

Vertrag über die Auftragsverarbeitung nach Artikel 28 DSGVO

InkluDocs – Fassung 1.1 vom 9. September 2026

Dieser Vertrag wird geschlossen zwischen dem Kunden, der den Dienst InkluDocs nutzt (im Folgenden: **Verantwortlicher**),

und

Steve Weidel, INKLUTEC, Ehestorfer Weg 94 C, 21075 Hamburg (im Folgenden: **Auftragsverarbeiter**).

§ 1 Gegenstand und Dauer

(1) Der Auftragsverarbeiter erbringt für den Verantwortlichen den Dienst InkluDocs: die Erzeugung, Verwaltung und den Export von Alternativtexten und Langbeschreibungen für Bilder in Dokumenten und auf Webseiten, einschließlich KI-gestützter Analyse der übermittelten Inhalte.

(2) Gegenstand der Verarbeitung sind die vom Verantwortlichen hochgeladenen oder per URL-Scan übermittelten Dokumente, Bilder und Texte sowie die daraus erzeugten Beschreibungen.

(3) Die Dauer entspricht der Laufzeit des Nutzungsvertrags über InkluDocs. Dieser Vertrag endet automatisch mit dem Nutzungsvertrag.

§ 2 Art und Zweck der Verarbeitung, Datenarten, betroffene Personen

(1) **Art und Zweck:** Speicherung, Analyse und KI-gestützte Beschreibung von Bildinhalten zur Herstellung digitaler Barrierefreiheit; Export der Ergebnisse; auf Wunsch Prüf- und Freigabeworkflows.

(2) **Datenarten:** Die hochgeladenen Dokumente können personenbezogene Daten jeder Art enthalten, insbesondere Namen, Kontaktdaten, Fotografien von Personen, berufsbezogene Angaben sowie — abhängig vom Dokument — besondere Kategorien nach Artikel 9 DSGVO (zum Beispiel eine erkennbare Behinderung auf Fotos oder in Texten). Der Verantwortliche entscheidet allein, welche Dokumente er übermittelt.

(3) **Kategorien betroffener Personen:** Beschäftigte, Kundinnen und Kunden, Mitglieder, Antragstellende und sonstige Personen, die in den Dokumenten des Verantwortlichen erscheinen.

(4) **Ort der Verarbeitung:** Hosting und Datenhaltung in Rechenzentren in Deutschland; die KI-Verarbeitung durch Google Vertex AI kann weltweit erfolgen (Einzelheiten in Anlage 2 und § 6).

§ 3 Pflichten und Rechte des Verantwortlichen

(1) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte betroffener Personen allein verantwortlich. Er stellt sicher, dass er berechtigt ist, die Daten an den

Auftragsverarbeiter zu übermitteln, und dass eine Rechtsgrundlage nach Artikel 6 und, soweit einschlägig, Artikel 9 DSGVO vorliegt.

(2) Der Verantwortliche erteilt alle Weisungen zur Verarbeitung. Die Nutzung der Funktionen des Dienstes gilt als Weisung; darüber hinausgehende Weisungen erfolgen in Textform.

(3) Er ist berechtigt, die Einhaltung dieses Vertrags nach Maßgabe von § 4 Absatz 9 zu überprüfen.

(4) Er unterrichtet den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

(5) Die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde nach Artikel 33 DSGVO und, soweit erforderlich, die Benachrichtigung betroffener Personen nach Artikel 34 DSGVO obliegen dem Verantwortlichen. Der Auftragsverarbeiter unterstützt ihn dabei nach § 4 Absatz 5 und 6.

(6) Der Verantwortliche benennt die zur Erteilung von Weisungen berechtigten Personen (Anlage 3).

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen; die Nutzung der Funktionen des Dienstes durch den Verantwortlichen gilt als Weisung. Erweiterte oder abweichende Weisungen bedürfen der Textform.

(2) Er verwendet die übermittelten Inhalte **nicht für das Training von KI-Modellen** und stellt Gleiches vertraglich bei seinen Unterauftragsverarbeitern sicher.

