Auftragsverarbeitungsvertrag

gemäß Art. 28 Abs. 3 DS-GVO

Zwischen den nachfolgend bezeichneten Vertragsparteien wird folgender Vertrag zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 der Datenschutz-Grundverordnung (DS-GVO) geschlossen.

Die Vertragsparteien

AUFTRAGGEBER

Unternehmensbezeichnung / Firma:
[Vollständiger Firmenname des Auftraggebers]

Straße, Hausnummer:
[Straße und Hausnummer]

PLZ, Ort:
[PLZ und Ort]

Vertreten durch:
[Name der vertretungsberechtigten Person]

– im Folgenden: Auftraggeber –

und

AUFTRAGSVERARBEITER

Unternehmensbezeichnung / Firma:
4rce.com Digital Technologies GmbH

Straße, Hausnummer:
Grafentraubach 910

PLZ, Ort:

84082 Laberweinting

Vertreten durch:
Volker Geith (Geschäftsführer)

Kontakt Datenschutz:
info@4rce.com | https://aicollab.app

Handelsregister: Amtsgericht Straubing, HRB 13771
USt-IdNr.: DE459375923

– im Folgenden: Auftragsverarbeiter –

schließen folgenden Vertrag:

1. Allgemeine Bestimmungen und Auftragsgegenstand

1.1 Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragsverarbeiter (Art. 28 DS-GVO) im Rahmen der Nutzung der KI-Kollaborationsplattform aicollab.app. Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Verarbeitung sind Anlage 1 zu entnehmen.

1.2 Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO. Er allein ist für die Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 DS-GVO und die Wahrung der Betroffenenrechte verantwortlich.

1.3 Die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gliedert sich in zwei technisch und rechtlich unterschiedliche Verarbeitungsebenen:

a) Datenspeicherung (stets EU): Sämtliche gespeicherten Daten des Auftraggebers – einschließlich Chatverläufe, hochgeladene Dokumente, Nutzerdaten, Wissensdatenbanken und Projektinhalte – werden ausschließlich auf Servern in Deutschland (Centron.de Rechenzentrum, ISO 27001-zertifiziert) gespeichert und verwaltet. Für die Datenspeicherung gilt unbeschränkt: Verarbeitung im Sinne von Art. 44 ff. DS-GVO findet ausschließlich innerhalb der EU/EWR statt.

b) KI-Modell-Inferenz (abhängig von der Konfiguration): Bei der Verarbeitung von Prompts durch KI-Modelle werden Anfragen und Ausgaben über den KI-Routing-Dienst OpenRouter (openrouter.ai) an die jeweiligen KI-Modell-Anbieter weitergeleitet. Der geografische Ort dieser Verarbeitung sowie der Umfang der Datenweitergabe an Modell-Anbieter hängen von folgenden Einstellungen ab:

i. EU-Modell-Routing AKTIVIERT: Prompts und Ausgaben werden ausschließlich über Microsoft Azure AI Foundry (Standort: Sweden Central, Schweden/EU) als EU-Modell-Endpunkt geroutet. Eine Übertragung in Drittstaaten findet nicht statt. Die Verarbeitung erfolgt innerhalb der EU.

ii. EU-Modell-Routing NICHT aktiviert: Prompts und Ausgaben können über OpenRouter an Modell-Anbieter außerhalb der EU/EWR (z.B. USA) übermittelt werden. Die Übertragung in Drittstaaten erfolgt auf Basis der Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DS-GVO) gemäß den Bedingungen von OpenRouter.

iii. ZDRP (Zero Data Retention Policy) AKTIVIERT: OpenRouter übermittelt alle Anfragen mit dem Parameter 'data_collection: deny' an die Modell-Anbieter. Diese sind dadurch vertraglich verpflichtet, Prompts und Ausgaben weder zu speichern noch für das Training ihrer Modelle zu verwenden (OpenRouter Zero Data Retention). Die ZDRP ist technisch im ZDRP-API-Schlüssel des Auftragsverarbeiters implementiert und erfordert einen entsprechenden Tarif (Pro/Teams/Enterprise).

iv. ZDRP NICHT aktiviert (Free-Tier): Modell-Anbieter können Prompts und Ausgaben gemäß ihren eigenen Nutzungsbedingungen für das Training ihrer Modelle verwenden. Die datenschutz-rechtliche Verantwortung für diese Konfigurationsentscheidung liegt beim Auftraggeber.

