.tune

AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

gemäß Art. 28 DSGVO

zwischen

(Unternehmen)

(Straße)

(PLZ Stadt)

– nachfolgend „Auftraggeber" oder „Verantwortlicher" –

und

TUNE.eco GmbH

Osterwaldstr. 10

80805 München

– nachfolgend „Auftragnehmer" oder „Auftragsverarbeiter" –

§ 1 Gegenstand und Dauer der Auftragsverarbeitung

(1) Vertragsgegenstand

Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Auftragsverarbeitungsvertrags.

(2) Art der Verarbeitung

Der Auftragnehmer erbringt folgende Verarbeitungstätigkeiten:

- Bereitstellung und Betrieb einer cloudbasierten KI-Plattform
- Verarbeitung von Eingaben (Prompts) der Nutzer des Auftraggebers
- Generierung von Ausgaben (Responses) durch KI-Modelle
- Speicherung von Nutzerdaten und Interaktionshistorie
- Bereitstellung von Analysedaten zur Nutzung der Plattform
- Featurebereitstellung für Automatisierung von Prozess(ketten)
- Technischer Support und Wartung

(3) Zweck der Verarbeitung

Die Verarbeitung erfolgt ausschließlich zum Zweck der Bereitstellung der im Hauptvertrag vereinbarten KI-Plattform und der damit verbundenen Dienstleistungen.

(4) Art der personenbezogenen Daten

Im Rahmen der Nutzung des KI-Produkts können folgende Kategorien personenbezogener Daten verarbeitet werden:

a) Nutzerdaten:

- Namen, E-Mail-Adressen, User-IDs der Nutzer
- IP-Adressen, Gerätekennungen
- Login-Daten und Zeitstempel
- Nutzungspräferenzen

b) Eingabedaten (Prompts):

- Vom Nutzer eingegebene Texte, Dokumente, Fragen
- Hochgeladene Dateien (sofern personenbezogene Daten enthalten)
- Kontextinformationen zu Anfragen

c) Interaktionsdaten:

- Nutzungshistorie, Häufigkeit der Nutzung
- Verlauf von Konversationen
- Feedback und Bewertungen

d) Unternehmensdaten des Auftraggebers:

Die konkreten Kategorien hängen vom Einsatzzweck ab und können nach Entscheidung des Auftraggebers umfassen: Kundendaten, Mitarbeiterdaten, Bewerberdaten, Vertragsdaten, Kommunikationsdaten, Geschäftsdaten, etc.

Hinweis: Die tatsächlich verarbeiteten Kategorien werden durch die Nutzung des Auftraggebers bestimmt. Der Auftraggeber ist dafür verantwortlich, nur solche Daten einzugeben, deren Verarbeitung rechtlich zulässig ist.

(5) Kategorien betroffener Personen

Je nach Nutzung durch den Auftraggeber können betroffen sein:

a) Nutzer der KI-Plattform:

- Mitarbeiter des Auftraggebers
- Externe Dienstleister des Auftraggebers
- Beauftragte Dritte

b) Dritte Personen (sofern in Eingaben genannt oder Daten hochgeladen):

- Kunden des Auftraggebers
- Geschäftspartner, Lieferanten
- Bewerber, Vertragspartner
- Mitarbeiter von Geschäftspartnern
- Sonstige natürliche Personen

Die konkrete Betroffenheit hängt vom Verwendungszweck und den vom Auftraggeber eingegebenen Daten ab.

(6) Dauer der Verarbeitung

Die Verarbeitung erfolgt für die Dauer des Hauptvertrags. Nach Beendigung gelten die Regelungen in § 12 dieses Vertrags.

(7) Datenstandort und Drittlandtransfer

a) Die Datenverarbeitung erfolgt primär auf Servern in Deutschland.

b) Zur Erbringung der Dienstleistung werden personenbezogene Daten an Subauftragsverarbeiter in Drittländern (insbesondere USA) übermittelt. Dies betrifft insbesondere die Nutzung von KI-Modellen der in § 11 und Anlage 1 genannten Anbieter.

c) Für Drittlandübermittlungen werden die EU-Standardvertragsklauseln gemäß Beschluss (EU) 2021/914 der Europäischen Kommission eingesetzt. Zusätzlich werden geeignete Garantien und Schutzmaßnahmen gemäß Art. 46 DSGVO implementiert.

d) Der Auftraggeber stimmt diesen Drittlandübermittlungen im Rahmen der genehmigten Subauftragsverarbeiter (siehe § 11) hiermit zu.

