Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO

Stand: 28.05.2026

zwischen

dem Kunden (nachfolgend „Auftraggeber" oder „Verantwortlicher")

– Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO –

und

Kipti GmbH Hermann-Glüsenkamp-Straße 5 49086 Osnabrück Geschäftsführer: Björn Schriewer Registergericht: Amtsgericht Osnabrück, HRB 222888

(nachfolgend „Auftragnehmer" oder „Auftragsverarbeiter")

– Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO –

– Auftraggeber und Auftragnehmer nachfolgend gemeinsam „Parteien" –

Präambel

Der Auftraggeber nutzt die cloudbasierte, KI-gestützte Dokumentations- und Kommunikationsplattform „Kipti" (nachfolgend „Plattform") des Auftragnehmers auf Grundlage der Allgemeinen Geschäftsbedingungen (AGB) des Auftragnehmers (nachfolgend „Hauptvertrag"). Im Rahmen der Nutzung der Plattform verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers.

Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV") konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Auftragsverarbeitung gemäß Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, nachfolgend „DSGVO").

Auftraggeber im Sinne dieses AVV ist:

a) Bei einem **Organisationskunden** (§ 1 Abs. 2 lit. a AGB): die Organisation selbst, vertreten durch den Administrator, der den AVV im Rahmen der Organisationsregistrierung akzeptiert.

b) Bei einem **Einzelkunden** (§ 1 Abs. 2 lit. b AGB): der Einzelkunde selbst, der den AVV in eigener Person als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO akzeptiert.

---

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Rahmen der Bereitstellung und Nutzung der Plattform gemäß dem Hauptvertrag.

(2) Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags. Dieser AVV endet automatisch mit Beendigung des Hauptvertrags, unbeschadet der Pflichten zur Datenlöschung und -rückgabe gemäß § 12\.

(3) Dieser AVV ist Bestandteil des Hauptvertrags. Im Falle von Widersprüchen zwischen den Bestimmungen dieses AVV und dem Hauptvertrag gehen die Bestimmungen dieses AVV in Bezug auf datenschutzrechtliche Regelungen vor.

---

§ 2 Art und Zweck der Verarbeitung

(1) Die Verarbeitung erfolgt zum Zweck der Bereitstellung der Plattform und der darin enthaltenen Funktionalitäten für den Auftraggeber, insbesondere:

a) Hosting und Speicherung von Dokumentationsdaten (Notizen, Beobachtungen, Berichte, Profile) auf der Plattform;

b) Bereitstellung der KI-gestützten Chatfunktion zur Strukturierung und Aufbereitung gespeicherter Informationen;

c) KI-gestützte Erstellung von Zusammenfassungen, Berichten und Dokumentationsentwürfen;

d) Bereitstellung von Kommunikationsfunktionen zwischen autorisierten Plattform-Nutzern;

e) technischer Support und Wartung der Plattform (Sicherheit und Verfügbarkeit);

f) Benutzerverwaltung und Zugriffskontrolle (Erkennen von Nutzung entgegen AGB);

g) Bereitstellung von Produkt-, Onboarding- und Dokumentationsvideos.

(2) Die Art der Verarbeitung umfasst insbesondere das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung (innerhalb der Plattform), Abgleichen, Verknüpfen, Einschränken, Löschen und Vernichten von personenbezogenen Daten.

(3) Die Verarbeitung im Rahmen der KI-Funktionen umfasst die Übermittlung von Daten an KI-Modelle, die ausschließlich bei Anbietern mit Sitz im Europäischen Wirtschaftsraum (EWR) bezogen werden, die die Verarbeitung innerhalb der Europäischen Union durchführen, oder vom Auftragnehmer selbst innerhalb der eigenen europäischen Infrastruktur gehostet werden. Eine Übermittlung an oder Verarbeitung durch Modell- oder Plattformanbieter mit Sitz außerhalb des EWR findet nicht statt. Die Verwendung von Kundendaten zum Training oder zur Verbesserung von KI-Modellen ist vertraglich ausgeschlossen.

(4) Die Plattform ist nicht für automatisierte Entscheidungsfindung im Sinne des Art. 22 DSGVO oder Profiling im Sinne des Art. 4 Nr. 4 DSGVO bestimmt. Der Auftragnehmer hat technische und organisatorische Maßnahmen getroffen, die darauf ausgerichtet sind, eine solche Nutzung zu verhindern, insbesondere durch die Beschränkung der KI-Funktionen auf unterstützende Dokumentationstätigkeiten mit ausschließlichem Vorschlagscharakter (Human-in-the-Loop-Prinzip). Der Auftraggeber stellt im Rahmen seiner Verantwortlichkeit sicher, dass die Plattform durch seine Nutzer nicht für Profiling oder automatisierte Entscheidungen eingesetzt wird.

