Vereinbarung zur Auftragsverarbeitung (AVV)

nach Art. 28 Datenschutz-Grundverordnung (DSGVO)

Version 1.0, Stand: 22. September 2026

Parteien

Kunde (Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO):

Firma / Name: _____

Anschrift: _____

E-Mail des scryp-Kontos: _____

scryp (Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO):

Gökhan Sagir, Einzelunternehmer, handelnd unter der Marke scryp
Erdbergstraße 121/9, 1030 Wien, Österreich
UID: ATU83108129
Datenschutz-Kontakt: datenschutz@scryp.at

Im Folgenden „Kunde" und „scryp", gemeinsam „Parteien".

Worum es geht

Der Kunde nutzt scryp, um Audio- und Videoaufnahmen transkribieren und auswerten zu lassen. In diesen Aufnahmen sprechen Menschen, deren personenbezogene Daten der Kunde verantwortet. scryp verarbeitet diese Daten nur im Auftrag des Kunden. Diese Vereinbarung legt fest, was scryp mit den Daten tun darf, wie scryp sie schützt und was am Ende mit ihnen geschieht.

1. Gegenstand und Geltung

1.1 Diese Vereinbarung gilt für alle personenbezogenen Daten, die scryp bei der Erbringung des Dienstes scryp nach den Allgemeinen Geschäftsbedingungen (AGB, abrufbar unter www.scryp.at/agb) im Auftrag des Kunden verarbeitet. Der Vertrag über die Nutzung des Dienstes wird im Folgenden „Hauptvertrag" genannt. Die jeweils aktuelle Fassung dieser Vereinbarung ist unter www.scryp.at/avv abrufbar.

1.2 Nicht Gegenstand dieser Vereinbarung sind die Daten der Vertragsbeziehung selbst, also Konto-, Vertrags-, Abrechnungs- und Support-Daten des Kunden. Diese verarbeitet scryp als eigener Verantwortlicher nach seiner Datenschutzerklärung (www.scryp.at/datenschutz).

1.3 Die Anlagen 1 bis 3 sind Bestandteil dieser Vereinbarung. Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag geht in Fragen des Datenschutzes diese Vereinbarung vor.

1.4 Diese Vereinbarung ist für Kunden bestimmt, die scryp im Rahmen einer beruflichen, geschäftlichen oder behördlichen Tätigkeit nutzen. Bei rein privater Nutzung ist die DSGVO nach Art. 2 Abs. 2 lit. c nicht anwendbar, und es ist kein Auftragsverarbeitungsvertrag erforderlich.

2. Art, Zweck und Umfang der Verarbeitung

2.1 Art und Zweck der Verarbeitung, die Arten der Daten und die Kategorien der betroffenen Personen sind in Anlage 1 beschrieben.

2.2 scryp verarbeitet die Daten ausschließlich in Mitgliedstaaten der Europäischen Union. Die Verarbeitungsorte sind in Anlage 1 und Anlage 3 genannt.

2.3 Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags zuzüglich der in Ziffer 12 geregelten Löschfristen.

3. Weisungen

3.1 scryp verarbeitet die Daten nur auf dokumentierte Weisung des Kunden. Die Weisungen des Kunden sind der Hauptvertrag, diese Vereinbarung und die Nutzung der Funktionen des Dienstes durch den Kunden (insbesondere Hochladen, Transkribieren, Auswerten, Bearbeiten, Teilen, Exportieren und Löschen). Jede Nutzung einer Funktion ist eine dokumentierte Einzelweisung, die dazugehörige Verarbeitung auszuführen.

3.2 Weitere Weisungen erteilt der Kunde schriftlich; E-Mail an datenschutz@scryp.at genügt. Weisungsberechtigt sind der Kontoinhaber und die Personen, die der Kunde für sein scryp-Konto einsetzt. Weisungen, die über den Leistungsumfang des Dienstes hinausgehen, gelten als Antrag auf eine Leistungsänderung.

3.3 Verstößt eine Weisung nach Auffassung von scryp gegen die DSGVO oder andere Datenschutzvorschriften, informiert scryp den Kunden unverzüglich. scryp darf die Ausführung aussetzen, bis der Kunde die Weisung bestätigt oder ändert.