Für eine vollständig DSGVO-konforme Nutzung im Rahmen dieses AVV ist der Einsatz der Plattform ausschließlich mit aktiviertem ZDRP und – bei Verarbeitung besonders sensibler Daten – zusätzlich mit EU-Modell-Routing zulässig. Der Auftraggeber trägt die Verantwortung für die entsprechende Konfiguration in seinem Organisations-Account auf aicollab.app.

1.4 Die Vergütung wird außerhalb dieses Vertrags im jeweiligen Hauptvertrag (Nutzungsvertrag / Lizenzvertrag) zwischen den Parteien vereinbart.

2. Vertragslaufzeit und Kündigung

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und endet automatisch mit Beendigung des zugrundeliegenden Hauptvertrags über die Nutzung der Plattform aicollab.app. Er kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung gegenüber dem Auftragsverarbeiter zu. In dieser Rolle kann er insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragsverarbeiter ist verpflichtet, den Weisungen des Auftraggebers Folge zu leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.

3.2 Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragsverarbeiter substantiiert anzweifelt, ist der Auftragsverarbeiter berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.

3.3 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisungen sind auf Verlangen des Auftragsverarbeiters schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragsverarbeiter hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3.4 Der Auftraggeber benennt auf Verlangen des Auftragsverarbeiters eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragsverarbeiter unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen

Umfang zu kontrollieren oder durch Dritte kontrollieren zu lassen. Der Auftragsverarbeiter wird diese Kontrollen dulden und sie im erforderlichen Maße unterstützen. Er wird dem Auftraggeber insbesondere die für die Kontrollen erforderlichen Auskünfte vollständig und wahrheitsgemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme/-systeme gewähren sowie Vorort-Kontrollen ermöglichen. Sofern der Auftraggeber der Verarbeitung der Daten außerhalb der Geschäftsräume zugestimmt hat, hat der Auftragsverarbeiter dafür zu sorgen, dass der Auftraggeber auch diese Räume zu Kontrollzwecken begehen darf.

4.2 Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragsverarbeiters nicht mehr als erforderlich beeinträchtigen. Insbesondere sollen Vorortkontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlauffrist erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.

4.3 Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragsverarbeiters

5.1 Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragsverarbeiter erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig.

5.2 Der Auftragsverarbeiter hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 DS-GVO notwendigen technischen und organisatorischen Maßnahmen implementiert und das nach Art. 30 Abs. 2 DS-GVO erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen.

5.3 Sofern der Auftragsverarbeiter nach der DS-GVO oder sonstigen gesetzlichen Vorschriften zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen in Einklang mit den gesetzlichen Vorschriften ausgewählt hat und sichert dem Auftraggeber zu, diesen unter Angabe seiner Kontaktdaten zu benennen (z.B. per E-Mail). Änderungen über Person und/oder Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber unverzüglich mitzuteilen.

5.4 Die Datenverarbeitung außerhalb der Betriebsstätten des Auftragsverarbeiters oder der Subunternehmer und/oder in Privatwohnungen (z.B. Fernzugriff oder Homeoffice) ist nur mit ausdrücklicher Zustimmung des Auftraggebers gestattet.

5.5 Der Auftragsverarbeiter hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DS-GVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

5.6 Der Auftragsverarbeiter wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

6. Technische und organisatorische Maßnahmen

6.1 Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 2 dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DS-GVO ausgewählt und mit dem Auftraggeber abgestimmt.

6.2 Der Auftragsverarbeiter wird die technischen und organisatorischen Maßnahmen bei Bedarf und/oder anlassbezogen überprüfen und anpassen. Erforderliche Anpassungen werden vom Auftragsverarbeiter dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt. Wesentliche Änderungen, durch die das Schutzniveau verringert werden könnte, sind vorab mit dem Auftraggeber abzustimmen.

7. Unterstützungspflichten des Auftragsverarbeiters

7.1 Der Auftragsverarbeiter wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DS-GVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12–22 DS-GVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.