(3) Alle mit der Verarbeitung befassten Personen sind zur Vertraulichkeit verpflichtet.

(4) Er trifft die technischen und organisatorischen Maßnahmen nach Anlage 1 und passt sie dem Stand der Technik an, ohne das Schutzniveau zu senken.

(5) Er unterstützt den Verantwortlichen im Rahmen des Zumutbaren bei der Beantwortung von Betroffenenanfragen (Artikel 12 bis 23 DSGVO), bei der Sicherheit der Verarbeitung, bei Meldungen von Verletzungen (Artikel 33 und 34 DSGVO) und bei Datenschutz-Folgenabschätzungen (Artikel 35 und 36 DSGVO).

(6) Verletzungen des Schutzes personenbezogener Daten meldet er dem Verantwortlichen unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis, mit den Angaben nach Artikel 33 Absatz 3 DSGVO.

(7) Er informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt, und darf die Ausführung bis zur Bestätigung aussetzen.

(8) Nach Ende des Nutzungsvertrags oder auf Verlangen löscht er alle personenbezogenen Daten oder gibt sie heraus (Wahl des Verantwortlichen), einschließlich Kopien und Sicherungen nach deren Rotationszyklus von 14 Tagen, soweit keine gesetzliche Aufbewahrungspflicht besteht. Der Verantwortliche kann sein Konto und alle Daten jederzeit selbst über die Kontolöschung entfernen.

(9) Er weist die Einhaltung dieses Vertrags auf Anfrage nach (aktuelle Beschreibung der technischen und organisatorischen Maßnahmen, Zertifikate und Prüfberichte der Rechenzentrumsbetreiber, Auskünfte) und ermöglicht — nach angemessener Ankündigung, höchstens einmal jährlich, gegen

Erstattung des Aufwands bei anlasslosen Prüfungen — Kontrollen durch den Verantwortlichen oder einen beauftragten Prüfer.

§ 5 Unterauftragsverarbeiter

- (1) Der Verantwortliche genehmigt allgemein die Einschaltung der in Anlage 2 genannten Unterauftragsverarbeiter.
- (2) Änderungen teilt der Auftragsverarbeiter mindestens vier Wochen vor Wirksamwerden in Textform mit (E-Mail an die Kontoadresse). Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen; führt der Widerspruch zu keiner Einigung, kann jede Seite den Nutzungsvertrag zum Wirksamwerden der Änderung kündigen.
- (3) Mit jedem Unterauftragsverarbeiter bestehen Verträge, die diesem Vertrag im Schutzniveau entsprechen. Beauftragt ein Unterauftragsverarbeiter weitere Stellen, gelten dieselben Anforderungen.

§ 6 Drittlandübermittlung

- (1) Hosting, Datenhaltung und E-Mail-Versand finden in der Europäischen Union statt. Die KI-Verarbeitung durch Google Vertex AI (Anlage 2, Nummer 2) erfolgt über einen globalen Endpunkt und damit gegebenenfalls außerhalb des Europäischen Wirtschaftsraums; die KI-Verarbeitung des Chat-Assistenten durch Amazon Bedrock (Anlage 2, Nummer 3) findet in der Europäischen Union statt.
- (2) Eine Übermittlung in Drittländer erfolgt nur, soweit die Voraussetzungen des Kapitels V DSGVO erfüllt sind. Für die in Anlage 2 genannten Anbieter mit US-Konzernbezug gelten der Angemessenheitsbeschluss zum EU-US Data Privacy Framework und — unabhängig davon und zusätzlich — die EU-Standardvertragsklauseln, die Bestandteil der jeweiligen Auftragsverarbeitungsverträge sind.
- (3) Sollte der Angemessenheitsbeschluss aufgehoben, ausgesetzt oder für ungültig erklärt werden, bleibt die Übermittlung auf Grundlage der Standardvertragsklauseln zulässig. Der Auftragsverarbeiter prüft in diesem Fall unverzüglich, ob zusätzliche Schutzmaßnahmen erforderlich sind, und unterrichtet den Verantwortlichen über das Ergebnis.