§ 2 Pflichten des Auftraggebers

(1) Verantwortlichkeit

Der Auftraggeber ist alleinverantwortlich für die Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach Art. 12-22 DSGVO.

(2) Rechtmäßigkeit der Verarbeitung

Der Auftraggeber garantiert, dass die Verarbeitung der übermittelten personenbezogenen Daten rechtmäßig ist und eine geeignete Rechtsgrundlage (z.B. Einwilligung, Vertragserfüllung, berechtigtes Interesse) vorliegt.

(3) Weisungsrecht

a) Der Auftraggeber hat das Recht, dem Auftragnehmer Weisungen zur Art und Weise der Datenverarbeitung zu erteilen.

b) Weisungen sind in Textform (z.B. E-Mail) zu erteilen.

c) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn eine Weisung nicht umsetzbar ist oder gegen Datenschutzvorschriften verstößt.

(4) Informationspflichten

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler, Unregelmäßigkeiten oder Verstöße bei der Datenverarbeitung feststellt.

(5) Kontrollrechte

a) Der Auftraggeber ist berechtigt, die Einhaltung der datenschutzrechtlichen Vorschriften beim Auftragnehmer zu kontrollieren.

b) Kontrollen sind nach rechtzeitiger Ankündigung (mindestens 14 Tage) zu den üblichen Geschäftszeiten durchzuführen.

c) Der Auftraggeber kann sich bei Kontrollen durch qualifizierte Dritte (z.B. Auditoren, Datenschutzbeauftragte) vertreten lassen.

§ 3 Pflichten des Auftragnehmers

(1) Weisungsgebundenheit

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der dokumentierten Weisungen des Auftraggebers, sofern er nicht durch EU-Recht oder Recht der Mitgliedstaaten zu einer Verarbeitung verpflichtet ist (Art. 28 Abs. 3 lit. a DSGVO). In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht verbietet.

(2) Zweckbindung

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten ausschließlich für die in § 1 genannten Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt, es sei denn, sie sind zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder Datensicherung erforderlich.

(3) Nutzung anonymisierter Daten

Der Auftragnehmer und seine Subauftragsverarbeiter dürfen die verarbeiteten personenbezogenen Daten NICHT verwenden für:

a) Training, Verbesserung oder Weiterentwicklung von KI-Modellen

b) Weitergabe an Dritte außerhalb der genehmigten Subauftragsverarbeiter

c) Eine Nutzung vollständig anonymisierter, technisch nicht reversibler Betriebs- und Leistungsdaten (z. B. Latenzen, Fehlerraten, Tokenverbrauch), die keinen Rückschluss auf betroffene Personen ermöglichen, ist zulässig, sofern diese der Verbesserung von Stabilität und Sicherheit der Plattform dient.

(4) Vertraulichkeit

a) Der Auftragnehmer verpflichtet alle mit der Verarbeitung betrauten Personen zur Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b DSGVO bzw. stellt sicher, dass diese einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

b) Diese Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

(5) Datensicherheit

Der Auftragnehmer gewährleistet die in § 8 und Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen.

(6) Unterstützung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber angemessen bei:

- der Beantwortung von Auskunftsersuchen betroffener Personen (Art. 15 DSGVO)
- der Wahrnehmung von Betroffenenrechten (Art. 16-22 DSGVO)
- der Meldung von Datenschutzverletzungen (Art. 33-34 DSGVO)
- Datenschutz-Folgenabschätzungen (Art. 35 DSGVO)
- vorherigen Konsultationen mit Aufsichtsbehörden (Art. 36 DSGVO)

Soweit die Unterstützung einen erheblichen Mehraufwand verursacht, kann der Auftragnehmer eine angemessene Vergütung verlangen.

§ 4 Betroffenenrechte

(1) Verantwortlichkeit

Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

(2) Weiterleitung von Anfragen

Der Auftragnehmer leitet Anfragen betroffener Personen, die erkennbar an den Auftraggeber gerichtet sind, unverzüglich an diesen weiter.

(3) Unterstützung

Soweit der Auftraggeber die Mitwirkung des Auftragnehmers zur Wahrung von Betroffenenrechten benötigt (z.B. Auskunft, Löschung, Datenübertragbarkeit), unterstützt der Auftragnehmer den Auftraggeber angemessen. Die Modalitäten und ggf. anfallende Vergütungen werden gesondert vereinbart.

§ 5 Datenschutzkoordination

Der Auftragnehmer benennt eine zentrale Kontaktstelle für datenschutzbezogene Anfragen des Auftraggebers, welche diese innerhalb angemessener Fristen beantwortet.