7.2 Der Auftragsverarbeiter wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DS-GVO bei dessen Pflichten nach Art. 32–36 DS-GVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

8.1 Der Auftragsverarbeiter ist nur mit Zustimmung des Auftraggebers zum Einsatz von Unterauftragsverarbeitern (Subunternehmer) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden Subunternehmerverhältnisse sind diesem Vertrag beigefügt als Anlage 3. Für die in Anlage 3 aufgezählten Subunternehmer gilt die Zustimmung mit Unterzeichnung dieses Vertrags als erteilt. Beabsichtigt der Auftragsverarbeiter den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber in schriftlicher oder elektronischer Form anzeigen, damit dieser deren Einsatz prüfen kann.

8.2 Subunternehmer werden vom Auftragsverarbeiter unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Nebenleistungen, die der Auftragsverarbeiter zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt (z.B. Telekommunikationsleistungen, Post- und Transportdienstleistungen, Wartung und Benutzerservice) stellen keine Unterauftragsverhältnisse dar.

8.3 Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DS-GVO im Betrieb des Subunternehmers.

8.4 Im Vertrag mit dem Subunternehmer ist festzuschreiben, welche Verantwortlichkeiten der Subunternehmer hat, damit der Auftraggeber diese entsprechend überprüfen kann.

8.5 Die Weiterleitung von Daten an den Unterauftragsverarbeiter ist erst zulässig, wenn der Subunternehmer seine Pflichten nach Art. 32 Abs. 4 und 29 DS-GVO gegenüber den ihm unterstellten Personen erfüllt hat.

8.6 Der Auftragsverarbeiter ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Unterauftragsverarbeiter verantwortlich. Er haftet gegenüber dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.

8.7 Der Auftragsverarbeiter hat sich von seinen Unterauftragsverarbeitern bestätigen zu lassen, dass diese – soweit gesetzlich vorgeschrieben – einen Datenschutzbeauftragten benannt haben.

8.8 Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DS-GVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten des Auftragsverarbeiters

9.1 Verstöße gegen diesen Vertrag oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragsverarbeiter selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

9.2 Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 DS-GVO zu unterstützen. Eigenständige Meldungen an Behörden oder Betroffene nach Art. 33 und 34 DS-GVO darf der Auftragsverarbeiter erst nach vorheriger Weisung des Auftraggebers durchführen.

9.3 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragsverarbeiter um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragsverarbeiter die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragsverarbeiter dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.

9.4 Der Auftragsverarbeiter wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen). Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragsverarbeiters in geeigneter Weise zu überprüfen. Die Löschung wird vom Auftragsverarbeiter auf Anfrage schriftlich bestätigt.

11. Datengeheimnis und Vertraulichkeit

11.1 Der Auftragsverarbeiter ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln und einschlägige Geheimnisschutzregeln, denen der Auftraggeber unterliegt (z.B. § 203 StGB), zu beachten.

11.2 Der Auftragsverarbeiter verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragsverarbeiter aufnehmen.

11.3 Der Auftragsverarbeiter wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

12. Schlussbestimmungen

12.1 Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

12.2 Sollte sich die DS-GVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

12.3 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

12.4 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

12.5 Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand für Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist, soweit gesetzlich zulässig, der Sitz des Auftragsverarbeiters.

Unterschriften

Durch ihre nachfolgenden Unterschriften bestätigen die Vertragsparteien, den vorliegenden Auftragsverarbeitungsvertrag gelesen, verstanden und akzeptiert zu haben.