3.4 scryp verwendet die Daten nicht für eigene Zwecke. Insbesondere werden Aufnahmen, Transkripte und Auswertungen des Kunden nicht zum Training oder zur Verbesserung von KI-Modellen verwendet und nicht an Dritte weitergegeben, soweit diese Vereinbarung nichts anderes vorsieht.

3.5 Verlangt eine Behörde oder ein Gericht von scryp die Herausgabe von Daten des Kunden, informiert scryp den Kunden unverzüglich, soweit dies rechtlich zulässig ist, verweist die Stelle an den Kunden und gibt nur heraus, wozu scryp gesetzlich verpflichtet ist. scryp prüft dabei, ob eine gesetzliche Verschwiegenheitspflicht des Kunden der Herausgabe entgegensteht (§ 6 Abs. 5 DSG).

4. Pflichten des Kunden

4.1 Der Kunde ist für die Rechtmäßigkeit der Aufnahmen und ihrer Verarbeitung verantwortlich. Er sorgt insbesondere für eine Rechtsgrundlage (Art. 6, bei besonderen Kategorien Art. 9 DSGVO), für die Information der betroffenen Personen (Art. 13 und 14 DSGVO) und dafür, dass keine nicht öffentlichen Äußerungen ohne Einverständnis der Sprechenden aufgenommen werden (zum Beispiel § 120 StGB in Österreich).

4.2 Enthalten Aufnahmen besondere Kategorien personenbezogener Daten (zum Beispiel Gesundheitsdaten) oder Inhalte, die einem Berufsgeheimnis unterliegen, prüft der Kunde vorab, ob die Verarbeitung zulässig ist und ob eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) erforderlich ist. scryp stellt dafür die Informationen aus dieser Vereinbarung und ihren Anlagen bereit.

4.3 Der Kunde hält die E-Mail-Adresse seines scryp-Kontos aktuell. An diese Adresse richtet scryp alle Mitteilungen nach dieser Vereinbarung, insbesondere Meldungen nach Ziffer 10.

4.4 Der Kunde hat das Recht, scryp Weisungen zu erteilen, Nachweise zu verlangen und Prüfungen nach Ziffer 11 durchzuführen.

5. Vertraulichkeit und Berufsgeheimnis

5.1 scryp gestattet den Zugang zu den Daten nur Personen, die auf das Datengeheimnis (§ 6 DSG) und zur Vertraulichkeit verpflichtet und über die Folgen einer Verletzung belehrt sind (Art. 28 Abs. 3 lit. b, Art. 29 DSGVO). Die Verpflichtung besteht über das Ende der Tätigkeit hinaus.

5.2 scryp ist so gebaut, dass Inhalte des Kunden (Aufnahmen, Transkripte, Auswertungen, Datei- und Ordnernamen) nur verschlüsselt gespeichert werden und im Klartext nur für die Dauer der jeweiligen Verarbeitung im Arbeitsspeicher der Verarbeitungsserver vorliegen. Personen bei scryp haben im laufenden Betrieb keinen Zugriff auf Inhalte im Klartext. Einzelheiten stehen in Anlage 2.

5.3 Unterliegt der Kunde einer gesetzlichen Verschwiegenheitspflicht (zum Beispiel § 9 RAO, § 54 ÄrzteG, § 121 StGB), verpflichtet sich scryp als Hilfskraft des Kunden, alle Inhalte, die scryp im Rahmen der Leistung zugänglich werden, in gleicher Weise geheim zu halten. Für Kunden, die deutschem Recht unterliegen, gilt dies zugleich als Verpflichtung zur Geheimhaltung nach § 203 Abs. 4 StGB (Deutschland). Auf Wunsch bestätigt scryp diese Verpflichtung in einer gesonderten Erklärung.

6. Sicherheit der Verarbeitung

6.1 scryp trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 2 beschrieben sind.