---

§ 3 Art der personenbezogenen Daten

(1) Folgende Arten personenbezogener Daten sind Gegenstand der Verarbeitung:

Daten der dokumentierten Personen:

a) Stammdaten (z.B. Name, Vorname, Geburtsdatum, Klasse/Gruppe, Geschlecht);

b) pädagogische Dokumentationsdaten (z.B. Beobachtungen, Notizen, Lernstandsbeschreibungen, Entwicklungsverläufe, Berichte, Bewertungsentwürfe);

c) Kommunikationsdaten (z.B. Gesprächsnotizen, Elterngespräch-Protokolle, Austausch zwischen Fachkräften);

d) gegebenenfalls besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO, insbesondere Gesundheitsdaten, soweit vom Auftraggeber im Rahmen der bestimmungsgemäßen Nutzung in die Plattform eingegeben.

Daten der Plattform-Nutzer (Endnutzer und Einzelkunden):

a) Registrierungsdaten (z.B. Name, E-Mail-Adresse, Funktion/Rolle);

b) Nutzungsdaten (z.B. Log-In-Zeiten, Aktivitätsprotokolle, Einstellungen);

c) Inhaltsdaten (z.B. von Nutzern erstellte Notizen, Eingaben, Chatverläufe mit der KI-Funktion);

d) technische Videoabrufdaten beim Abspielen von Kipti-Produkt-, Onboarding- oder Dokumentationsvideos (z.B. IP-Adresse, User-Agent, grober Standort, Abrufzeitpunkt, Auslieferungsprotokolle).

(2) Die Entscheidung über Art und Umfang der verarbeiteten personenbezogenen Daten liegt allein beim Auftraggeber. Der Auftragnehmer hat keinen Einfluss darauf, welche personenbezogenen Daten über die Plattform verarbeitet werden.

---

§ 4 Kategorien betroffener Personen

Die von der Verarbeitung betroffenen Personen umfassen:

a) Dokumentierte Personen, über die der Auftraggeber oder seine Nutzer Informationen in der Plattform erfassen (z. B. Schülerinnen und Schüler, Kinder, Klientinnen und Klienten, betreute oder begleitete Personen), einschließlich Minderjähriger;

b) Sorgeberechtigte und Angehörige der dokumentierten Personen;

c) Plattform-Nutzer (z. B. Fachkräfte, Mitarbeitende, Verwaltungskräfte oder private Nutzer);

d) sonstige Personen, deren Daten vom Auftraggeber in die Plattform eingegeben werden.

§ 5 Weisungsgebundenheit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO), es sei denn, er ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Weisungen des Auftraggebers werden in der Regel durch die Nutzung der Plattform und deren Konfiguration erteilt. Dieser AVV, der Hauptvertrag und die Konfiguration der Plattform durch den Auftraggeber gelten als dokumentierte Weisungen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung bis zu einer Bestätigung oder Änderung durch den Auftraggeber auszusetzen.

(4) Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, bedürfen einer gesonderten schriftlichen Vereinbarung, einschließlich einer Vereinbarung über etwaige zusätzliche Vergütungen.

§ 6 Vertraulichkeit

(1) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung personenbezogener Daten betrauten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

(2) Der Auftragnehmer gewährleistet, dass sämtliche Personen, die Zugang zu personenbezogenen Daten des Auftraggebers haben, diese ausschließlich entsprechend den Weisungen des Auftraggebers verarbeiten, sofern sie nicht gesetzlich zur Verarbeitung verpflichtet sind.

§ 7 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO).

(2) Die zum Zeitpunkt des Vertragsschlusses getroffenen technisch-organisatorischen Maßnahmen sind in Anlage 1 zu diesem AVV beschrieben.

(3) Der Auftragnehmer ist berechtigt, die technisch-organisatorischen Maßnahmen während der Laufzeit des Vertrages zu ändern, soweit das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen wird der Auftragnehmer dem Auftraggeber in Textform mitteilen.