Ort, Datum	Ort, Datum
_____, den _____	_____, den _____
Unterschrift (Auftraggeber)	*Unterschrift (Auftragsverarbeiter / aicollab.app)*

Anlage 1 – Auftragsdetails

Der vorliegende Vertrag umfasst (ggf. im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:

- Bereitstellung und Betrieb der KI-Kollaborationsplattform unter der Domain aicollab.app
- Verarbeitung von Nutzeranfragen (Prompts) und Dokumenten durch KI-Modelle im Rahmen der Plattformnutzung
- Speicherung von Nutzerinhalten, Konversationsverläufen und Projektdaten auf EU-basierten Servern
- Bereitstellung von Kollaborations- und Kommunikationsfunktionen für Teams und Organisationen
- Verwaltung von Nutzerkonten, Zugriffsrechten und Rollenzuweisungen (User Management)
- Generierung und Speicherung von KI-Ausgaben (Texte, Zusammenfassungen, Analysen) auf Basis von Nutzeranfragen
- Bereitstellung technischer Support- und Wartungsleistungen sowie Sicherheitsupdates
- Protokollierung von Nutzungsaktivitäten zur Systemsicherheit und Qualitätssicherung
- Verarbeitung von Zahlungs- und Abrechnungsdaten über externe Zahlungsdienstleister (soweit zutreffend)

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

- Stammdaten der Nutzer: Name, E-Mail-Adresse, Berufsbezeichnung, Abteilung, Profilinformationen
- Authentifizierungsdaten: Nutzername, verschlüsseltes Passwort, API-Schlüssel, Session-Token
- Nutzergenerierte Inhalte: KI-Prompts, Eingabetexte, hochgeladene Dokumente, Chatnachrichten, Kommentare, Projektergebnisse
- KI-Ausgaben: Generierte Texte, Zusammenfassungen, Analysen und sonstige KI-erzeugte Inhalte
- Kommunikationsdaten: Nachrichten und Kommentare innerhalb der Plattform
- Nutzungs- und Protokolldaten: Login-Zeitstempel, Aktivitätslogs, Fehlermeldungen, API-Anfragen
- Technische Daten: IP-Adressen, Browser-Typ, Betriebssystem, Geräte-ID
- Abrechnungsdaten: Rechnungsadresse, Zahlungsreferenzen (keine vollständigen Zahlungsdaten – diese verbleiben beim Zahlungsdienstleister)

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

- Beschäftigte des Auftraggebers (Mitarbeiterinnen und Mitarbeiter, Führungskräfte, Auszubildende)
- Externe Mitarbeiter, Freelancer und Kollaborationspartner des Auftraggebers
- Administratoren und IT-Verantwortliche des Auftraggebers
- Ggf. Kunden oder Kontaktpersonen des Auftraggebers, sofern deren Daten in die Plattform eingegeben werden

Zweck der Datenverarbeitung:

Erbringung der unter diesem Vertrag vereinbarten KI-gestützten Kollaborations- und Analysedienstleistungen im Rahmen der Nutzung der Plattform aicollab.app durch den Auftraggeber und dessen autorisierten Nutzern.

⚠ **Wichtiger Hinweis zur datenschutzkonformen Nutzung (ZDRP + EU-Modell-Routing)**

Datenspeicherung: Alle gespeicherten Daten (Chats, Uploads, Nutzerdaten) verbleiben stets in Deutschland (Centron.de, ISO 27001). Dies gilt ohne Ausnahme und unabhängig von jeder Einstellung.

Für eine vollständig DSGVO-konforme Verarbeitung im Rahmen dieses AVV gilt:

1. ZDRP (Zero Data Retention Policy) – PFLICHT: Muss auf Organisationsebene aktiviert sein. Nur dann übermittelt OpenRouter alle KI-Anfragen mit 'data_collection: deny' an Modell-Anbieter, sodass Prompts und Ausgaben nicht für das Modell-Training verwendet werden. Im Free-Tier (ohne ZDRP) können Modell-Anbieter Daten gemäß ihren AGB für Training nutzen.

2. EU-Modell-Routing – EMPFOHLEN bei sensiblen Daten: Stellt sicher, dass KI-Anfragen ausschließlich über EU-basierte Modell-Endpunkte laufen. Ohne EU-Routing können Prompts über OpenRouter an Anbieter außerhalb der EU/EWR (z.B. USA) übermittelt werden (Grundlage: Standardvertragsklauseln nach Art. 46 DS-GVO).

Ohne aktives ZDRP ist die Nutzung der Plattform im Rahmen dieses AVV nicht zulässig. Der Auftraggeber trägt die Verantwortung für die korrekte Konfiguration.