Kontakt:

DataCo GmbH

Sandstraße 33

80335 München, Deutschland

privacy@dataguard.com

§ 6 Meldung von Datenschutzverletzungen

(1) Meldepflicht

Der Auftragnehmer meldet dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch binnen 24 Stunden nach Kenntniserlangung.

(2) Inhalt der Meldung

Die Erstmeldung enthält alle zu diesem Zeitpunkt verfügbaren Informationen.

Weitergehende Angaben werden im Rahmen fortlaufender Untersuchungen in Folgeberichten nachgereicht, sobald diese verfügbar sind, insbesondere:

- Beschreibung der Art der Verletzung
- Betroffene Kategorien und ungefähre Anzahl betroffener Personen
- Betroffene Kategorien und ungefähre Anzahl betroffener Datensätze
- Wahrscheinliche Folgen der Verletzung
- Ergriffene oder vorgeschlagene Maßnahmen zur Behebung
- Kontaktdaten für weitere Informationen

(3) Unterstützung

Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Pflichten nach Art. 33 und 34 DSGVO (Meldung an die Aufsichtsbehörde bzw. Benachrichtigung Betroffener).

(4) Dokumentation

Der Auftragnehmer dokumentiert alle Datenschutzverletzungen, einschließlich der Umstände, der Auswirkungen und der ergriffenen Abhilfemaßnahmen.

§ 7 Kontroll- und Prüfungsrechte

(1) Kontrollrechte

Der Auftraggeber hat das Recht, die Einhaltung der Datenschutzvorschriften und dieses Vertrags beim Auftragnehmer zu kontrollieren.

(2) Durchführung

a) Kontrollen sind nach rechtzeitiger Ankündigung (mindestens 14 Tage) zu den üblichen Geschäftszeiten durchzuführen.

b) Der Auftraggeber kann sich durch qualifizierte Dritte (z.B. Wirtschaftsprüfer, Datenschutzbeauftragte) vertreten lassen, die zur Verschwiegenheit verpflichtet sind.

c) Kontrollen sind so durchzuführen, dass der Geschäftsbetrieb des Auftragnehmers nicht mehr als erforderlich beeinträchtigt wird.

(3) Informationspflichten

Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung seiner Pflichten zur Verfügung.

(4) Alternative: Audit-Berichte

Anstelle eigener Kontrollen kann der Auftraggeber aktuelle Audit-Berichte, Zertifizierungen oder Testberichte unabhängiger Prüfer akzeptieren (z.B. ISO 27001, SOC 2).

§ 8 Technische und organisatorische Maßnahmen (TOMs)

(1) Schutzniveau

Der Auftragnehmer gewährleistet ein dem Risiko angemessenes Schutzniveau gemäß Art. 32 DSGVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung.

(2) Konkrete Maßnahmen

Die aktuell implementierten technischen und organisatorischen Maßnahmen sind in Anlage 2 detailliert beschrieben.

(3) Anpassung

Der Auftragnehmer ist berechtigt, Maßnahmen durch funktional gleichwertige oder bessere Sicherheitsmaßnahmen zu ersetzen oder anzupassen, sofern das vereinbarte Schutzniveau nicht abgesenkt wird.

(4) Abstimmung

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren werden zwischen Auftragnehmer und Auftraggeber abgestimmt.

(5) Benachrichtigung

Soweit die getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

§ 9 Laufzeit und Kündigung

(1) Laufzeit

Dieser Auftragsverarbeitungsvertrag gilt für die Dauer des Hauptvertrags zwischen den Parteien.

(2) Ordentliche Kündigung

Der AVV endet automatisch mit Beendigung des Hauptvertrags.

(3) Außerordentliche Kündigung

Der Auftraggeber kann diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn:

- ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzbestimmungen vorliegt
- der Auftragnehmer eine rechtmäßige Weisung nicht ausführen kann oder will
- der Auftragnehmer Kontrollrechte vertragswidrig verweigert
- der Auftragnehmer gegen wesentliche Pflichten aus diesem Vertrag verstößt

§ 10 Haftung

(1) Gesetzliche Haftung

Die Haftung richtet sich nach den gesetzlichen Bestimmungen, insbesondere Art. 82 DSGVO.

(2) Haftungsbeschränkung

Für leichte Fahrlässigkeit haftet der Auftragnehmer nur bei Verletzung wesentlicher Vertragspflichten (Kardinalpflichten), beschränkt auf den typischerweise vorhersehbaren Schaden.

