



Vertrag zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

für die Nutzung des Dienstes „ChatDecoder“

zwischen

[Name des Kunden / Unternehmens]

[Straße, Hausnummer]

[PLZ, Ort]

vertreten durch: **[Name der/des Vertretungsberechtigten]**

– nachfolgend „**Verantwortlicher**“ oder „**Auftraggeber**“ –

und

Girona Softwareentwicklung und Vertriebsgesellschaft mbH

Machnower Str. 21

14165 Berlin

vertreten durch die Geschäftsführung: Carsten Graeber & Nico Merzbach

E-Mail: office@girona.de

– nachfolgend „**Auftragsverarbeiter**“ –

– beide zusammen „die Parteien“ –

Hinweis: Dies ist ein Vertragsentwurf auf Basis der Anforderungen des Art. 28 DSGVO, erstellt auf Grundlage der auf der ChatDecoder-Website beschriebenen Verarbeitungstätigkeiten. Er ersetzt keine rechtliche Prüfung im Einzelfall. Die mit **[Platzhaltern]** gekennzeichneten Stellen sind vor Nutzung auszufüllen; der gesamte Vertrag sollte vor Unterzeichnung durch einen Rechtsanwalt bzw. eine Datenschutzbeauftragte/einen Datenschutzbeauftragten geprüft werden.

Präambel

Der Auftragsverarbeiter betreibt den Online-Dienst „ChatDecoder“, mit dem Nutzer WhatsApp-Chatverläufe und darin enthaltene Sprachnachrichten hochladen können, um diese transkribieren, analysieren und auswerten zu lassen (z. B. Sentiment-/Gesprächsanalyse, Chronologie, „Ask your Chat“-Funktion). Der Verantwortliche setzt ChatDecoder im Rahmen seiner eigenen Geschäftstätigkeit ein und lädt hierzu personenbezogene Daten (insbesondere Chatinhalte, ggf. auch Daten Dritter, z. B. von Chatpartnern) hoch. Dieser Vertrag regelt die Rechte und Pflichten der Parteien im

Zusammenhang mit der hiermit verbundenen Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen der Nutzung von ChatDecoder. Einzelheiten zu Gegenstand, Art, Zweck und Dauer der Verarbeitung, der Art der personenbezogenen Daten sowie den Kategorien betroffener Personen ergeben sich aus **Anlage 1** zu diesem Vertrag.

(2) Die Laufzeit dieses Vertrags entspricht der Laufzeit des zwischen den Parteien bestehenden Hauptvertrags über die Nutzung von ChatDecoder (Nutzungsvertrag/AGB). Er endet automatisch mit dessen Beendigung, ohne dass es einer gesonderten Kündigung bedarf.

2. Weisungsgebundenheit

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Nutzung der Funktionen von ChatDecoder (Upload, Auswahl der Analysefunktionen, Löschung) durch den Verantwortlichen gilt als Weisung im Sinne dieses Vertrags. Weitergehende Weisungen sind in Textform (auch per E-Mail) zu erteilen.

(3) Hält der Auftragsverarbeiter eine Weisung des Verantwortlichen für rechtswidrig, informiert er den Verantwortlichen unverzüglich und ist berechtigt, die Ausführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung durch den Verantwortlichen auszusetzen.

3. Vertraulichkeit

Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, und dass ihnen die für sie geltenden Bestimmungen zum Datenschutz bekannt sind. Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung der jeweiligen Tätigkeit fort.

4. Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen (TOM) gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Dem Auftragsverarbeiter ist es gestattet, alternative adäquate Maßnahmen

umzusetzen, sofern das Sicherheitsniveau der festgelegten Maßnahmen dabei nicht unterschritten wird.

5. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragsverarbeiter darf die verarbeiteten Daten nicht eigenmächtig berichtigen, löschen oder in ihrer Verarbeitung einschränken, sondern nur nach dokumentierter Weisung des Verantwortlichen. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(2) Soweit im Leistungsumfang von ChatDecoder vorgesehen, ermöglicht der Auftragsverarbeiter dem Verantwortlichen die selbstständige Berichtigung, Löschung und Einschränkung der von ihm verarbeiteten Daten (insbesondere Löschung eigener Analyseergebnisse über das Nutzerkonto) und unterstützt ihn dabei im Rahmen seiner Möglichkeiten.

(3) Hochgeladene Rohdaten (Original-Exportdateien und enthaltene Audiodateien) werden unmittelbar nach Abschluss der jeweiligen Verarbeitung (Transkription/Analyse) automatisiert aus den temporären Speichern des Auftragsverarbeiters gelöscht.

6. Unterstützung des Verantwortlichen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen, soweit dies möglich ist, bei der Erfüllung seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch).

(2) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten (Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen an die Aufsichtsbehörde und Benachrichtigung betroffener Personen, Datenschutz-Folgenabschätzung, vorherige Konsultation), unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

(3) Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten im Zusammenhang mit den im Auftrag verarbeiteten Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Bekanntwerden, und unterstützt ihn bei der Erfüllung seiner Meldepflichten nach Art. 33, 34 DSGVO.

7. Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine Genehmigung zur Beauftragung weiterer Auftragsverarbeiter (Unterauftragsverarbeiter), insbesondere zur Bereitstellung von Hosting-, Transkriptions- und KI-Analyseleistungen, sofern die Voraussetzungen dieses Absatzes eingehalten werden.

(2) Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in **Anlage 3** aufgeführt. Der Auftragsverarbeiter informiert den Verantwortlichen vorab in Textform über die beabsichtigte Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern. Der Verantwortliche kann der Änderung innerhalb von 14 Tagen nach Zugang der Information aus wichtigem, sachlich

begründetem Grund in Textform widersprechen. Erfolgt kein Widerspruch innerhalb dieser Frist, gilt die Änderung als genehmigt.

(3) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter im Wege einer Vereinbarung zu im Wesentlichen denselben Datenschutzpflichten, wie sie in diesem Vertrag festgelegt sind, insbesondere zu ausreichenden Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen sowie zum Ausschluss der Nutzung der Daten zu Trainingszwecken für KI-/Sprachmodelle.

(4) Erfüllt ein Unterauftragsverarbeiter seine Datenschutzpflichten nicht, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten dieses Unterauftragsverarbeiters.

8. Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von ihm beauftragten Prüfer durchgeführt werden, und trägt zu diesen bei.

(2) Kontrollen sind mit angemessenem Vorlauf (mindestens zwei Wochen) unter Berücksichtigung des laufenden Geschäftsbetriebs des Auftragsverarbeiters schriftlich anzukündigen und auf das erforderliche Maß zu beschränken. Der Auftragsverarbeiter kann anstelle einer Vor-Ort-Kontrolle geeignete Nachweise erbringen, z. B. aktuelle Zertifizierungen, Testate oder Auditberichte unabhängiger Prüfer, soweit diese geeignet sind, die Einhaltung dieses Vertrags nachzuweisen.

(3) Der Verantwortliche trägt die Kosten für die Ermöglichung von Vor-Ort-Kontrollen, sofern nicht ein Verstoß des Auftragsverarbeiters gegen diesen Vertrag oder gesetzliche Vorgaben festgestellt wird; in diesem Fall trägt der Auftragsverarbeiter die Kosten.

9. Verarbeitung außerhalb der EU/des EWR

Eine Verarbeitung personenbezogener Daten in einem Drittstaat außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums findet nur statt, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der EU-Kommission oder Abschluss von EU-Standardvertragsklauseln mit dem jeweiligen Empfänger). Der Auftragsverarbeiter informiert den Verantwortlichen auf Anfrage über die getroffenen Garantien.

10. Löschung und Rückgabe von Daten nach Auftragsende

Nach Beendigung der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter alle personenbezogenen Daten, die im Auftrag des Verantwortlichen verarbeitet wurden, vollständig, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (z. B. handels- oder steuerrechtliche Aufbewahrungspflichten für Rechnungsdaten). Eine Rückgabe der Daten erfolgt auf Wunsch des Verantwortlichen in einem gängigen, maschinenlesbaren Format, soweit im Leistungsumfang von ChatDecoder technisch vorgesehen bzw. gesondert vereinbart.

11. Haftung

Für die Haftung der Parteien gelten die gesetzlichen Bestimmungen, insbesondere Art. 82 DSGVO, sowie ergänzend die Haftungsregelungen des zwischen den Parteien bestehenden Hauptvertrags (AGB), soweit diese nicht im Widerspruch zu zwingenden Vorschriften der DSGVO stehen.

12. Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrags sowie seiner Anlagen bedürfen der Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(3) Bei Widersprüchen zwischen diesem Vertrag und Bestimmungen aus sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag/den AGB, gehen die Regelungen dieses Vertrags in Bezug auf die Verarbeitung personenbezogener Daten vor.

(4) Es gilt deutsches Recht. Gerichtsstand ist, soweit gesetzlich zulässig, Berlin.

