ticketnummer, Meeting-ID oder Call-ID), Teilnehmerkennung (z.B. Mitarbeiter-ID) und technisch notwendige Verbindungsdaten.
- **Vom Verantwortlichen bereitgestellte Zusatzdaten:** Etwaige zugeordnete Stammdaten zu Gesprächspartnern (z.B. Kundennamen aus CRM, sofern in der Anwendung verknüpft), oder Gesprächsnotizen, die vor/nach dem Gespräch manuell ergänzt werden.

Besondere Kategorien personenbezogener Daten: Im Regelfall werden keine besonderen Kategorien nach Art. 9 Abs. 1 DSGVO systematisch erhoben. Es kann jedoch nicht ausgeschlossen werden, dass im Rahmen von Telefongesprächen **sensible Informationen** (etwa Gesundheitsdaten, politische Meinungen, Religionszugehörigkeit, o. ä.) zur Sprache kommen und somit in den Aufzeichnungen/Transkripten enthalten sind. Eine solche Verarbeitung ist nicht zielgerichtet und erfolgt lediglich inzidentell im Rahmen des Gesprächsverlaufs. Der Verantwortliche hat – soweit möglich – dafür zu sorgen, dass keine unnötigen besonderen Kategorien personenbezogener Daten im Gespräch offengelegt werden. Sofern doch, findet Art. 9 Abs. 2 DSGVO (z.B. Einwilligung oder Offensichtlichmachen durch die betroffene Person) entsprechende Anwendung als Rechtsgrundlage im Verantwortungsbereich des Verantwortlichen.

Kategorien betroffener Personen:

- **Gesprächsteilnehmer des Verantwortlichen:** Mitarbeiter des Verantwortlichen, die an den aufgezeichneten Telefonaten teilnehmen (z.B. Kundendienst-Mitarbeiter, Vertriebspersonal, Sachbearbeiter).
- **Externe Gesprächspartner:** Jede Person, die mit dem Verantwortlichen telefoniert und deren Gespräch vom Dienst erfasst wird – z.B. **Kunden, Interessenten, Lieferanten, Geschäftspartner** oder sonstige Dritte, die an den Telefonaten beteiligt sind. Dies kann sowohl Verbraucher (natürliche Personen) als auch Vertreter juristischer Personen betreffen, soweit deren Äußerungen personalbeziehbar sind.
- **Sonstige Betroffene:** Personen, über die in den Telefonaten gesprochen wird, sofern deren personenbezogene Daten Gegenstand der Unterhaltung sind. Beispielsweise könnte im Gespräch auf Dritte Bezug genommen werden (z.B. namentliche Erwähnung von Ansprechpartnern, Kollegen, Patienten, etc.), wodurch auch deren Daten indirekt Teil der Verarbeitung werden.

(Der Verantwortliche hat sicherzustellen, dass alle betroffenen externen Gesprächspartner – soweit erforderlich – über die Aufzeichnung und Verarbeitung informiert wurden und ggf. eingewilligt haben.)

Anlage 2 – Subunternehmerliste

Die folgenden Unterauftragsverarbeiter (Subunternehmer) werden vom Auftragsverarbeiter zum Zweck der Erfüllung der vertraglich vereinbarten Dienstleistung eingesetzt. Der Verantwortliche

stimmt der Beauftragung dieser Subunternehmer zu. Der Auftragsverarbeiter hat mit jedem Subunternehmer einen DSGVO-konformen Auftragsverarbeitungsvertrag geschlossen und gewährleistet durch geeignete vertragliche Vereinbarungen, dass die gleichen Datenschutzpflichten, wie sie in diesem AVV festgelegt sind, auch von den Subunternehmern eingehalten werden.