(3) Ausschlüsse

Eine Haftung für mittelbare Schäden, Folgeschäden oder entgangenen Gewinn ist ausgeschlossen, soweit gesetzlich zulässig.

(4) Schadensminderung

Beide Parteien verpflichten sich, zur Vermeidung und Minderung von Schäden beizutragen.

§ 11 Subauftragsverarbeiter

(1) Allgemeine Genehmigung

Der Auftraggeber erteilt hiermit seine allgemeine Genehmigung zur Beauftragung der in Anlage 1 genannten Subauftragsverarbeiter. Der Auftragnehmer darf diese zur Erbringung der vertraglich vereinbarten Leistungen einsetzen.

(2) Genehmigte Subauftragsverarbeiter

Die zum Zeitpunkt des Vertragsschlusses genehmigten Subauftragsverarbeiter sind in Anlage 1 (Genehmigte Subauftragsverarbeiter) vollständig aufgeführt.

(3) Pflichten gegenüber Subauftragsverarbeitern

a) Der Auftragnehmer stellt sicher, dass mit allen Subauftragsverarbeitern Verträge gemäß Art. 28 DSGVO geschlossen werden.

b) Diese Verträge enthalten mindestens die gleichen Datenschutzpflichten wie dieser AVV.

c) Der Auftragnehmer bleibt gegenüber dem Auftraggeber vollumfänglich verantwortlich für die Erfüllung der Pflichten des Subauftragsverarbeiters.

(4) Änderungen bei Subauftragsverarbeitern

a) Der Auftragnehmer informiert den Auftraggeber mindestens 30 Kalendertage im Voraus über geplante Änderungen (Hinzufügung oder Ersetzung von Subauftragsverarbeitern) per E-Mail.

b) Die Mitteilung enthält:

- Name und Anschrift des Subauftragsverarbeiters
- Art der übertragenen Verarbeitungstätigkeiten
- Datenstandort
- Rechtsgrundlage bei Drittlandübermittlungen

c) Der Auftraggeber kann binnen 14 Kalendertagen nach Zugang der Mitteilung schriftlich (Textform ausreichend) widersprechen, wenn berechtigte datenschutzrechtliche Bedenken bestehen.

d) Bei fristgerechtem Widerspruch hat der Auftragnehmer folgende Optionen:

- Verzicht auf den neuen Subauftragsverarbeiter, oder
- Einräumung eines außerordentlichen Kündigungsrechts für den Auftraggeber mit einer Frist von 30 Kalendertagen

(5) Drittlandübermittlungen

a) Die Übermittlung personenbezogener Daten an Subauftragsverarbeiter in Drittländern (insbesondere USA) erfolgt nur, soweit dies für die Erbringung der vertraglich vereinbarten Leistungen erforderlich ist und eine geeignete Übermittlungsgrundlage gemäß Art. 44 ff. DSGVO besteht.

b) Der Auftragnehmer bewertet Drittlandsübermittlungen risikobasiert und führt, soweit erforderlich, ein Transfer Impact Assessment (TIA) durch. Falls nötig, ergreift der Auftragnehmer zusätzliche technische oder organisatorische Schutzmaßnahmen.

c) Der Auftragnehmer informiert den Auftraggeber auf Anfrage über die wesentlichen Inhalte der eingesetzten Schutzmaßnahmen und die Ergebnisse des TIA. Die Vorlage vollständiger Detailunterlagen oder vertraulicher Dokumente von Subauftragsverarbeitern ist nicht erforderlich.

(6) Verbot des Model-Trainings

Der Auftragnehmer verpflichtet Subauftragsverarbeiter, personenbezogene Daten ausschließlich für die vereinbarten Zwecke zu verarbeiten und diese nicht für Training, Fine-Tuning oder Modellverbesserungen zu verwenden. Die Sicherstellung erfolgt auf Grundlage der jeweils gültigen Vertragsbedingungen oder offiziellen Policies der Subauftragsverarbeiter. Der Auftragnehmer haftet nicht für Verstöße von Subauftragsverarbeitern.

§ 12 Datenrückgabe und Löschung nach Vertragsende

(1) Datenexport

Auf Verlangen des Auftraggebers stellt der Auftragnehmer binnen 14 Kalendertagen nach Vertragsende sämtliche vom Auftraggeber bereitgestellten oder im Rahmen der Verarbeitung entstandenen Daten in einem gängigen, maschinenlesbaren Format (z.B. JSON, CSV, Excel) zur Verfügung.