§ 7 Haftung und Schlussbestimmungen

- (1) Für die Haftung gilt Artikel 82 DSGVO; im Übrigen gelten die Regelungen des Nutzungsvertrags.
- (2) Bei Widersprüchen zwischen diesem Vertrag und dem Nutzungsvertrag geht in Datenschutzfragen dieser Vertrag vor.
- (3) Es gilt deutsches Recht.

Anlage 1 – Technische und organisatorische Maßnahmen (Artikel 32 DSGVO)

1. Verschlüsselung

Alle Übertragungen erfolgen über TLS. Zugangsdaten werden verschlüsselt gespeichert; Passwörter ausschließlich als kryptografischer Hash. Sicherungen liegen auf verschlüsselten Datenträgern des Rechenzentrumsbetreibers.

2. Vertraulichkeit

- **Zutrittskontrolle:** ISO-27001-zertifizierte Rechenzentren in Deutschland (Hetzner Online GmbH); kein physischer Zugriff Dritter.
- **Zugangskontrolle:** SSH-Schlüssel statt Passwörtern, personalisierte Administrationszugänge, Firewall, automatische Sperren bei wiederholten Fehlversuchen, Anmelde-Ratenbegrenzung in der Anwendung.
- **Zugriffskontrolle:** Rollenkonzept in der Anwendung (Inhaber, Team-Mitglieder, Gastzugänge mit eigenem Token); Administrationszugriff nur durch den Betreiber.
- **Trennungskontrolle:** getrennte Produktions-, Test- und Demonstrationsumgebungen mit eigenen Konfigurationen; mandantenbezogene Datentrennung über Konten- und Projektzuordnung in der Datenbank.

3. Integrität

Protokollierung von Anmeldungen und wesentlichen Änderungen; Übermittlung an Unterauftragsverarbeiter ausschließlich verschlüsselt.

4. Verfügbarkeit und Belastbarkeit

Tägliche Sicherung um 3 Uhr nachts mit einer Aufbewahrung von 14 Tagen; dokumentiertes Wiederherstellungsverfahren; laufende Überwachung durch Verfügbarkeits- und Aufgabenwächter; zeitnahes Einspielen von Sicherheitsaktualisierungen.

5. Regelmäßige Überprüfung

Wiederkehrende Sicherheitsprüfungen, Test der Wiederherstellung und Überprüfung der technischen und organisatorischen Maßnahmen mindestens jährlich. Für die Rechenzentrumsinfrastruktur liegt ein jährlicher Prüfbericht des TÜV Rheinland vor, der Kunden auf Anfrage vorgelegt wird.

6. Auftragskontrolle

Sorgfältige Auswahl der Unterauftragsverarbeiter, abgeschlossene Auftragsverarbeitungsverträge (Anlage 2), Weisungsbindung, keine Nutzung der Inhalte zu eigenen Zwecken, kein Training von KI-Modellen mit Kundendaten.

7. Löschkonzept

Kundendaten bleiben gespeichert, bis der Kunde sie löscht oder sein Konto entfernt. Die Kontolöschung steht jederzeit als Selbstbedienung bereit und entfernt Dateien, Bilder, erzeugte

Texte, Chatverläufe, Freigabe-Links und Schlüssel unwiderruflich. Sicherungen rotieren nach 14 Tagen aus.