6.2 scryp darf diese Maßnahmen weiterentwickeln und durch gleichwertige oder bessere ersetzen. Das Schutzniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen dokumentiert scryp und teilt sie dem Kunden mit. Die jeweils aktuelle Fassung der Anlage 2 ist unter www.scryp.at/avv abrufbar.

6.3 scryp überprüft die Wirksamkeit der Maßnahmen mindestens einmal jährlich und teilt dem Kunden das Ergebnis auf Anfrage mit.

7. Unterauftragsverarbeiter

7.1 Der Kunde genehmigt die in Anlage 3 genannten Unterauftragsverarbeiter (allgemeine Genehmigung nach Art. 28 Abs. 2 DSGVO).

7.2 Will scryp einen Unterauftragsverarbeiter hinzufügen oder ersetzen, informiert scryp den Kunden mindestens 30 Tage vor dem Einsatz per E-Mail an die Adresse des scryp-Kontos. Der Kunde kann innerhalb von 14 Tagen nach Zugang dieser Mitteilung aus wichtigem datenschutzrechtlichem Grund schriftlich widersprechen; E-Mail genügt. Widerspricht der Kunde nicht, gilt die Änderung als genehmigt.

7.3 Finden die Parteien nach einem Widerspruch keine Lösung, kann der Kunde den Hauptvertrag zum Zeitpunkt des geplanten Einsatzes kündigen. Entgelte, die der Kunde für die Zeit nach der Beendigung vorausbezahlt hat, erstattet scryp anteilig.

7.4 scryp legt jedem Unterauftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die scryp nach dieser Vereinbarung treffen, insbesondere ausreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Erfüllt ein Unterauftragsverarbeiter seine Pflichten nicht, haftet scryp dem Kunden gegenüber für dessen Pflichten wie für eigenes Verhalten.

7.5 Nebenleistungen ohne Zugriff auf Kundendaten, zum Beispiel Telekommunikation, Reinigung oder Wartung ohne Datenzugang, sind keine Unterauftragsverarbeitung.

8. Verarbeitungsort und Drittländer

8.1 scryp verarbeitet und speichert die Daten in Österreich und Deutschland. Eine Übermittlung in Länder außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums findet durch scryp nicht statt.

8.2 Sollte ein Unterauftragsverarbeiter Daten in einem Drittland verarbeiten, geschieht dies nur in dem in Anlage 3 beschriebenen Umfang und nur mit einer geeigneten Garantie nach Kapitel V DSGVO (zum Beispiel Angemessenheitsbeschluss der EU-Kommission oder EU-Standardvertragsklauseln).

9. Unterstützung des Kunden

9.1 Rechte der betroffenen Personen: Der Kunde kann Auskunft, Berichtigung, Löschung und Datenübertragbarkeit in den meisten Fällen selbst über die Funktionen des Dienstes erfüllen (Anzeigen, Bearbeiten, Exportieren, Löschen). Weil scryp Inhalte nur verschlüsselt vorhält, kann scryp nicht feststellen, welche Personen in einer Aufnahme vorkommen. Wendet sich eine betroffene Person an scryp, leitet scryp die Anfrage unverzüglich an den Kunden weiter und beantwortet sie nicht selbst, es sei denn, der Kunde weist scryp dazu an.

9.2 Sicherheit, Datenschutzverletzungen, Datenschutz-Folgenabschätzung und Konsultation der Aufsichtsbehörde (Art. 32 bis 36 DSGVO): scryp unterstützt den Kunden mit den Informationen, die scryp vorliegen, insbesondere mit dieser Vereinbarung, Anlage 2 und den Angaben zu einem Vorfall nach Ziffer 10.

9.3 Unterstützung, die über die Bereitstellung der in dieser Vereinbarung beschriebenen Informationen und Funktionen hinausgeht, darf scryp nach vorheriger Ankündigung angemessen nach Aufwand vergüten lassen. Das gilt nicht, wenn die Unterstützung wegen eines Fehlers von scryp erforderlich wird.