(2) Löschfrist

a) Der Auftragnehmer löscht sämtliche personenbezogenen Daten des Auftraggebers spätestens 30 Kalendertage nach Vertragsende vollständig und unwiederbringlich.

b) Dies umfasst:

- Alle Eingaben (Prompts) und Ausgaben (Responses)
- Nutzerdaten, Benutzerkonten und Zugangsdaten
- Interaktionshistorien, Chat-Verläufe und Logs
- Alle Kopien, Sicherungskopien und Backups

(3) Subauftragsverarbeiter

Der Auftragnehmer stellt sicher, dass auch alle Subauftragsverarbeiter die Daten gemäß Absatz 2 löschen und bestätigt dies auf Anfrage.

(4) Ausnahmen

a) Soweit gesetzliche Aufbewahrungspflichten (z.B. Steuerrecht, Handelsrecht) oder berechtigte Interessen zur Rechtsverteidigung bestehen, dürfen Daten länger aufbewahrt werden.

b) In diesem Fall:

- informiert der Auftragnehmer den Auftraggeber unverzüglich
- werden die Daten gesperrt und nur für den Aufbewahrungszweck verwendet
- erfolgt die Löschung unverzüglich nach Wegfall des Aufbewahrungsgrunds

(5) Löschbestätigung

Auf Anfrage bestätigt der Auftragnehmer die vollständige Löschung schriftlich binnen 14 Tagen nach erfolgter Löschung.

§ 13 Schlussbestimmungen

(1) Salvatorische Klausel

Sollte eine Bestimmung dieses Vertrags ganz oder teilweise unwirksam oder undurchführbar sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck der ursprünglichen Regelung am nächsten kommt.

(2) Insolvenz und Gefährdung

Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (z.B. Pfändung, Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, informiert der Auftragnehmer den Auftraggeber unverzüglich.

(3) Vertraulichkeit

a) Beide Parteien verpflichten sich, alle im Zusammenhang mit diesem Vertrag erlangten Informationen vertraulich zu behandeln und nur zur Durchführung des Vertrags zu verwenden.

b) Diese Verpflichtung besteht auch nach Beendigung des Vertrags fort.

c) Ausgenommen sind Informationen, die:

- öffentlich bekannt sind oder werden
- dem Empfänger bereits zuvor bekannt waren
- von Dritten rechtmäßig offengelegt wurden
- aufgrund gesetzlicher Verpflichtungen offengelegt werden müssen

(4) Schriftform

Nebenabreden, Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für die Änderung dieser Schriftformklausel. Ausnahme: Weisungen gemäß § 2 Abs. 3 können in Textform erteilt werden.

(5) Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts im Sinne von § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(6) Sprachfassung

Die Vertragsparteien können diesen Vertrag übersetzen. Maßgeblich ist jedoch stets die deutsche Originalfassung.

(7) Rangfolge

Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag geht der AVV in datenschutzrechtlichen Fragen vor.

_____, den _____ München, den _____

_____ _____

Unterschrift Auftraggeber **Unterschrift TUNE.eco GmbH**

Anlagen:

- Anlage 1: Genehmigte Subauftragsverarbeiter
- Anlage 2: Technische und organisatorische Maßnahmen (TOMs)

.tune

ANLAGE 1

Genehmigte Subauftragsverarbeiter

Im Rahmen der Erbringung der Dienstleistungen gemäß Hauptvertrag setzt TUNE.eco GmbH folgende Subauftragsverarbeiter ein:

1. KI-MODELL-ANBIETER

1.1 OpenAI Ireland Ltd.

Leistung: Bereitstellung von Large Language Models (GPT-4, GPT-3.5, o1, etc.)

Datenstandort: USA / EU

Rechtsgrundlage Drittland zwischen OpenAI Ireland Ltd und **OpenAI OpCo, LLC**: EU-Standardvertragsklauseln (SCC) gemäß Beschluss (EU) 2021/914

Besonderheiten: OpenAI garantiert vertraglich, dass Kundendaten nicht für Model-Training verwendet werden (siehe OpenAI Business Terms, API Data Usage Policies)

1.2 Anthropic PBC

Leistung: Bereitstellung von Large Language Models (Claude 3.5, Claude 4, etc.)

Datenstandort: USA

Rechtsgrundlage Drittland: EU-Standardvertragsklauseln (SCC) gemäß Beschluss (EU) 2021/914

Besonderheiten: Anthropic garantiert vertraglich, dass Kundendaten nicht für Model-Training verwendet werden

1.3 Google Cloud EMEA Limited

Leistung: Bereitstellung von Large Language Models (Gemini, PaLM, etc.)