Anlage 2 – Unterauftragsverarbeiter (Stand 9. September 2026)

1. **Hetzner Online GmbH**, Industriestraße 25, 91710 Gunzenhausen, Deutschland — Serverbetrieb und Hosting; Rechenzentrum in Deutschland. Auftragsverarbeitungsvertrag nach Artikel 28 DSGVO besteht; die technischen und organisatorischen Maßnahmen werden jährlich vom TÜV Rheinland geprüft.
2. **Google Cloud EMEA Limited**, 70 Sir John Rogerson's Quay, Dublin 2, Irland — KI-Dienst Google Vertex AI mit dem Modell Gemini für die Analyse der Bilder, die Erzeugung der Beschreibungen und der Quickinfos. Die Verarbeitung erfolgt über den globalen Endpunkt und damit gegebenenfalls außerhalb der Europäischen Union. Eingaben und Ausgaben werden nicht für Modelltraining genutzt; der Zwischenspeicher von Google ist für das Projekt abgeschaltet, Eingaben und Ausgaben werden nicht über die Bearbeitung der Anfrage hinaus gespeichert. Bei Verdacht auf Missbrauch kann Google Eingaben bis zu 90 Tage ausschließlich zur Prüfung dieses Verdachts protokollieren; eine Befreiung davon ist beantragt. Grundlage ist das Google Cloud Data Processing Addendum mit integrierten EU-Standardvertragsklauseln; Google LLC ist unter dem EU-US Data Privacy Framework zertifiziert; zum US-Konzernbezug siehe § 6.
3. **Amazon Web Services EMEA SARL**, 38 avenue John F. Kennedy, L-1855 Luxemburg — KI-Dienst Amazon Bedrock in der Region Frankfurt am Main für den Chat-Assistenten. Eingaben und Ausgaben werden nicht dauerhaft gespeichert, nicht an den Modellanbieter weitergegeben und nicht für Modelltraining genutzt. Grundlage ist der AWS-Datenverarbeitungszusatz mit integrierten EU-Standardvertragsklauseln; zum US-Konzernbezug siehe § 6.
4. **ALL-INKL.COM – Neue Medien Münnich**, Hauptstraße 68, 02742 Friedersdorf, Deutschland — Versand von Transaktions-E-Mails und Betrieb der Support-Postfächer. Auftragsverarbeitungsvertrag nach Artikel 28 DSGVO besteht.
5. **Tavily Inc.**, Vereinigte Staaten — nur bei aktiver Nutzung der optionalen Websuche im Chat-Assistenten; übermittelt wird ausschließlich die jeweilige Suchanfrage. Grundlage sind die EU-Standardvertragsklauseln. Wer die Websuche nicht nutzt, löst keine Übermittlung aus.

Nicht als Unterauftragsverarbeiter beteiligt: PDFix (lokal auf unserem Server eingesetzte Programmbibliothek, kein Datenabfluss); Stripe (eigener Verantwortlicher für die Zahlungsabwicklung, erhält keine Dokumentdaten — Einzelheiten in der Datenschutzerklärung); Anthropic (der Modellanbieter erhält über Amazon Bedrock bei den eingesetzten Modellen keine Kundendaten).

Anlage 3 – Weisungsberechtigte

Weisungen erteilt der Verantwortliche über die Funktionen des Dienstes oder in Textform an kontakt@inkludoc.de, alternativ an support@inkludoc.de. Auf Seiten des Auftragsverarbeiters ist Steve Weidel empfangsberechtigt.

Abschluss

Dieser Vertrag kann nach Artikel 28 Absatz 9 DSGVO in elektronischer Form geschlossen werden. Er gilt mit der Zustimmung des Verantwortlichen als geschlossen; eine eigenhändige Unterschrift ist nicht erforderlich.

Ort und Datum der Zustimmung: _____

Verantwortlicher (Firma, Name): _____

INKLUTEC · Inhaber: Steve Weidel · Ehestorfer Weg 94 C · 21075 Hamburg · kontakt@inklutec.de · Steuernummer 47/261/02509 · Gemäß § 19 UStG wird keine Umsatzsteuer berechnet.

Fassung 1.1 vom 9. September 2026 (Fassung 1.0 vom 24. August 2026: Anlage 2 um Google Cloud EMEA Limited ergänzt, § 2 Absatz 4 und § 6 Absatz 1 angepasst). Änderungen der Anlage 2 werden nach § 5 Absatz 2 mitgeteilt.