10. Meldung von Verletzungen des Schutzes personenbezogener Daten

10.1 Wird scryp eine Verletzung des Schutzes personenbezogener Daten bekannt, die Daten des Kunden betrifft, meldet scryp dies dem Kunden ohne unangemessene Verzögerung, spätestens innerhalb von 48 Stunden nach Kenntnis, per E-Mail an die Adresse des scryp-Kontos.

10.2 Die Meldung enthält, soweit bekannt: die Art der Verletzung, die betroffenen Datenarten und die ungefähre Zahl der Betroffenen, die wahrscheinlichen Folgen, die ergriffenen und vorgeschlagenen Maßnahmen und eine Kontaktstelle bei scryp. Informationen, die noch nicht vorliegen, reicht scryp ohne unangemessene Verzögerung nach.

10.3 scryp dokumentiert die Verletzung und unterstützt den Kunden bei der Meldung an die Aufsichtsbehörde und der Benachrichtigung der betroffenen Personen. Meldungen an Behörden oder betroffene Personen für den Kunden gibt scryp nur auf dessen Weisung ab. Die Meldung an den Kunden ist kein Schuldeingeständnis.

11. Nachweise und Prüfungen

11.1 scryp stellt dem Kunden alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind. Dazu gehören diese Vereinbarung, die Beschreibung der Maßnahmen in Anlage 2, das Verzeichnis nach Art. 30 Abs. 2 DSGVO, die Zertifizierungen der Unterauftragsverarbeiter und schriftliche Auskünfte auf begründete Fragen des Kunden.

11.2 Reichen diese Nachweise im Einzelfall nicht aus, kann der Kunde selbst oder durch einen zur Vertraulichkeit verpflichteten Prüfer, der kein Wettbewerber von scryp ist, eine Prüfung einschließlich Inspektion durchführen. Prüfungen finden höchstens einmal pro Kalenderjahr statt, nach Ankündigung von mindestens 30 Tagen, während der üblichen Geschäftszeiten und ohne Störung des Betriebs. Bei konkreten Anhaltspunkten für einen Verstoß oder auf Verlangen einer Aufsichtsbehörde ist die Prüfung auch kurzfristig und häufiger möglich.

11.3 Die Prüfung erstreckt sich nicht auf Daten anderer Kunden und nicht auf Rechenzentren von Unterauftragsverarbeitern. Für diese gelten deren Zertifizierungen und Prüfberichte. Jede Partei trägt ihre eigenen Kosten der Prüfung.

12. Löschung und Rückgabe der Daten

12.1 Während der Laufzeit kann der Kunde seine Daten jederzeit selbst löschen und in gängigen Formaten exportieren. Gelöschte Inhalte werden sofort aus dem aktiven Datenbestand entfernt.

12.2 Hochgeladene Originaldateien löscht scryp automatisch nach Abschluss der Verarbeitung, im Regelfall innerhalb weniger Minuten, spätestens jedoch 72 Stunden nach dem Hochladen. Gespeichert bleiben nur die verschlüsselte Wiedergabeversion, das verschlüsselte Transkript und die verschlüsselten Auswertungen.

12.3 Nach Ende des Hauptvertrags stehen die Inhalte dem Kunden noch bis zu 90 Tage zum Export zur Verfügung. Danach löscht scryp sie einschließlich aller Kopien automatisch. Löscht der Kunde sein Konto, werden alle Daten sofort gelöscht.

12.4 Sicherungskopien dienen nur der Wiederherstellung des Gesamtsystems. Sie enthalten Inhalte des Kunden ausschließlich verschlüsselt und werden spätestens nach 30 Tagen überschrieben. Eine Wiederherstellung einzelner gelöschter Kundendaten aus Sicherungskopien findet nicht statt.

12.5 Daten, die scryp aufgrund gesetzlicher Aufbewahrungspflichten weiter speichern muss (zum Beispiel Rechnungsdaten nach § 132 BAO), sind von der Löschung ausgenommen. Sie werden gesperrt und nach Ablauf der Frist gelöscht.