Subunternehmer	**Anschrift / Sitz**	**Tätigkeit (ausgelagerte Verarbeitung)**	**Datenübermittlung in Drittland?**
OpenAI, Inc.(OpenAI API Dienst)	San Francisco, California, USA	KI-gestützte Sprachverarbeitung (Automatische Transkription der Audiodaten und Generierung von Zusammenfassungen mittels Machine Learning)	**Ja** – Übermittlung in die **USA** (kein Angemessenheitsbeschluss; Garantien: EU-Standardvertragsklauseln abgeschlossen, zusätzliche Sicherheitsmaßnahmen umgesetzt)
Microsoft Ireland Operations Ltd.(Azure Cloud Services)	One Microsoft Place, Dublin, Irland (EU)	Cloud-Infrastruktur (Hosting der Anwendung und Speicherung der aufgezeichneten Audiofiles, Transkriptionen und Zusammenfassungen in europäischen Rechenzentren)	**Nein** – Verarbeitung innerhalb der **EU** (Irland); keine Drittlandübertragung erforderlich.
sipgate GmbH(Telefondienstleister)	Gladbacher Str. 74, 40219 Düsseldorf, Deutschland	Telekommunikations-Plattform (Zurverfügungstellung von VoIP-Telefonie-Anschlüssen, Verbindungsaufbau der Telefonate und ggf. Aufzeichnung der Gespräche im Rahmen des Dienstes)	**Nein** – Verarbeitung in **Deutschland** (EU); keine Übermittlung in Drittstaaten.

Hinweise:

1. **OpenAI, Inc.:** Bei diesem Subunternehmer handelt es sich um einen Anbieter in einem Drittland (USA). Die Übermittlung erfolgt nur, soweit zur KI-Verarbeitung erforderlich, und unter den in Abschnitt 6 des AV-Vertrags genannten Bedingungen (Standardvertragsklauseln, technische Schutzmaßnahmen etc.). OpenAI verarbeitet die erhaltenen Daten ausschließlich für die vom Auftragsverarbeiter vorgegebene Verarbeitung und nicht für eigene Zwecke (Training ist deaktiviert).

2. **Microsoft Azure (Ireland):** Microsoft wird als Unterauftragsverarbeiter für Hosting und Speicherung genutzt. Die Serverstandorte sind gemäß Vertrag auf die EU beschränkt (Region **Westeuropa - Ireland**). Microsoft verarbeitet Daten nur nach Weisung des Auftragsverarbeiters und nicht zu eigenen Zwecken.

3. **sipgate GmbH:** Sipgate fungiert als Telekommunikations-Dienstleister (Anbieter von Telefonnummern/VoIP) und ermöglicht die technische Durchleitung und ggf. Aufzeichnung der Anrufe. Sipgate ist ein Anbieter mit Sitz in Deutschland und unterliegt damit vollständig der DSGVO sowie dem deutschen Telekommunikationsgesetz (TKG). Ein separater Auftragsverarbeitungsvertrag zwischen Lumitra und sipgate ist abgeschlossen.

Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage weitere Informationen über die einzelnen Subunternehmer und deren Datenschutzgarantien zur Verfügung (z.B. Auszüge aus den Verträgen oder Zertifizierungen). Änderungen in dieser Subunternehmerliste erfolgen gemäß Abschnitt 5 des AV-Vertrags.

Anlage 3 – Technische und organisatorische Maßnahmen (TOM)

Nachfolgend sind die wesentlichen technischen und organisatorischen Maßnahmen aufgeführt, die der Auftragsverarbeiter gem. Art. 32 DSGVO zum Schutz der im Auftrag verarbeiteten personenbezogenen Daten implementiert hat. Diese Maßnahmen gewährleisten ein dem Risiko angemessenes Schutzniveau, bezogen auf Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme. Der Auftragsverarbeiter passt die Maßnahmen bei Bedarf an den aktuellen Stand der Technik an.

- **Zugangs- und Zutrittskontrolle (physisch):** Rechenzentrumsstandorte verfügen über umfangreiche physische Sicherheitsmaßnahmen. Die Cloud-Infrastruktur (Microsoft Azure, Irland) ist ISO 27001-zertifiziert und schützt vor unbefugtem Zutritt durch mehrstufige Sicherheitskonzepte: Zugangsberechtigungen werden strikt geprüft, es gibt 24/7-Überwachung, Videoüberwachung, Alarmanlagen und Personenkontrollen. Unbefugten ist der Zugang zu Serverräumen verwehrt. Die Büroräume der Lumitra GmbH sind ebenfalls gesichert (Zutrittskontrolle durch Schließsystem, Alarmanlage außerhalb der Geschäftszeiten, Zugang nur für autorisierte Mitarbeiter).