Datenstandort: USA / EU

Rechtsgrundlage Drittland zwischen Google Cloud EMEA Limited und Google LLC: Angemessenheitsbeschluss Data Privacy Framework

Besonderheiten: Google Cloud AI garantiert vertraglich, dass Kundendaten nicht für Model-Training verwendet werden (siehe Google Cloud AI/ML Products Terms)

2. INFRASTRUKTUR-ANBIETER

2.1 Hetzner Online GmbH

Anschrift:Industriestr. 25, 91710 Gunzenhausen

Leistung: Bereitstellung von Server-Infrastruktur, Datenbanken, Storage

Datenstandort: Deutschland / EU

Rechtsgrundlage: Verarbeitung innerhalb EU/EWR, Art. 28 DSGVO

Besonderheiten: ISO 27001 zertifiziert

3. WEITERE SUBAUFTRAGSVERARBEITER

3.1 E-Mail-Versand & Workspace

3.1.1. Google LLC

Anschrift: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Leistung: Workspace, Mail Postfächer

Datenstandort: USA / EU

Rechtsgrundlage Drittland: EU-Standardvertragsklauseln (SCC) gemäß Beschluss (EU) 2021/914

3.2 Entwicklungspartner

3.2.1 Futurebrains

Anschrift: Weberstraße 9, 76133 Karlsruhe, Deutschland

3.2.2 SolveIT

Anschrift: Przasnyska Street nr 6, lok. 65, 01-756 Warsaw, Poland

3.2.3 EUVIC

Anschrift: Gliwice at ul. Przewozowa 32, 44-100 Gliwice, Poland

WICHTIGE HINWEISE:

1. Änderungen

TUNE.eco GmbH behält sich vor, weitere Subauftragsverarbeiter hinzuzuziehen oder bestehende zu ersetzen. Änderungen werden dem Auftraggeber gemäß § 11 Abs. 4 des AVV mindestens 30 Tage im Voraus mitgeteilt.

2. Aktualität

Diese Liste wird regelmäßig aktualisiert. Die jeweils aktuelle Fassung kann beim Datenschutzbeauftragten angefordert werden.

3. Widerspruchsrecht

Der Auftraggeber kann gegen die Beauftragung neuer Subauftragsverarbeiter binnen 14 Tagen nach Mitteilung widersprechen (siehe § 11 Abs. 4 AVV).

4. Verträge

Mit allen genannten Subauftragsverarbeitern wurden Verträge gemäß Art. 28 DSGVO geschlossen. Bei Drittlandübermittlungen wurden EU-Standardvertragsklauseln vereinbart und Transfer Impact Assessments durchgeführt.

Stand dieser Anlage: Mai 2026

Diese Anlage ist Bestandteil des Auftragsverarbeitungsvertrags zwischen TUNE.eco GmbH und dem Auftraggeber.

.tune

ANLAGE 2

Technische und organisatorische Maßnahmen (TOMs) gemäß Art. 32 DSGVO

PRÄAMBEL

Die TUNE.eco GmbH hat technische und organisatorische Maßnahmen implementiert, um ein dem Risiko angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten. Die Maßnahmen berücksichtigen den Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung.

Stand:	März 2026
Nächste Prüfung:	September 2026
ISO 27001:	In Vorbereitung mit DataGuard, Audit geplant Ende Mai 2026

Die TUNE.eco GmbH ist eine vollständig remote arbeitende Organisation (Remote-First) und betreibt eine cloudbasierte SaaS-Plattform. Die nachfolgenden Maßnahmen beschreiben den tatsächlichen IST-Stand der technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten.

Dieses Dokument unterscheidet transparent zwischen implementierten, in Umsetzung befindlichen, geplanten und offenen Maßnahmen.

1. ZUTRITTSKONTROLLE

1.1 Physische Sicherheit der Infrastruktur

TUNE betreibt keine eigenen Server. Das Hosting erfolgt bei Hetzner (DE). Physische Sicherheitsmaßnahmen werden durch den Hosting-Provider gewährleistet:

Maßnahme	Details / IST-Stand	Status
Rechenzentrum	Hetzner, Deutschland – ISO 27001 zertifiziert	IMPLEMENTIERT
Physischer Zugang	Über Hetzner: Badge-Systeme, Videoüberwachung, 24/7 Security	IMPLEMENTIERT
Redundanz	Redundante Stromversorgung und Klimatisierung durch Provider	IMPLEMENTIERT

1.2 Remote-Work-Sicherheit

TUNE ist eine Remote-First-Organisation ohne eigene Büroräume. Für die Verarbeitung personenbezogener Daten gelten folgende Regelungen:

Maßnahme	Details / IST-Stand	Status
Home-Office-Pflicht	Personenbezogene Daten dürfen ausschließlich im Home Office verarbeitet werden	IMPLEMENTIERT

Verbot öffentl. Bereiche	Keine Datenverarbeitung in Cafés, Co-Working-Spaces, öffentl. Verkehrsmitteln	IMPLEMENTIERT
Clean-Desk-Policy	in Home-Office.Richtlinie enthalten	IMPLEMENTIERT
Home-Office-Richtlinie	Schriftliche Richtlinie für alle Mitarbeiter	IMPLEMENTIERT

2. ZUGANGSKONTROLLE

2.1 Authentifizierung

Maßnahme	Details / IST-Stand	Status
MFA/2FA	Auf den Admin-Zugängen aktiv	IMPLEMENTIERT
Passwort-Manager	heylogin im Einsatz für das gesamte Team	IMPLEMENTIERT
Passwort-Richtlinie	Mind. 12 Zeichen, Komplexität – durchgesetzt via heylogin	IMPLEMENTIERT
SSO	Google Workspace SSO für interne Anwendungen	IMPLEMENTIERT

2.2 Berechtigungsverwaltung

Maßnahme	Details / IST-Stand	Status
RBAC	Rollenbasierte Zugriffskontrolle in .tune Plattform	IMPLEMENTIERT
Least Privilege	wird umgesetzt und gepflegt	IMPLEMENTIERT
Berechtigungs-Review	regelmäßiges dokumentierter Review	IMPLEMENTIERT

2.3 Endpoint Security

Maßnahme	Details / IST-Stand	Status
MDM	Miradore wird aktuell ausgerollt	IMPLEMENTIERT
Bildschirmsperre	Automatische Sperre konfiguriert auf verwalteten Geräten	IMPLEMENTIERT
Privacy Screens	Beschafft und an Mitarbeiter zur Nutzung übergeben	IMPLEMENTIERT
Remote Wipe	Miradore-Rollout verfügbar	IMPLEMENTIERT

3. ZUGRIFFSKONTROLLE

3.1 Datenverschlüsselung

Maßnahme	Details / IST-Stand	Status
Daten in Transit	TLS 1.2+ für alle Verbindungen (HTTPS)	IMPLEMENTIERT
Daten at Rest	Verschlüsselung über Hetzner (serverseitig)	IMPLEMENTIERT
Backups	Verschlüsselte Backups	IMPLEMENTIERT

3.2 Mandantentrennung

Maßnahme	Details / IST-Stand	Status
Multi-Tenancy	Logische Trennung der Kundendaten auf Applikationsebene	IMPLEMENTIERT
Datenisolierung	Separate Tenant-IDs, keine Vermischung von Kundendaten	IMPLEMENTIERT

3.3 Netzwerk- und Logging

Maßnahme	Details / IST-Stand	Status
Firewall	Firewall-Konfiguration über Hetzner	IMPLEMENTIERT
DDoS-Schutz	Über Hetzner Cloud-Infrastruktur	IMPLEMENTIERT
Zugriffsprotokolle	Logging-Service in .tune Plattform integriert (kein SIEM)	IMPLEMENTIERT
Log-Aufbewahrung	Logs werden aufbewahrt, Aufbewahrungsdauer zu formalisieren	IN UMSETZUNG
SIEM / IDS/IPS	aktuelles Monitoring vorhanden, SIEM Erweiterung wird aktuell auf Notwendigkeit geprüft	IMPLEMENTIERT

4. WEITERGABEKONTROLLE

Maßnahme	Details / IST-Stand	Status
Verschlüsselte Übertragung	TLS für alle API-Kommunikation und Datenübertragungen	IMPLEMENTIERT
AVV mit Subunternehmern	Auftragsverarbeitungsverträge mit Hosting- und KI-Anbietern	IMPLEMENTIERT
Kein Model-Training	Vertragliche Garantie: Kundendaten werden nicht für KI-Training genutzt	IMPLEMENTIERT
EU-SCCs / TIA	Standardvertragsklauseln für US-Anbieter, Transfer Impact Assessments	IMPLEMENTIERT
Verschlüsselte Komm.	Interne Kommunikation über verschlüsselte Tools (Google Workspace)	IMPLEMENTIERT