12.6 Auf Verlangen bestätigt scryp die Löschung schriftlich; E-Mail genügt.

13. Haftung

13.1 Gegenüber betroffenen Personen haften die Parteien nach Art. 82 DSGVO.

13.2 Im Verhältnis der Parteien zueinander gelten die Haftungsregelungen des Hauptvertrags, soweit gesetzlich zulässig. Für Unterauftragsverarbeiter haftet scryp wie für eigenes Verhalten (Ziffer 7.4).

13.3 Hat eine Partei Schadenersatz an betroffene Personen geleistet, kann sie von der anderen Partei den Teil zurückverlangen, der deren Anteil an der Verantwortung für den Schaden entspricht (Art. 82 Abs. 5 DSGVO).

13.4 Hält der Kunde eine Weisung aufrecht, obwohl scryp ihn nach Ziffer 3.3 auf deren Rechtswidrigkeit hingewiesen hat, stellt der Kunde scryp von allen Ansprüchen Dritter und Bußgeldern frei, die auf dieser Weisung beruhen.

14. Laufzeit, Aussetzung und Beendigung

14.1 Diese Vereinbarung gilt, solange scryp Daten für den Kunden verarbeitet, also für die Dauer des Hauptvertrags und bis zum Abschluss der Löschung nach Ziffer 12.

14.2 Eine Nutzung des Dienstes ohne diese Vereinbarung ist für Kunden nach Ziffer 1.4 nicht vorgesehen. Die Kündigung dieser Vereinbarung gilt daher zugleich als Kündigung des Hauptvertrags.

14.3 Verstößt scryp gegen diese Vereinbarung, kann der Kunde verlangen, dass scryp die betroffene Verarbeitung aussetzt, bis der Verstoß behoben ist. Stellt scryp einen erheblichen Verstoß nicht innerhalb eines Monats nach Aufforderung ab, kann der Kunde den Hauptvertrag fristlos kündigen.

15. Schlussbestimmungen

15.1 Diese Vereinbarung wird in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO). Für Kunden nach Ziffer 1.4 wird sie durch die Einbeziehung in die AGB mit dem Abschluss des Hauptvertrags Bestandteil des Vertrags; Vertragspartei ist dann der Inhaber des scryp-Kontos mit den dort hinterlegten Angaben. Daneben kann sie durch beidseitige Unterzeichnung dieses Dokuments geschlossen werden, auch als elektronische Kopie.

15.2 Änderungen dieser Vereinbarung bedürfen der Schriftform; E-Mail genügt. scryp darf Anlage 2 nach Ziffer 6.2 und Anlage 3 nach Ziffer 7.2 anpassen. Andere Änderungen kündigt scryp mindestens 30 Tage vor dem

Inkrafttreten per E-Mail an; der Kunde kann bis dahin widersprechen und den Hauptvertrag zu diesem Zeitpunkt kündigen. scryp hält jede Fassung dieser Vereinbarung mit Versionsnummer und Datum vor.

15.3 Es gilt österreichisches Recht; die DSGVO bleibt unberührt. Ist der Kunde Unternehmer, ist für alle Streitigkeiten aus dieser Vereinbarung das sachlich zuständige Gericht in Wien ausschließlich zuständig. Zwingende gesetzliche Gerichtsstände bleiben unberührt.

15.4 Sollte eine Bestimmung unwirksam sein, bleibt der Rest der Vereinbarung wirksam. An die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung, die ihrem Zweck am nächsten kommt.

15.5 Ansprechpartner für alle Fragen dieser Vereinbarung ist bei scryp datenschutz@scryp.at. Auf Seiten des Kunden ist es die E-Mail-Adresse des scryp-Kontos, sofern der Kunde nichts anderes mitteilt.

15.6 scryp stellt diese Vereinbarung in mehreren Sprachen bereit. Verbindlich ist die deutsche Fassung; Übersetzungen dienen dem Verständnis. Bei Abweichungen gilt der deutsche Wortlaut.