- **Zugangskontrolle (digital zu Systemen):** Zugriff auf IT-Systeme und Anwendungen, in denen personenbezogene Daten verarbeitet werden, ist nur nach erfolgreicher Authentifizierung möglich. Lumitra setzt ein **rollenbasiertes Benutzerkontosystem** ein: Mitarbeiter erhalten individuell zugewiesene Nutzerkonten mit starken Passwörtern; wo möglich wird **Mehr-Faktor-Authentifizierung (MFA)** eingesetzt. Es bestehen Richtlinien zur Passwortstärke und regelmäßigen Passwortänderung. Benutzerkonten werden gesperrt oder gelöscht, sobald der jeweilige Mitarbeiter keinen Zugriff mehr benötigt (z.B. bei Abteilungswechsel oder Ausscheiden). Automatische **Sperrmechanismen** greifen bei Inaktivität oder mehrfachen Fehlanmeldungen. Administratorenrechte werden nur sehr wenigen, besonders vertrauenswürdigen Personen erteilt und deren Verwendung wird protokolliert.

- **Zugriffskontrolle (innerhalb der Systeme auf Daten):** Das **Prinzip der Minimalberechtigung** wird konsequent umgesetzt. Jeder Mitarbeiter des Auftragsverarbeiters hat nur auf die Daten Zugriff, die er zur Erfüllung seiner Aufgabe benötigt. Unterschiedliche Berechtigungsstufen und Rollen (z.B. Administrator, Entwickler, Support) stellen sicher, dass kein unberechtigter Datenzugriff erfolgt.

Besonders schützenswerte Bereiche (z.B. Datenbanken mit Gesprächsaufzeichnungen) sind zusätzlich durch separate Rechte beschränkt. Zugriffe der Administratoren und System-Operatoren werden protokolliert (**Logging** von Zugriffen und Änderungen), sodass missbräuchliche Aktivitäten erkannt werden können. Mitarbeiter des technischen Supports greifen – sofern erforderlich – nur nach vorheriger Freigabe und zu Supportzwecken auf Kundendaten zu und diese Zugriffe werden dokumentiert. Alle Mitarbeiter sind auf das Datengeheimnis und die Wahrung der Vertraulichkeit verpflichtet (vgl. Abschnitt 3, Vertraulichkeit).

- **Weitergabekontrolle (Übertragungsschutz):** Personenbezogene Daten werden bei der Übertragung über öffentliche Netze **verschlüsselt**. Der Zugriff auf die Weboberfläche/API des Lumitra-Dienstes erfolgt ausschließlich über **HTTPS** (TLS 1.2 oder höher), sodass die Kommunikation zwischen dem Verantwortlichen und dem Dienst vor Abhören/Manipulation geschützt ist. Die interne Kommunikation zwischen Diensten sowie die Übertragung von Audiodaten zur OpenAI-API erfolgt ebenfalls über verschlüsselte Verbindungen (TLS). Unverschlüsselte Protokolle werden nicht verwendet. E-Mails, die personenbezogene Daten enthalten (z.B. automatisch generierte Benachrichtigungen), werden nach Möglichkeit ebenfalls transportverschlüsselt versandt (TLS zwischen Mailservern). Exporte oder Downloads von Gesprächsaufzeichnungen oder Transkripten durch den Verantwortlichen erfolgen über die gesicherte Weboberfläche; alternativ wird bei Übermittlungen auf individuelle Anfrage hin z.B. ein verschlüsselter Download-Link bereitgestellt. Datenträger, die für Transport oder Backup genutzt werden (z.B. portables Backup-Medium), werden verschlüsselt oder pseudonymisiert, sodass ein Zugriff durch Unbefugte ausgeschlossen ist.

- **Eingabekontrolle (Protokollierung):** Die Systeme protokollieren die relevanten Verarbeitungsschritte und Eingaben, soweit möglich und verhältnismäßig. Insbesondere administrative Eingriffe (z.B. Änderungen an Systemeinstellungen, Anlegen oder Löschen von Benutzerkonten, Abruf von Gesprächsdaten durch Administratoren) werden mit Zeitstempel, verantwortlichem Benutzer und Art der Aktion aufgezeichnet. Zugriffsprotokolle auf die Audio- und Textdaten werden gespeichert und regelmäßig ausgewertet, um unautorisierte Zugriffe erkennen zu können. Die Protokolldaten sind gegen Manipulation geschützt und werden vertraulich behandelt. Der Verantwortliche kann auf Anfrage Protokollauszüge erhalten, soweit dies erforderlich ist, um die Korrektheit der Verarbeitung nachzuvollziehen.