§ 8 Unterauftragsverarbeitung

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine schriftliche Genehmigung, Unterauftragsverarbeiter zur Erfüllung seiner vertraglichen Pflichten einzusetzen (Art. 28 Abs. 2 DSGVO).

(2) Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 2 zu diesem AVV aufgeführt. Der Auftraggeber genehmigt den Einsatz der dort genannten Unterauftragsverarbeiter.

(3) Der Auftragnehmer wird den Auftraggeber mindestens vierzehn (14) Tage im Voraus in Textform über die beabsichtigte Hinzuziehung oder Auswechslung eines Unterauftragsverarbeiters informieren. Der Auftraggeber hat das Recht, innerhalb dieser Frist der Änderung aus berechtigten datenschutzrechtlichen Gründen in Textform zu widersprechen.

(4) Widerspricht der Auftraggeber fristgerecht und begründet, wird der Auftragnehmer nach besten Kräften eine alternative Lösung suchen, die den Bedenken des Auftraggebers Rechnung trägt. Kann keine einvernehmliche Lösung gefunden werden,

haben der Auftraggeber und der Auftragnehmer jeweils das Recht, den Hauptvertrag und diesen AVV mit einer Frist von drei (3) Monaten zum Monatsende außerordentlich zu kündigen.

(5) Der Auftragnehmer stellt vertraglich sicher, dass die Bestimmungen dieses AVV auch gegenüber den Unterauftragsverarbeitern gelten. Insbesondere wird der Auftragnehmer den Unterauftragsverarbeitern mindestens gleichwertige Datenschutzpflichten auferlegen, wie sie in diesem AVV vereinbart sind (Art. 28 Abs. 4 DSGVO).

(6) Der Auftragnehmer haftet gegenüber dem Auftraggeber für die Einhaltung der Datenschutzpflichten durch die von ihm eingesetzten Unterauftragsverarbeiter wie für eigenes Handeln.

---

§ 9 Unterstützung bei Betroffenenrechten

(1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Pflichten zur Beantwortung von Anträgen betroffener Personen auf Wahrnehmung ihrer Rechte gemäß Kapitel III der DSGVO (Art. 28 Abs. 3 lit. e DSGVO).

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer zur Geltendmachung ihrer Rechte, wird der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer wird die Anfrage nicht eigenständig beantworten, es sei denn, der Auftraggeber hat ihn hierzu ausdrücklich angewiesen.

(3) Der Auftragnehmer stellt dem Auftraggeber über die Plattform die technischen Möglichkeiten zur Verfügung, Anträge betroffener Personen zu erfüllen, insbesondere zur Auskunftserteilung, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit.

---

§ 10 Meldepflichten bei Datenschutzverletzungen

(1) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 48 Stunden, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist (Art. 33 Abs. 2 DSGVO). Die Benachrichtigung erfolgt in Textform an die vom Auftraggeber hierfür angegebene Kontaktadresse.

(2) Die Benachrichtigung enthält mindestens die folgenden Angaben, soweit dem Auftragnehmer bekannt:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze;

b) den Namen und die Kontaktdaten der Ansprechperson beim Auftragnehmer für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung;

d) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(3) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und arbeitet dabei mit dem Auftraggeber zusammen.

(4) Die Pflicht des Auftraggebers, eine Datenschutzverletzung gegenüber der zuständigen Aufsichtsbehörde (Art. 33 DSGVO) und gegebenenfalls gegenüber den betroffenen Personen (Art. 34 DSGVO) zu melden, bleibt von diesem AVV unberührt. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung dieser Pflichten.

---

§ 11 Unterstützung bei Datenschutzfolgenabschätzung

(1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten im Zusammenhang mit der Durchführung einer Datenschutzfolgenabschätzung (Art. 35 DSGVO) und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde (Art. 36 DSGVO) (Art. 28 Abs. 3 lit. f DSGVO).

(2) Die Unterstützung erfolgt insbesondere durch die Bereitstellung von Informationen über:

a) die Art der Verarbeitung und die eingesetzten technisch-organisatorischen Maßnahmen;

b) die eingesetzten Unterauftragsverarbeiter und deren Standorte;

c) die Zertifizierungen und Audit-Berichte der eingesetzten Infrastrukturdienstleister (insbesondere des Hosting-Dienstleisters gemäß Anlage 2);

d) die Architektur der KI-Funktionen und die Maßnahmen zum Schutz personenbezogener Daten im Rahmen der KI-Verarbeitung.