Unterschriften

Für den Kunden	**Für scryp**
Ort, Datum	Ort, Datum
Name, Funktion	Gökhan Sagir, Einzelunternehmer
Unterschrift	Unterschrift

Anlage 1: Beschreibung der Verarbeitung

Punkt	Beschreibung
Gegenstand	Bereitstellung des Dienstes scryp: Transkription von Audio- und Videoaufnahmen mit Spracherkennung und Sprechererkennung, im Ultra-Plan zusätzlich KI-Funktionen (KI-gestützte Auswertung: Zusammenfassung, Protokoll, Aufgabenliste, Social-Media-Text), sowie Speicherung, Bearbeitung, Export und Teilen der Ergebnisse.
Zweck	Der Kunde lässt eigene Aufnahmen in Text umwandeln und auswerten, zum Beispiel Besprechungen, Interviews, Diktate, Beratungsgespräche, Vorträge oder Podcasts.
Art der Verarbeitung	Entgegennahme verschlüsselter Dateien, kurzzeitige Entschlüsselung im Arbeitsspeicher der Verarbeitungsserver, automatische Transkription und Auswertung, Verschlüsselung der Ergebnisse, verschlüsselte Speicherung, Bereitstellung im Konto des Kunden, Löschung.
Datenarten	Sprachaufnahmen und Videos (Stimme, gesprochene Inhalte), daraus erzeugte Transkripte und Auswertungen, Sprecherzuordnungen, vom Kunden vergebene Datei- und Ordnernamen, technische Metadaten (Dauer, Dateigröße, Zeitpunkte, erkannte Sprache, Verarbeitungsstatus), bei geteilten Transkripten der Teilen-Link. Alle Inhalte werden verschlüsselt gespeichert; nur die technischen Metadaten liegen im Klartext vor.
Besondere Kategorien (Art. 9 DSGVO)	Möglich, abhängig vom Inhalt der Aufnahmen des Kunden (zum Beispiel Gesundheitsdaten in Arztdiktaten, Angaben in Beratungs- oder Mandantengesprächen). scryp kennt den Inhalt nicht. Die Zulässigkeit prüft der Kunde nach Ziffer 4.2.
Garantien für besondere Kategorien	Verschlüsselung im Browser des Kunden, Klartext nur im Arbeitsspeicher der eigenen Server von scryp in Wien, keine Weitergabe von Inhalten an Unterauftragsverarbeiter im Klartext, kein Zugriff von Personen auf Inhalte im laufenden Betrieb, Verschwiegenheitspflicht nach Ziffer 5, kein Training von KI-Modellen mit Kundendaten.
Betroffene Personen	Personen, die in den Aufnahmen sprechen oder genannt werden (zum Beispiel Mitarbeiter, Kunden, Patienten, Mandanten, Interviewpartner, Teilnehmer von Besprechungen und Veranstaltungen), sowie die Nutzer des Kundenkontos.
Verarbeitungsorte	Transkription und KI-Auswertung: eigene GPU-Server von scryp in Wien, Österreich. Webanwendung, Schnittstellen, Datenbank, verschlüsselter Dateispeicher und Sicherungskopien: Rechenzentrum der Hetzner Online GmbH in Nürnberg, Deutschland.
Dauer	Laufzeit des Hauptvertrags zuzüglich Löschfristen nach Ziffer 12.

Anlage 2: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Stand: 22. September 2026. Die Maßnahmen beschreiben den Regelbetrieb von scryp.