- **Pseudonymisierung und Datenminimierung:** Soweit es der Verarbeitungszweck zulässt, bemüht sich Lumitra um **Datenminimierung**. Beispielsweise können im System anstatt Klarnamen von Gesprächspartnern interne IDs oder Pseudonyme verwendet werden, sofern der Verantwortliche dies unterstützt (z.B. Kundennummer anstelle Name). Die KI-gestützte Verarbeitung erfolgt zwar auf Real-Daten, jedoch werden die Eingabedaten bei OpenAI nicht dauerhaft gespeichert (Trainingsnutzung deaktiviert, Löschung dort laut OpenAI-Richtlinien binnen ca. 30 Tagen). Sensible Inhalte der Gespräche werden vom Verantwortlichen nach Möglichkeit vorab anonymisiert oder nachträglich aus den Transkripten entfernt, falls sie für den Zweck nicht erforderlich sind. Bei Support-Anfragen, in denen Lumitra-Mitarbeiter Gesprächsdaten einsehen müssen, kann der Verantwortliche auf Wunsch vorab bestimmte sensible Passagen anonymisieren. Wo machbar, werden Teile der Verarbeitung im **Speicher** durchgeführt,

ohne langfristige Speicherung (z.B. Kurzzeit-Zwischenspeicher der Audio-Streams, die nach Transkription sofort verworfen werden).

- **Verschlüsselung (Datenspeicherung):** Alle dauerhaften Speichermedien, auf denen personenbezogene Gesprächsdaten liegen, sind verschlüsselt. Dies umfasst die Datenbanken für Transkripte und Zusammenfassungen (Server-seitige **AES-256 Verschlüsselung** auf Volume-Ebene) sowie ggf. in der Cloud gespeicherte Audiodateien (Storage-Verschlüsselung bei Azure). Schlüssel werden sicher verwaltet und nur autorisierten Systemprozessen zugänglich gemacht. Darüber hinaus sind die Datenbankinhalte durch Zugriffskontrollen geschützt (siehe Zugriffskontrolle oben). Backups werden ebenfalls verschlüsselt gespeichert. So ist sichergestellt, dass bei einem physischen Zugriff auf die Speichermedien (z.B. im Falle eines Festplattenklaus) kein Klartextzugriff auf die Daten möglich ist.
- **Integritäts- und Übermittlungskontrolle:** Um die **Integrität** der verarbeiteten Daten zu wahren, kommen Prüfsummen und Validierungen zum Einsatz (z.B. Prüfsummen für Dateien, um Veränderungen zu erkennen). Änderungen an Transkript-Daten durch berechtigte Nutzer werden versioniert oder protokolliert, sodass versehentliche oder unbefugte Änderungen nachvollziehbar sind. Bei der Übertragung der Daten wird durch TLS nicht nur Vertraulichkeit, sondern auch Integrität gegen Manipulation gewährleistet. Eingaben von Benutzern in die Weboberfläche werden serverseitig validiert (um z.B. injection-Angriffe zu verhindern).
- **Verfügbarkeitskontrolle:** Der Dienst ist auf hohe **Verfügbarkeit** ausgelegt. Microsoft Azure gewährleistet durch redundante Systemarchitektur (Cluster, Load Balancer, verteilte Datenspeicherung) eine sehr hohe Betriebszeit. Es werden **regelmäßige Backups** aller relevanten Daten erstellt (automatisierte tägliche Backups der Transkript-Datenbank und wöchentliche Snapshots der gespeicherten Audiodateien). Die Backups werden an einem geografisch getrennten Azure-Standort innerhalb der EU aufbewahrt, um auch bei regionalen Ausfällen den Datenbestand wiederherstellen zu können. Notfallpläne (Disaster-Recovery-Plan) sind definiert: Bei Systemausfällen können Backups innerhalb kurzer Zeit (i.d.R. < 4 Stunden) eingespielt und der Dienst wiederhergestellt werden. Wichtige Serverkomponenten sind gegen Stromausfall (USV, Backup-Generatoren im Rechenzentrum) und gegen Netzwerkausfall (redundante Leitungen) abgesichert. Regelmäßige **Stresstests** und Monitoring der Systemauslastung stellen sicher, dass auch unter hoher Last die Performance erhalten bleibt. Bei Erreichen definierter Schwellwerte wird automatisch skaliert (Azure Autoscale), um die Dienstverfügbarkeit sicherzustellen.
- **Belastbarkeit und Wiederherstellung:** Lumitra testet die **Notfallmechanismen** regelmäßig. Backup-Routinen werden überwacht; erfolgreiche und fehlgeschlagene Backup-Läufe werden gemeldet. Datenwiederherstellungsübungen (Restore-Tests) finden in regelmäßigen Abständen statt, um sicherzustellen, dass Backups im Ernstfall korrekt eingespielt werden können. Es existiert ein internes **Notfallhandbuch**, das Abläufe bei schwerwiegenden Vorfällen (z.B. kompletter Systemausfall, Cyberangriff) festlegt. Verantwortlichkeiten im Krisenfall sind benannt (Incident Response Team). Durch diese Vorkehrungen wird eine schnelle Wiederaufnahme des Betriebs und Minimierung von Ausfallzeiten gewährleistet.
- **Organisatorische Maßnahmen und Management:** Lumitra hat interne **Datenschutz- und IT-Sicherheitsrichtlinien**, die den Umgang mit personenbezogenen Daten regeln.