---

§ 12 Löschung und Rückgabe von Daten

(1) Nach Beendigung des Hauptvertrags löscht der Auftragnehmer sämtliche im Auftrag verarbeiteten personenbezogenen Daten, sofern nicht eine Verpflichtung zur Speicherung nach Unionsrecht oder dem Recht der Mitgliedstaaten besteht (Art. 28 Abs. 3 lit. g DSGVO).

(2) Vor der Löschung stellt der Auftragnehmer dem Auftraggeber für einen Zeitraum von dreißig (30) Tagen nach Beendigung des Hauptvertrags die Möglichkeit bereit, die personenbezogenen Daten in einem gängigen, strukturierten und maschinenlesbaren Format zu exportieren.

(3) Nach Ablauf der in Absatz 2 genannten Frist, spätestens jedoch neunzig (90) Tage nach Beendigung des Hauptvertrags, löscht der Auftragnehmer sämtliche personenbezogenen Daten des Auftraggebers unwiderruflich, einschließlich aller vorhandenen Kopien, soweit keine gesetzlichen Aufbewahrungspflichten dem entgegenstehen.

(4) Der Auftragnehmer bestätigt dem Auftraggeber auf dessen Verlangen die vollständige Löschung der Daten in Textform.

(5) Bestehende gesetzliche Aufbewahrungspflichten bleiben von der Löschungspflicht unberührt. In diesem Fall beschränkt der Auftragnehmer die Verarbeitung auf das gesetzlich erforderliche Maß und löscht die Daten unverzüglich nach Wegfall des Aufbewahrungsgrundes.

---

§ 13 Audit und Kontrolle

(1) Der Auftragnehmer stellt dem Auftraggeber die erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen – einschließlich Inspektionen – durch den Auftraggeber oder einen von diesem beauftragten Prüfer (Art. 28 Abs. 3 lit. h DSGVO).

(2) Der Auftraggeber ist berechtigt, nach rechtzeitiger Vorankündigung (in der Regel mindestens vier (4) Wochen) und während der üblichen Geschäftszeiten Inspektionen durchzuführen oder durch einen sachkundigen, zur Geheimhaltung verpflichteten Dritten durchführen zu lassen. Die Häufigkeit der Inspektionen ist auf einmal pro Kalenderjahr beschränkt, es sei denn, es besteht ein begründeter Verdacht auf einen Datenschutzverstoß.

(3) Als gleichwertige Maßnahme zu einer Vor-Ort-Inspektion kann der Auftragnehmer dem Auftraggeber auf Anfrage die folgenden Nachweise zur Verfügung stellen:

a) aktuelle Zertifizierungen (z. B. ISO 27001, ISO 27701, C5) oder gleichwertige Zertifizierungen;

b) Audit-Berichte unabhängiger Dritter (z. B. SOC 2 Type II);

c) eine aktuelle Zusammenfassung der technisch-organisatorischen Maßnahmen.

(4) Die Kosten der Audits trägt grundsätzlich der Auftraggeber, es sei denn, das Audit ergibt einen erheblichen Verstoß des Auftragnehmers gegen die Bestimmungen dieses AVV. In diesem Fall trägt der Auftragnehmer die Kosten.

---

§ 14 Datenverarbeitung in Drittländern

(1) Der Auftragnehmer verarbeitet die personenbezogenen Daten des Auftraggebers ausschließlich innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums (EU/EWR).

(2) Eine Übermittlung personenbezogener Daten in ein Drittland (d. h. außerhalb des EU/EWR) findet nicht statt, es sei denn, es liegt eine der folgenden Voraussetzungen vor:

a) ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO;

b) geeignete Garantien gemäß Art. 46 DSGVO, insbesondere Standardvertragsklauseln der Europäischen Kommission; oder

c) die ausdrückliche, dokumentierte Weisung des Auftraggebers.

(3) Der Auftragnehmer gewährleistet, dass auch die eingesetzten Unterauftragsverarbeiter die personenbezogenen Daten ausschließlich innerhalb der EU/des EWR verarbeiten, es sei denn, die Voraussetzungen des Absatzes 2 sind erfüllt.