1. Verschlüsselung und Zero-Knowledge-Architektur

- Aufnahmen werden bereits im Browser des Kunden mit AES-256-GCM verschlüsselt, bevor sie an scryp übertragen werden. Für jede Datei wird ein eigener Dateischlüssel (FEK) erzeugt.
- Dateischlüssel werden mit einem Hauptschlüssel des Kontos (MEK) verschlüsselt. Der Hauptschlüssel ist nur mit dem Passwort des Kunden zugänglich (Ableitung mit PBKDF2-SHA256, 600.000 Iterationen). scryp kennt weder Passwort noch Hauptschlüssel im Klartext.
- Für die Transkription übermittelt der Browser den Dateischlüssel mit einem Server-Schlüssel (RSA-4096, OAEP) verschlüsselt an scryp. Der Verarbeitungsserver entschlüsselt die Aufnahme ausschließlich im Arbeitsspeicher. Temporäre Dateien liegen in einem RAM-Dateisystem und werden nach dem Auftrag verworfen; unverschlüsselte Inhalte werden zu keinem Zeitpunkt auf Datenträger geschrieben.
- Transkripte und Auswertungen werden direkt nach der Erstellung mit dem Dateischlüssel verschlüsselt und nur verschlüsselt gespeichert. Datei- und Ordnernamen werden im Browser verschlüsselt.
- Beim Teilen eines Transkripts wird der Dateischlüssel mit einem aus dem Teilen-Passwort abgeleiteten Schlüssel verschlüsselt. Empfänger entschlüsseln ausschließlich im eigenen Browser.
- Ausnahme URL-Upload: Ruft der Kunde eine Aufnahme über eine Internetadresse ab, lädt der Verarbeitungsserver die Datei direkt, verarbeitet sie im Arbeitsspeicher und löscht sie danach; Transkript und Wiedergabeversion werden wie sonst verschlüsselt gespeichert.
- Alle Verbindungen sind mit TLS 1.2 oder 1.3 verschlüsselt.

2. Zutrittskontrolle

- Webanwendung, Datenbank, Dateispeicher und Sicherungskopien laufen im Rechenzentrum der Hetzner Online GmbH in Nürnberg (ISO/IEC 27001 zertifiziert, BSI-C5-Testat Typ 2) mit Zutrittskontrolle, Videoüberwachung und Sicherheitspersonal des Betreibers.
- Die GPU-Server für Transkription und KI-Auswertung stehen in eigenen, abgeschlossenen Räumen von scryp in Wien. Zutritt haben nur berechtigte Personen; der Zugang ist mechanisch versperrt und zusätzlich biometrisch gesichert.
- Alle Datenträger dieser Server sind vollständig verschlüsselt. Bei Diebstahl oder Ausbau eines Datenträgers bleiben die Daten ohne den Schlüssel unlesbar. Unverschlüsselte Inhalte liegen auf diesen Servern nur während eines laufenden Auftrags im Arbeitsspeicher vor und werden nie auf einen Datenträger geschrieben.

3. Zugangs- und Zugriffskontrolle

- Serverzugang nur für Administratoren von scryp über verschlüsselte SSH-Verbindungen mit persönlichen Schlüsseln beziehungsweise zufällig erzeugten, starken Passwörtern; Zugriff nach dem Prinzip der geringsten Rechte.
- Getrennte Verwaltungsoberfläche mit eigener Anmeldung, beschränkt auf freigegebene IP-Adressen. Die Verwaltungsoberfläche zeigt nur Konto- und Auftragsmetadaten, keine Inhalte.
- Benutzerkonten: Passwörter werden mit Argon2id gehasht; Schutz vor Anmeldeversuchen durch Ratenbegrenzung und zeitweise Sperre; Sitzungen laufen ohne Cookies mit kurzlebigen Token.
- Schutz der Schnittstellen vor Missbrauch und Überlastung durch Ratenbegrenzung und automatische Sperren.
- Automatisierte Dienste (Verarbeitungsserver) authentifizieren sich mit eigenen, rotierbaren Zugangsdaten und erhalten nur die für den jeweiligen Auftrag nötigen Schlüssel.

4. Trennungskontrolle und Pseudonymisierung

- Kryptografische Trennung: Jeder Kunde hat einen eigenen Hauptschlüssel, jede Datei einen eigenen Dateischlüssel. Inhalte eines Kunden sind mit fremden Schlüsseln nicht lesbar.
- Logische Trennung von Produktions-, Datenbank-, Cache- und Überwachungssystemen in getrennten Netzwerkbereichen.
- Verarbeitungsaufträge an die GPU-Server enthalten keine Namen und keine E-Mail-Adressen, nur die für den Auftrag nötigen technischen Daten.