Mitarbeiter werden **regelmäßig geschult** in Bezug auf Datenschutz (DSGVO-Bestimmungen, Vertraulichkeit) und IT-Sicherheit (sicheres Passwortverhalten, Phishing-Erkennung, etc.). Neue Mitarbeiter erhalten initiale Schulungen vor Datenzugriff. Verstöße gegen die Richtlinien werden sanktioniert. Es bestehen Prozesse für **Incident Management**: Sicherheitsvorfälle können Mitarbeiter jederzeit an ein internes Incident Response Team melden, welches umgehend Gegenmaßnahmen einleitet. Lumitra unterzieht sich zudem freiwilligen **externen Audits** im Bereich IT-Sicherheit jährlich, um Schwachstellen zu identifizieren und zu beheben (z.B. Penetrationstests durch Spezialisten).

- **Datenschutz-Management und Privacy-by-Design:** Bereits bei der Entwicklung und Weiterentwicklung des Mitschrift-Dienstes berücksichtigt Lumitra die Prinzipien des **Privacy by Design und Default**. Es werden nur erforderliche Datenfelder erhoben, viele Funktionen sind für Nutzer datenschutzfreundlich voreingestellt (z.B. standardmäßige Anonymisierung von Gesprächspartnernamen, wenn vom Verantwortlichen gewünscht). Änderungen an der Applikation durchlaufen eine **Datenschutz-Folgenabschätzung** (falls erforderlich) und werden vom internen Datenschutz-Verantwortlichen geprüft. Lumitra führt ein **Verzeichnis der Verarbeitungstätigkeiten** für die im Auftrag durchgeführten Prozesse und aktualisiert dieses bei Änderungen.

Diese technische und organisatorische Maßnahmenliste stellt den **aktuellen Stand** zum Vertragsabschluss dar. Der Auftragsverarbeiter behält sich vor, Weiterentwicklungen seiner Sicherheitsmaßnahmen vorzunehmen, sofern dadurch das Schutzniveau nicht reduziert wird. Wesentliche Änderungen werden mit dem Verantwortlichen abgestimmt. Der Verantwortliche kann überprüfen, ob die Maßnahmen den vereinbarten Anforderungen genügen und gegebenenfalls zusätzliche Sicherheitsmaßnahmen verlangen, sofern dies aufgrund besonderer Umstände der Verarbeitung erforderlich ist. Die Parteien arbeiten vertrauensvoll zusammen, um ein hohes Datenschutzniveau dauerhaft zu gewährleisten.

Ende des AV-Vertrags