(4) Der Auftragnehmer betreibt die für die Verarbeitung personenbezogener Daten dokumentierter Personen genutzte Infrastruktur ausschließlich bei Anbietern mit Sitz und Verarbeitungsort innerhalb der EU bzw. des EWR. Für das primäre Daten-Hosting (einschließlich der Datenbanken) nutzt der Auftragnehmer eine in Deutschland betriebene, nach dem BSI C5-Kriterienkatalog zertifizierte Cloud-Infrastruktur eines europäischen Anbieters. Datensicherungen (Backups) werden ausschließlich bei europäischen Anbietern mit Speicherort innerhalb der EU vorgehalten. Für diese Teile der Infrastruktur ist sichergestellt, dass sie ausschließlich aus der EU betrieben werden und Zugriffe auf personenbezogene Daten dokumentierter Personen ausschließlich aus der EU erfolgen. Technische Mittel für einen Zugriff auf diese Daten von außerhalb der EU bestehen nicht. Die technische Bereitstellung der KI-Funktionen (Modellinferenz) erfolgt nach Ermessen des Auftragnehmers entweder über selbst gehostete KI-Modelle innerhalb der vorgenannten Infrastruktur, über einen europäischen KI-Plattform-Anbieter oder ergänzend über einen direkten API-Zugriff beim jeweiligen europäischen Modellanbieter. Eine Übermittlung personenbezogener Daten dokumentierter Personen an oder Verarbeitung durch nicht-europäische Modell- oder Plattformanbieter findet nicht statt. Übrige Kundendaten (z. B. Kontakt-, Stamm- und Nutzungsdaten der Plattform-Nutzer) dürfen auch durch Dienstleister mit Sitz außerhalb des EWR verarbeitet werden, sofern mit ihnen ein Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO besteht, sie DSGVO- und, soweit anwendbar, KI-VO-konform handeln und bei Drittlandstransfers geeignete Garantien gemäß Art. 46 DSGVO (Standardvertragsklauseln) vereinbart sind.

---

§ 15 Haftung

(1) Für die Haftung des Auftragnehmers im Rahmen dieses AVV gelten die Haftungsbestimmungen des Hauptvertrags, sofern in diesem AVV nichts Abweichendes geregelt ist.

(2) Die Haftung des Auftragnehmers und des Auftraggebers gegenüber den betroffenen Personen für Schäden, die durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wurden, richtet sich nach Art. 82 DSGVO.

(3) Der Auftraggeber stellt den Auftragnehmer von Ansprüchen Dritter (einschließlich betroffener Personen und Aufsichtsbehörden) frei, die auf einer rechtswidrigen Datenverarbeitung durch den Auftraggeber, einer unzulässigen Weisung des Auftraggebers oder einer Verletzung der Pflichten des Auftraggebers aus diesem AVV beruhen. Dies gilt nicht, soweit der Auftragnehmer den Schaden durch eine Verletzung seiner Pflichten aus diesem AVV (mit-)verursacht hat.

---

§ 16 Datenschutzbeauftragter

Der Auftragnehmer hat einen Datenschutzbeauftragten benannt. Dieser ist erreichbar unter:

E-Mail: datenschutz@kipti.app Anschrift: Kipti GmbH, z. Hd. Datenschutzbeauftragter, Hermann-Glüsenkamp-Straße 5, 49086 Osnabrück

---

§ 17 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses AVV bedürfen der Textform. Dies gilt auch für eine Abbedingung dieses Textformerfordernisses.

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

(3) Es gilt das Recht der Bundesrepublik Deutschland.

(4) Für Streitigkeiten aus oder im Zusammenhang mit diesem AVV gilt die Gerichtsstandsvereinbarung des Hauptvertrags.

(5) Im Falle von Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen in Bezug auf datenschutzrechtliche Regelungen die Bestimmungen dieses AVV vor.

(6) Dieser AVV ist Bestandteil des Hauptvertrags und wird mit dessen Abschluss wirksam. Er endet automatisch mit Beendigung des Hauptvertrags, unbeschadet der Nachlaufpflichten gemäß § 12\.

Anlage 1: Technisch-organisatorische Maßnahmen (TOMs)

Der Auftragnehmer trifft die folgenden technisch-organisatorischen Maßnahmen gemäß Art. 32 DSGVO zum Schutz der im Auftrag verarbeiteten personenbezogenen Daten:

1\. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Die Plattform wird auf Servern in der EU betrieben. Die physische Sicherheit der Rechenzentren wird durch den Hosting-Dienstleister gemäß dessen Sicherheitsstandards gewährleistet, einschließlich:

- mehrstufiger physischer Zugangskontrollen;
- 24/7-Überwachung der Rechenzentren;
- biometrischer Zugangskontrollen und Besucherprotokollierung.