5. Integrität und Nachvollziehbarkeit

- Alle Änderungen an Anwendung und Infrastruktur erfolgen über versionierten Quellcode und automatisierte, nachvollziehbare Auslieferung; Software-Images werden über ihre Prüfsumme festgelegt.
- Kontoereignisse (zum Beispiel Anmeldung, Löschung, Abonnementänderungen) werden mit Zeitpunkt protokolliert, ohne IP-Adressen.
- Systemprotokolle enthalten keine Inhalte und werden nach 14 Tagen gelöscht. IP-Adressen werden nicht gespeichert und nicht protokolliert. Zur Abwehr von Missbrauch werden Zugriffe nur über ein kurzlebiges, mit einem geheimen Schlüssel gebildetes und nicht rückrechenbares Pseudonym gezählt, das nach höchstens einer Stunde verfällt.

6. Verfügbarkeit und Belastbarkeit

- Hochverfügbarer Cluster aus drei Servern mit Lastverteilung; Datenbank mit synchroner Replikation auf drei Knoten; Cache mit automatischem Failover.
- Tägliche verschlüsselte Sicherung der Datenbank mit Wiederherstellung zu jedem Zeitpunkt der letzten 30 Tage; Cluster-Konfiguration alle sechs Stunden gesichert. Sicherungen liegen im Rechenzentrum in Nürnberg.
- Auslieferung neuer Versionen ohne Betriebsunterbrechung; Schutz vor Überlastungsangriffen auf Netzwerk- und Anwendungsebene.
- Laufende Überwachung mit automatischer Alarmierung bei Störungen.

7. Löschung und Datensparsamkeit

- Hochgeladene Originaldateien werden nach der Verarbeitung gelöscht, im Regelfall innerhalb weniger Minuten; eine automatische Regel entfernt liegengebliebene Uploads spätestens nach 72 Stunden.
- Der Kunde löscht Inhalte und Konto jederzeit selbst; die Löschung wirkt sofort im aktiven Datenbestand. Nach Ende eines Abonnements werden Inhalte nach 90 Tagen automatisch gelöscht.
- Keine Cookies, keine Tracking- oder Analysewerkzeuge Dritter, keine Speicherung von IP-Adressen.

8. Organisation

- Alle bei scryp tätigen Personen sind auf das Datengeheimnis und zur Vertraulichkeit verpflichtet und in die Sicherheitsarchitektur eingewiesen.
- scryp führt ein Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO). Datenschutz-Folgenabschätzung, Verzeichnis und diese Maßnahmen werden mindestens jährlich und bei wesentlichen Änderungen überprüft.
- Vorfallprozess: Erkennung durch Überwachung, Bewertung, Eindämmung, Meldung an betroffene Kunden nach Ziffer 10 der Vereinbarung, Nachbereitung.
- Unterauftragsverarbeiter werden vor dem Einsatz auf ihre Garantien geprüft und vertraglich nach Art. 28 Abs. 4 DSGVO verpflichtet.

Anlage 3: Unterauftragsverarbeiter

Stand: 22. September 2026.

Unterauftragsverarbeiter	Leistung	Daten	Ort der Verarbeitung	Garantie
Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Deutschland	Betrieb der Server für Webanwendung, Schnittstellen und Datenbank; verschlüsselter Objektspeicher; Sicherungskopien	Alle in Anlage 1 genannten Daten, Inhalte ausschließlich verschlüsselt	Nürnberg, Deutschland (EU)	Auftragsverarbeitungsvertrag; ISO/IEC 27001; BSI C5
Mailjet GmbH (Sinch-Konzern), Alt Moabit 2, 10557 Berlin, Deutschland	Versand von System-E-Mails (zum Beispiel Benachrichtigung „Transkript fertig")	E-Mail-Adresse des Kontos, Datum des Auftrags, Link zum Konto; keine Inhalte, keine Dateinamen	Frankreich (EU)	Auftragsverarbeitungsvertrag; ISO/IEC 27001
Microsoft Ireland Operations Ltd., Dublin, Irland	Empfang und Bearbeitung von Support-Anfragen per E-Mail (Microsoft 365)	Nur Daten, die der Kunde selbst in einer Support-Anfrage übermittelt	EU; Fernzugriff aus Drittländern möglich	Auftragsverarbeitungsvertrag; EU-Standardvertragsklauseln; EU-US Data Privacy Framework