Konfigurationspfad in aicollab.app: Organisations-Einstellungen → Datenschutz → ZDRP aktivieren & EU-Modell-Routing erzwingen (beide Optionen müssen auf 'Für alle Mitglieder erzwingen' gesetzt sein).

Anlage 2 – Technische und organisatorische Maßnahmen (TOMs) nach Art. 32 DS-GVO

Der Auftragsverarbeiter (aicollab.app) setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DS-GVO festgelegt.

I. Zweckbindung und Trennbarkeit

- ✓ Logische Mandantentrennung (softwareseitig) – strikte Trennung der Kundendaten
- ✓ Berechtigungskonzept mit rollenbasierter Zugriffskontrolle (RBAC)
- ✓ Trennung von Produktiv- und Testsystem
- ✓ Verschlüsselung von Datensätzen zur Verhinderung unberechtigter Zuordnung

II. Vertraulichkeit und Integrität

1. Verschlüsselung

- ✓ Transportverschlüsselung: TLS 1.3 für alle Datenübertragungen zwischen Client und Server
- ✓ Datenverschlüsselung im Ruhezustand (at rest): AES-256-Bit für alle gespeicherten Daten und Datenbankvolumes
- ✓ Ende-zu-Ende-verschlüsselte Kommunikation bei sensiblen Übertragungen

2. Pseudonymisierung

- ✓ Pseudonymisierung von Protokoll- und Analysedaten durch Hashing von IP-Adressen
- Vollständige Pseudonymisierung personenbezogener Daten auf gesonderter Anfrage möglich

3. Zutrittskontrolle (physisch – Rechenzentrum)

- ✓ Automatisches Zugangskontrollsystem beim Rechenzentrumsanbieter (ISO 27001-zertifiziert)
- ✓ Chipkarten-/Transponder-Schließsystem
- ✓ Videoüberwachung der Zugänge
- ✓ Personenkontrolle beim Empfang / Besucherregelung
- ✓ Alarmanlage und Sicherheitsdienst

4. Zugangskontrolle (logisch)

- ✓ Zuordnung von Benutzerrechten und Erstellen von Benutzerprofilen
- ✓ Passwort-Richtlinien (Mindestlänge 12 Zeichen, Komplexitätsanforderungen, regelmäßiger Wechsel)
- ✓ Multi-Faktor-Authentifizierung (MFA/2FA) für alle Administrator-Zugänge
- ✓ Einsatz von Hardware- und Software-Firewall
- ✓ VPN-gesicherter Fernzugriff für administrative Tätigkeiten
- ✓ Automatische Sitzungssperrung nach Inaktivität
- ✓ Verschlüsselung mobiler Datenträger und Notebooks

5. Zugriffskontrolle (Daten)

- ✓ Berechtigungskonzept mit Prinzip der geringsten Rechte (Least Privilege)
- ✓ Verwaltung der Rechte durch Systemadministratoren
- ✓ Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden)

- ✓ Anzahl der Administrator-Zugänge auf das Notwendigste reduziert
- ✓ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei Eingabe, Änderung und Löschung
- ✓ Physische Löschung von Datenträgern vor Wiederverwendung (DIN 66399)

6. Eingabekontrolle

- ✓ Protokollierung der Eingabe, Änderung und Löschung von Daten mit Zeitstempel
- ✓ Nachvollziehbarkeit durch individuelle Benutzernamen (nicht Benutzergruppen)
- ✓ Vergabe von Rechten zur Eingabe, Änderung und Löschung auf Basis des Berechtigungskonzepts

7. Auftragskontrolle (Subunternehmer)

- ✓ Auswahl des Subunternehmers unter Sorgfaltsgesichtspunkten (Datensicherheit)
- ✓ Voherige Prüfung und Dokumentation der beim Subunternehmer getroffenen Sicherheitsmaßnahmen
- ✓ Schriftliche Weisungen an den Subunternehmer (Auftragsverarbeitungsvertrag)
- ✓ Verpflichtung der Mitarbeiter des Subunternehmers auf das Datengeheimnis
- ✓ Wirksame Kontrollrechte gegenüber dem Subunternehmer vereinbart