1.2 Zugangskontrolle

- verschlüsselte Übertragung aller Daten mittels TLS 1.2 oder höher;
- Zugang zur Plattform ausschließlich über authentifizierte Benutzerkonten mit sicheren Passwörtern;
- Multi-Faktor-Authentifizierung für administrative Zugänge;
- regelmäßige Überprüfung und Aktualisierung von Zugriffsberechtigungen.

1.3 Zugriffskontrolle

- rollenbasiertes Berechtigungskonzept (Role-Based Access Control, RBAC);
- Zugriff auf personenbezogene Daten nach dem Prinzip der Erforderlichkeit (Least Privilege);
- logische Mandantentrennung zur Sicherstellung der Datenisolation zwischen verschiedenen Kunden;
- granulare Zugriffssteuerung innerhalb der Plattform (nutzer- und rollenbezogene Sichtbarkeit von Datensätzen);

1.4 Trennungskontrolle

- logische Mandantentrennung auf Datenbankebene;
- Trennung von Produktiv-, Test- und Entwicklungsumgebungen;
- Nutzung separater Datenbankschemata oder Row-Level Security zur Datenisolation.

2\. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

- Verschlüsselung sämtlicher Daten bei der Übertragung (TLS 1.2+);
- Verschlüsselung der Daten im Ruhezustand (AES-256 oder gleichwertig);
- sichere API-Kommunikation zwischen Plattformkomponenten;
- keine unverschlüsselte Übertragung personenbezogener Daten.

2.2 Eingabekontrolle

- Protokollierung von Dateneingaben und -änderungen;
- Möglichkeit zur Nachvollziehbarkeit, wer wann welche Daten eingegeben oder verändert hat;
- Versionierung von Änderungen an Datensätzen, soweit technisch möglich und zweckmäßig.

3\. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DSGVO)

- Einsatz einer Hosting-Infrastruktur eines europäischen Anbieters in der EU mit hoher Verfügbarkeit;
- regelmäßige automatisierte Datensicherungen (Backups);
- Wiederherstellbarkeit der Systeme und Daten nach einem physischen oder technischen Zwischenfall;
- Einsatz von Monitoring- und Alerting-Systemen;
- Notfallmanagement und dokumentierte Wiederherstellungsprozeduren.

4\. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- regelmäßige Überprüfung der technisch-organisatorischen Maßnahmen;
- Schwachstellenanalysen und Penetrationstests;
- Schulung der Mitarbeiter zu Datenschutz und Informationssicherheit;

- dokumentiertes Datenschutzmanagement-System;
- regelmäßige Überprüfung der eingesetzten Unterauftragsverarbeiter.

5\. Zertifizierungen der Hosting-Infrastruktur

Unser Hosting-Dienstleister hält mindestens die folgenden anerkannten Zertifizierungen und Prüfberichte vor:

- ISO/IEC 27001 (Informationssicherheits-Managementsystem);
- BSI C5 Typ 2 (Cloud Computing Compliance Criteria Catalogue).

Aktuelle Zertifikate und Prüfberichte werden dem Auftraggeber auf Anfrage gemäß § 13 Abs. 3 zur Verfügung gestellt.

Hinweis: Die vorstehenden Maßnahmen werden durch den Auftragnehmer kontinuierlich weiterentwickelt und dem Stand der Technik angepasst. Eine detaillierte technische Dokumentation kann auf Anfrage bereitgestellt werden.

Anlage 2: Liste der Unterauftragsverarbeiter

Der Auftragnehmer setzt zum Zeitpunkt des Vertragsschlusses die folgenden Unterauftragsverarbeiter ein. Sämtliche Unterauftragsverarbeiter, die personenbezogene Daten dokumentierter Personen verarbeiten, haben ihren Sitz im Europäischen Wirtschaftsraum (EWR) und verarbeiten diese Daten ausschließlich innerhalb der Europäischen Union. Mit allen Unterauftragsverarbeitern bestehen Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO; sie verpflichten sich zur Einhaltung der DSGVO und, soweit anwendbar, der KI-VO. Bei Drittlandübermittlungen besteht eine zulässige Grundlage nach Kapitel V DSGVO, insbesondere ein Angemessenheitsbeschluss gemäß Art. 45 DSGVO oder geeignete Garantien gemäß Art. 46 DSGVO, insbesondere Standardvertragsklauseln.