5. EINGABEKONTROLLE

Maßnahme	Details / IST-Stand	Status
Audit-Logging	Logging von Systemzugriffen und Datenänderungen in .tune	IMPLEMENTIERT
Versionskontrolle	Git-basierte Versionskontrolle für alle Code-Änderungen	IMPLEMENTIERT
Code-Review	Peer-Review für Code-Änderungen (4-Augen-Prinzip)	IMPLEMENTIERT
Change Management	Aufgebaut und Umgesetzt	IMPLEMENTIERT

6. AUFTRAGSKONTROLLE

6.1 Vertragliche Regelungen

Maßnahme	Details / IST-Stand	Status
AVV	Standardisierter Auftragsverarbeitungsvertrag mit Auftraggebern	IMPLEMENTIERT
Weisungsdokumentation	Dokumentierte Weisungen zur Datenverarbeitung	IMPLEMENTIERT
Zweckbindung	Verbot der Nutzung von Kundendaten zu eigenen Zwecken	IMPLEMENTIERT

6.2 Schulung und Vertraulichkeit

Maßnahme	Details / IST-Stand	Status
Datenschutz-Schulung	jährliche Schulung wird mit Partner DataGuard durchgeführt und dokumentiert	IMPLEMENTIERT
Vertraulichkeitserklg.	Schriftliche Verpflichtung der Mitarbeiter auf Vertraulichkeit	IMPLEMENTIERT
NDAs	NDAs mit externen Dienstleistern	IMPLEMENTIERT

7. TRENNUNGSGEBOT

Maßnahme	Details / IST-Stand	Status
Mandantentrennung	Logische Trennung auf Datenbankebene	IMPLEMENTIERT
Umgebungstrennung	Separate Entwicklungs- und Produktionsumgebungen	IMPLEMENTIERT
Kein KI-Training	Vertragliche Garantie: Kein Training von KI-Modellen mit Kundendaten	IMPLEMENTIERT
Datenminimierung	Privacy by Design als Prinzip im System-Design	IMPLEMENTIERT

Löschkonzept	Löschkonzept liegt zur Freigabe vor & wird in den laufenden Prozess eingebunden	IMPLEMENTIERT

8. DATENSCHUTZ-MANAGEMENT

Maßnahme	Details / IST-Stand	Status
Ext. DSB	DataGuard als externer Datenschutzbeauftragter beauftragt	IMPLEMENTIERT
VVT (Art. 30)	Verzeichnis der Verarbeitungstätigkeiten veröffentlicht	IMPLEMENTIERT
DSFA	Formaler Prozess für Datenschutz-Folgenabschätzungen entsteht aktuell	IMPLEMENTIERT
Datenschutz-Richtlinien	Incident Response Policy, Data Retention Policy, Home-Office-Richtlinie	IMPLEMENTIERT

9. INCIDENT RESPONSE

Maßnahme	Details / IST-Stand	Status
Meldeprozess	Bekannt: 24h an Auftraggeber, 72h an Aufsichtsbehörde	IMPLEMENTIERT
IR-Verantwortliche	CTO übernimmt Incident Management, GF die Kommunikation (kein dediziertes IR-Team)	IMPLEMENTIERT
Incident-Dokumentation	Incident Dokumentation wird in der Plattform geführt	IMPLEMENTIERT

10. ENTWICKLUNG UND BETRIEB

Maßnahme	Details / IST-Stand	Status
Secure Coding	OWASP Top 10 als Orientierung, Security by Design als Prinzip	IMPLEMENTIERT
Code Reviews	4-Augen-Prinzip für Code-Änderungen	IMPLEMENTIERT
Penetration Test	Erster externer Penetration Test läuft aktuell (Q1 2026)	IMPLEMENTIERT
Dependency Scanning	Prüfung auf bekannte Schwachstellen in Abhängigkeiten	IMPLEMENTIERT
Patch Management	Updates werden eingespielt	IMPLEMENTIERT

11. ZERTIFIZIERUNGEN UND NACHWEISE

Maßnahme	Details / IST-Stand	Status
Hetzner	ISO 27001, SOC 2 Type II	IMPLEMENTIERT
ISO 27001 (TUNE)	In Vorbereitung mit DataGuard, Audit geplant Ende Mai 2026	IN UMSETZUNG

ÄNDERUNGEN UND AKTUALISIERUNG

Diese technischen und organisatorischen Maßnahmen werden halbjährlich überprüft und an den Stand der Technik angepasst. Das Schutzniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen werden mit dem Auftraggeber abgestimmt und dokumentiert.

Diese Anlage ist Bestandteil des Auftragsverarbeitungsvertrags zwischen TUNE.eco GmbH und dem Auftraggeber.