Anlage 1 – Gegenstand, Dauer, Art und Zweck der Verarbeitung

Gegenstand	Bereitstellung des Dienstes „ChatDecoder“ zur Transkription und Analyse von durch den Verantwortlichen hochgeladenen WhatsApp-Chatverläufen und Sprachnachrichten.
Dauer	Entsprechend der Laufzeit des Hauptvertrags (Nutzungsvertrag) zwischen den Parteien; siehe Ziffer 1 Abs. 2.
Art der Verarbeitung	Erheben, Speichern (temporär bzw. bis zur Löschung durch den Nutzer), Transkribieren, Auswerten (Sentiment-/Gesprächsanalyse, Chronologie, „Ask your Chat“), Übermitteln an Unterauftragsverarbeiter zu Transkriptions-/Analysezwecken, Löschen.
Zweck der Verarbeitung	Erstellung der vom Verantwortlichen beauftragten Analysen und Auswertungen der hochgeladenen Kommunikationsinhalte zu dessen eigenen Zwecken (z. B. berufliche Nutzung, private Auswertung).
Art der personenbezogenen Daten	Kontodaten (Name, E-Mail-Adresse, Passwort-Hash); Inhalte hochgeladener Chat-Exporte (Text und Audio), einschließlich darin enthaltener Kommunikationsinhalte, ggf. Namen, Telefonnummern, Adressen, Standortdaten, Bild-/Sprachinhalte; Analyseergebnisse; Zahlungs- und Abrechnungsdaten; Nutzungs- und Protokolldaten (IP-Adresse, Zeitstempel, Browsertyp).
Kategorien betroffener Personen	Nutzer des Verantwortlichen (z. B. dessen Mandanten, Kunden, Mitarbeiter) sowie an den hochgeladenen Chatverläufen beteiligte Dritte (z. B. Chatpartner), soweit deren Daten in den hochgeladenen Inhalten enthalten sind.
Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)	Können im Einzelfall in hochgeladenen Chatinhalten enthalten sein (z. B. Angaben zu Gesundheit, Religion, politischer Meinung), sofern diese vom Chatpartner mitgeteilt wurden. Der Verantwortliche stellt sicher, dass eine Verarbeitung solcher Daten auf einer geeigneten Rechtsgrundlage erfolgt.

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

1. Vertraulichkeit

- Zutrittskontrolle zu den Serverstandorten durch die jeweiligen Hosting-Anbieter (Rechenzentren in der EU).
- Zugangskontrolle mittels individueller Benutzerkonten, Passwort-Hashing, rollenbasierter Zugriffsrechte.
- Zugriffskontrolle: Beschränkung des internen Zugriffs auf Kundendaten auf das für die Aufgabenerfüllung erforderliche Maß (Need-to-know-Prinzip).
- Verschlüsselung der Datenübertragung ausschließlich über TLS/HTTPS.
- Verschlüsselte Speicherung der Analyseergebnisse.
- Pseudonymisierungs-/Anonymisierungsoption für Namen, Telefonnummern und Adressen vor der Analyse (nutzerseitig aktivierbar).

2. Integrität

- Weitergabekontrolle: Übermittlung an Unterauftragsverarbeiter ausschließlich verschlüsselt und im Rahmen bestehender Auftragsverarbeitungsverträge.
- Eingabekontrolle durch Protokollierung sicherheitsrelevanter Ereignisse (z. B. Logins, Uploads).

3. Verfügbarkeit und Belastbarkeit

- Automatisierte, unmittelbare Löschung von Rohdaten (Original-Exportdateien, Audiodateien) nach Abschluss der Verarbeitung.
- Redundante Auslegung der Infrastruktur beim eingesetzten Hosting-Anbieter, regelmäßige Datensicherungen der Systemumgebung.
- Schutzmaßnahmen gegen Datenverlust und Wiederherstellungsverfahren im Rahmen der Hosting-Infrastruktur.

4. Verfahren zur regelmäßigen Überprüfung

- Regelmäßige Überprüfung der Sicherheitsmaßnahmen und Aktualisierung der eingesetzten Software-Komponenten.
- Vertragliche Bindung sämtlicher Unterauftragsverarbeiter an Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO, einschließlich vertraglichem Ausschluss der Nutzung von Kundendaten zu KI-Trainingszwecken.
- Datenminimierung durch zweckgebundene, temporäre Verarbeitung ohne dauerhafte Vorhaltung von Rohdaten.

Hinweis: Diese Übersicht ist als Grundgerüst zu verstehen und sollte durch den Auftragsverarbeiter um konkrete, aktuell tatsächlich umgesetzte Maßnahmen (z. B. genaue Hosting-Anbieter, Zertifizierungen, Verschlüsselungsstandards) ergänzt werden.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

Unternehmen	Sitz	Gegenstand der Verarbeitung
[z. B. Hosting-Anbieter]	[Land]	Hosting der Anwendung und Speicherung von Nutzerdaten
[Transkriptionsdienst]	[Land]	Umwandlung von Sprachnachrichten in Text
[KI-/Analysedienst]	[Land]	Inhaltliche Analyse der Chatverläufe (Sentiment, Chronologie, „Ask your Chat“)
[Zahlungsdienstleister]	[Land]	Abwicklung von Guthabenaufładungen (PCI-DSS-zertifiziert)

Vor Unterzeichnung ist diese Liste durch den Auftragsverarbeiter um die tatsächlich eingesetzten Dienstleister mit vollständiger Anschrift zu vervollständigen.

Unterschriften

Ort, Datum

Ort, Datum

Für den Verantwortlichen
[Name des Kunden]

Für den Auftragsverarbeiter
Girona Softwareentwicklung und
Vertriebsgesellschaft mbH

Dieses Dokument wurde als Vertragsentwurf erstellt und ersetzt keine individuelle Rechtsberatung. Vor Verwendung wird eine Prüfung durch eine Rechtsanwältin/einen Rechtsanwalt oder eine Datenschutzbeauftragte/einen Datenschutzbeauftragten empfohlen, insbesondere im Hinblick auf die konkret eingesetzten Unterauftragsverarbeiter (Anlage 3) und die tatsächlich umgesetzten technischen und organisatorischen Maßnahmen (Anlage 2).