Unterauftragsverarbeiter	*Sitz*	*Verarbeitungszweck*	*Verarbeitungsort*
Hetzner Online GmbH	*Deutschland*	*Primäres Hosting der Plattform und Datenbanken (Speicherung von Kundendaten und personenbezogenen Daten dokumentierter Personen)*	*EU (Deutschland: Falkenstein/Nürnberg)*
Scaleway S.A.S.	*Frankreich*	*(i) Bereitstellung von KI-Modellen für die Modellinferenz (Open-Source-/Open-Weight-Modelle); (ii) verschlüsselte Datensicherungen (Backups); (iii) transaktionaler E-Mail-Versand an Plattform-Nutzer (z. B. Registrierung, Authentifizierung, Systembenachrichtigungen)*	*EU (Frankreich: Paris)*
Inceptron AB	*Schweden*	*Bereitstellung weiterer KI-Modelle europäischer Anbieter im Wege des direkten API-Zugriffs (Open-Source-/Open-Weight-Modelle)*	*EU (Schweden)*
Stripe Payments Europe, Ltd.	*Irland*	*Zahlungsabwicklung; keine personenbezogenen Daten dokumentierter Personen*	*EU*
Attio Limited	*Vereinigtes Königreich*	*CRM zur Verwaltung von Geschäfts- und Vertriebskontakten (Stamm- und Kontaktdaten potenzieller und bestehender Kunden); keine personenbezogenen Daten dokumentierter Personen*	*Vereinigtes Königreich; bzw. mögliche Verarbeitung in Drittländern*
Mux, Inc.	*USA*	*Video-Hosting, adaptive Wiedergabe und Auslieferung; technische Videoabrufdaten; kein Mux-Data-Tracking; keine Daten dokumentierter Personen*	*Weltweit über Auslieferungsnetzwerke*
PostHog, Inc.	*USA*	*Produktanalyse (Nutzungs-, Verhaltens- und Stammdaten der Plattform-Nutzer); keine personenbezogenen Daten dokumentierter Personen*	*EU-Region des Anbieters*
Functional Software, Inc. (Sentry)	*USA*	*Fehlerüberwachung (technische Daten und Identifier der Plattform-Nutzer); keine personenbezogenen Daten dokumentierter Personen*	*EU-Region des Anbieters*
Cloudflare, Inc.	*USA*	*Authoritative DNS und DNS-01-Validierung von TLS-Zertifikaten; keine personenbezogenen Daten dokumentierter Personen*	*Weltweit*

Hinweise zur Datenverarbeitung:

Hilfsdienste (PostHog, Sentry, Attio): Diese Dienste verarbeiten ausschließlich Daten der Plattform-Nutzer bzw. Geschäftskontakte (Stamm-, Nutzungs- und technische Daten sowie systembezogene E-Mail-Inhalte) und erhalten keinen Zugriff auf personenbezogene Daten dokumentierter Personen. Mit allen Anbietern bestehen Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO. Bei Attio erfolgt die Verarbeitung primär im Vereinigten Königreich auf Grundlage des Angemessenheitsbeschlusses der EU-Kommission gemäß Art. 45 DSGVO; ergänzende Übermittlungen durch Attio in weitere Drittländer erfolgen auf Grundlage geeigneter Garantien gemäß Art. 46 DSGVO. Bei PostHog und Sentry (US-Unternehmen mit Verarbeitung in EU-Regionen) sind Standardvertragsklauseln gemäß Art. 46 DSGVO vereinbart.

Videoauslieferung (Mux): Mux verarbeitet technische Abruf- und Auslieferungsdaten (z. B. IP-Adresse, User-Agent, grob abgeleitete Standortdaten, Abrufzeitpunkte) zur Bereitstellung, Sicherheit und Fehleranalyse. Kipti nutzt Mux ohne Mux-Data-Tracking, ohne Mux-Cookies und ohne personenbezogene Nutzer-, Organisations-, Rollen- oder E-Mail-Metadaten. Drittlandübermittlungen erfolgen auf Grundlage der von Mux bereitgestellten Transfermechanismen, insbesondere EU-U.S. Data Privacy Framework bzw. Standardvertragsklauseln, soweit einschlägig.

Änderungen an der Liste der Unterauftragsverarbeiter werden dem Auftraggeber gemäß § 8 Abs. 3 dieses AVV mindestens vierzehn (14) Tage im Voraus mitgeteilt.