8. Transport- und Weitergabekontrolle

- ✓ TLS-Verschlüsselung aller Kommunikationswege (HTTPS/TLS 1.3)
- ✓ VPN-Tunnel für interne Kommunikation und administrative Zugänge
- ✓ Keine Übertragung personenbezogener Daten per unverschlüsselter E-Mail
- ✓ Speicherung der Plattformdaten (Konversationsverläufe, Nutzerdaten) auf EU-basierten Servern
- ⚠ KI-Modell-Anfragen (Prompts/Outputs): EU-Verarbeitung NUR bei aktiviertem EU-Modell-Routing auf Organisationsebene – andernfalls mögliche Verarbeitung in Drittstaaten (USA) auf Basis von SCC

9. ZDRP (Zero Data Retention Policy) – KI-Modell-Training

- ✓ ZDRP-Funktion verfügbar: Bei Aktivierung durch den Auftraggeber werden KI-Modell-Anbieter vertraglich verpflichtet, Prompts und Ausgaben nicht für das Training ihrer Modelle zu verwenden
- ✓ ZDRP-Verträge mit EU-fähigen Modell-Anbietern geschlossen (soweit verfügbar)
- ⚠ Ohne ZDRP-Aktivierung durch den Auftraggeber: KI-Modell-Anbieter können Eingaben/Ausgaben gemäß ihren eigenen AGB für Modelltraining verwenden – datenschutzrechtliche Verantwortung liegt beim Auftraggeber für diese Konfigurationsentscheidung
- ✓ ZDRP-Status je Organisation in der Administrationsoberfläche von aicollab.app einsehbar und erzwingbar ('Für alle Mitglieder erzwingen')

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit

- ✓ Erstellen und regelmäßiges Testen eines Backup- und Recovery-Konzepts
- ✓ Automatische tägliche Datensicherung (Backups) auf geografisch verteilten Systemen
- ✓ Überwachung der Systemverfügbarkeit mit automatischen Alarmierungen (Monitoring)
- ✓ Notfallplan (Business Continuity Plan) für kritische Systemausfälle
- ✓ Belastbares Datensicherungs- und Wiederherstellungskonzept
- ✓ Feuer- und Rauchmeldeanlagen sowie Feuerlöschgeräte in Serverräumen (beim Rechenzentrumsbetreiber)
- ✓ Unterbrechungsfreie Stromversorgung (USV) beim Rechenzentrumsbetreiber
- ✓ Serverräume nicht unter sanitären Anlagen und nicht in Hochwassergebieten

IV. Besondere Datenschutzmaßnahmen

- ✓ Datensicherheitskonzept liegt schriftlich vor
- ✓ Risikoanalyse wird regelmäßig durchgeführt
- ✓ Datenschutz-Folgenabschätzung (DSFA) für risikoreiche Verarbeitungen
- ✓ Privacy by Design und Privacy by Default als Grundprinzip der Plattformentwicklung
- ✓ Datenschutz-Leitlinien (Privacy Guardrails) für KI-Verarbeitungen implementiert
- ✓ Regelmäßige Mitarbeiterschulungen zu Datenschutz und Informationssicherheit

V. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von 12 Monaten und anlassbezogen prüfen, evaluieren und bei Bedarf anpassen.

Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

Folgende Subunternehmer sind zum Zeitpunkt des Vertragsschlusses im Einsatz. Mit Unterzeichnung dieses Vertrags gilt der Einsatz dieser Subunternehmer als genehmigt:

Hinweis zur Subunternehmer-Kategorisierung: Subunternehmer der Kategorie A sind stets aktiv. Subunternehmer der Kategorie B (KI-Modell-Anbieter) werden NUR dann für die Verarbeitung personenbezogener Daten tätig, wenn der Auftraggeber ZDRP + EU-Modell-Routing NICHT aktiviert hat; bei aktiviertem EU-Routing werden ausschließlich EU-fähige Endpunkte genutzt.

(Unternehmens-) Name und Anschrift	Beschreibung der Leistung	Ort der Leistungserbringung
KATEGORIE A – Immer aktiv (Plattform-Infrastruktur)		
centron GmbH (centron.de) Heganger 29 D-96103 Hallstadt info@centron.de ISO 27001 zertifiziert	Server-Infrastruktur, Hosting, Datenspeicherung, Netzwerkbetrieb der Plattform aicollab.app in Deutschland. Rechenzentrum Hallstadt/Bamberg, ISO 27001-zertifiziert.	Deutschland (Hallstadt / Bamberg)
Supabase, Inc. (supabase.com) 65 Chulia Street #38-02/03 OCBC Centre Singapore 049513	Datenbankdienst (PostgreSQL): Speicherung von Benutzerdaten, Organisationsdaten, Projektkonfigurationen und Nutzungsdaten. Supabase wird mit europäischem Datenbankstandort betrieben. Grundlage: Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DS-GVO).	EU (Europäische Region)
Cloudflare, Inc. (cloudflare.com) 101 Townsend St San Francisco, CA 94107, USA	CDN (Content Delivery Network), DDoS-Schutz, DNS-Dienste, TLS-Terminierung und Web Application Firewall (WAF) für aicollab.app. Daten werden nur temporär als Transit-Traffic verarbeitet, nicht dauerhaft gespeichert. Grundlage: Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DS-GVO).	USA / Global (SCC gem. Art. 46 DS-GVO)
TecSpace GmbH Süsterfeldstr. 25	Versand transaktionaler E-Mails (Registrierung,	Deutschland / EU

D-52072 Aachen info@tecspace.de HRB 18160, AG Aachen GF: André Matus DSB: datenschutz@tecspace.de	Benachrichtigungen, Passwort-Reset, Rechnungen). Hosted in Deutschland / EU.	
Freemius Inc. (freemius.com) 4023 Kennett Pike Wilmington, DE 19807, USA Merchant of Record (MoR)	Zahlungsabwicklung als Merchant of Record: Rechnungsstellung, Steuern, Zahlungsmanagement (Abonnements, Lizenzen). Freemius handelt als eigenständiger Händler; Grundlage: Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DS-GVO).	USA (SCC gem. Art. 46 DS-GVO)
Stripe, Inc. (stripe.com) 354 Oyster Point Blvd South San Francisco, CA 94080, USA (Zahlungsinfrastruktur via Freemius)	Technische Zahlungsinfrastruktur für Kreditkarten- und Bankzahlungen (wird durch Freemius als MoR eingesetzt). Stripe speichert keine vollständigen Zahlungsdaten des Auftraggebers bei aicollab.app. Grundlage: Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DS-GVO).	USA (SCC gem. Art. 46 DS-GVO)
KATEGORIE B – KI-Modell-Anbieter (abhängig von ZDRP + EU-Routing Konfiguration)		
Microsoft Corporation (Azure AI Foundry) One Microsoft Way Redmond, WA 98052, USA – NUR bei aktiviertem EU-Routing – (Datenverarbeitung: Sweden Central, EU)	EU-Modell-Endpunkt via Azure AI Foundry (Region: Sweden Central). Verarbeitung von KI-Prompts/-Ausgaben ausschließlich in der EU. Azure-Datenschutzzusage: DSGVO-konform. ZDRP: via OpenRouter 'data_collection: deny' – keine Nutzung für Modelltraining.	Schweden / EU (Azure Sweden Central)
OpenRouter, Inc. (openrouter.ai) 169 Madison Avenue New York, NY 10016, USA – NUR ohne EU-Routing (Standard-Modus) –	KI-Modell-Routing an internationale Anbieter (z.B. OpenAI, Anthropic, Google, Meta u.a.) ohne EU-Endpunkte. Mit ZDRP: 'data_collection: deny' – keine Nutzung für Modelltraining. Ohne ZDRP: Modelltraining durch Anbieter möglich. Grundlage: Standardvertragsklauseln (Art.	USA / International (SCC gem. Art. 46 DS-GVO)

	46 Abs. 2 lit. c DS-GVO).	

Hinweis: Der Auftragsverarbeiter informiert den Auftraggeber über geplante Änderungen bezüglich der Hinzuziehung oder des Austauschs von Subunternehmern und gibt dem Auftraggeber damit die Möglichkeit, Einwände gegen solche Änderungen zu erheben.

Stand dieses Vertrags: [Datum eintragen] | Version 1.0
