Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

gemäß Art. 28 DSGVO

Fassung 1.0 — gültig ab 2. August 2026

Zwischen

dem Kunden, wie im Hauptvertrag benannt

— nachfolgend **„Verantwortlicher"** —

und

Christian Fischer
Häuslhofstraße 28
5710 Kaprun
Österreich

handelnd unter der Geschäftsbezeichnung **„algonice"**
UID-Nummer: **ATU81765289**
E-Mail: support@algonice.eu

— nachfolgend **„Auftragsverarbeiter"** —

— gemeinsam die **„Parteien"** —

Präambel

Der Auftragsverarbeiter stellt dem Verantwortlichen den KI-Arbeitsplatz „algonice mit Ody" als Software-Dienst zur Verfügung (nachfolgend der **„Dienst"**). Der Verantwortliche und die von ihm berechtigten Personen geben dabei Inhalte in den Dienst ein, die personenbezogene Daten enthalten können.

Dieser Vertrag konkretisiert die Pflichten der Parteien nach Art. 28 DSGVO. Er gilt für jede Verarbeitung personenbezogener Daten, die der Auftragsverarbeiter im Rahmen der Bereitstellung des Dienstes für den Verantwortlichen vornimmt — **unabhängig davon, über welchen Vertriebsweg oder über welche Vermittlungsplattform der Dienst bezogen wurde**. Er wird mit Aufnahme der Nutzung wirksam; **eine gesonderte Unterzeichnung ist nicht erforderlich** (Art. 28 Abs. 9 DSGVO: Textform genügt).

Der Auftragsverarbeiter macht diesen Vertragstext dem Verantwortlichen **im Bestellvorgang sowie dauerhaft in der Anwendung und auf der Website zugänglich**, sodass er ihn vor Aufnahme der Nutzung zur Kenntnis nehmen, speichern und ausdrucken kann.

Soweit zwischen den Parteien weitere Vereinbarungen bestehen, geht dieser Vertrag ihnen in Fragen des Datenschutzes vor.

§ 1 Begriffsbestimmungen

1. Die Begriffe **„personenbezogene Daten"**, **„Verarbeitung"**, **„Verantwortlicher"**, **„Auftragsverarbeiter"**, **„betroffene Person"**, **„Aufsichtsbehörde"** und **„Verletzung des Schutzes personenbezogener Daten"** haben die Bedeutung, die ihnen Art. 4 DSGVO gibt.

2. **„Kundendaten"** sind alle personenbezogenen Daten, die der Auftragsverarbeiter im Rahmen der Erbringung des Dienstes im Auftrag des Verantwortlichen verarbeitet. Einzelheiten regelt **Anlage 1**.

3. **„Hauptvertrag"** ist die zwischen den Parteien bestehende Vereinbarung über die Nutzung des Dienstes, unabhängig von ihrer Bezeichnung und vom Vertriebsweg.

4. **„Unterauftragsverarbeiter"** ist jeder Dritte, den der Auftragsverarbeiter mit der Verarbeitung von Kundendaten betraut.

5. **„DSGVO"** ist die Verordnung (EU) 2016/679.

§ 2 Rollen und Verantwortlichkeiten

1. Der **Verantwortliche** bestimmt Zwecke und Mittel der Verarbeitung der Kundendaten. Er ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für das Vorliegen einer Rechtsgrundlage und für die Erfüllung der Informationspflichten gegenüber den betroffenen Personen.

2. Der **Auftragsverarbeiter** verarbeitet Kundendaten ausschließlich auf dokumentierte Weisung des Verantwortlichen und nur zu den in **Anlage 1** genannten Zwecken. Eine Verarbeitung zu eigenen Zwecken findet nicht statt. **Der Auftragsverarbeiter verwendet Kundendaten nicht zum Training von KI-Modellen und gibt sie zu diesem Zweck auch nicht weiter.**

3. Die **Nutzung des Dienstes durch den Verantwortlichen gilt als Weisung** im Sinne des Art. 28 Abs. 3 lit. a DSGVO. Darüber hinausgehende Einzelweisungen sind in Textform an support@algonice.eu zu richten. Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, können einer gesonderten Vergütung bedürfen.

4. Hält der Auftragsverarbeiter eine Weisung für **datenschutzrechtlich unzulässig**, teilt er dies dem Verantwortlichen unverzüglich mit. Er ist berechtigt, die Ausführung bis zur Bestätigung oder Änderung der Weisung auszusetzen (Art. 28 Abs. 3 S. 3 DSGVO).

5. Der Verantwortliche stellt sicher, dass er **keine besonderen Kategorien personenbezogener Daten** im Sinne des Art. 9 DSGVO und keine Daten über strafrechtliche Verurteilungen (Art. 10 DSGVO) in den Dienst eingibt, es sei denn, er hat die dafür erforderliche Rechtsgrundlage geschaffen und den Auftragsverarbeiter zuvor darüber informiert. Der Dienst ist für die Verarbeitung solcher Daten nicht besonders ausgelegt.

6. Der Verantwortliche verwaltet die **Benutzerkonten seiner Instanz selbst** und entscheidet, welchen Personen er Zugang gewährt.

§ 3 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich:

1. **Weisungsbindung** — Kundendaten nur gemäß § 2 zu verarbeiten und sie nicht in ein Drittland zu übermitteln, außer nach Maßgabe von § 6.

2. **Vertraulichkeit** — die Kundendaten vertraulich zu behandeln. Der Auftragsverarbeiter ist ein Einzelunternehmer und erbringt die Leistung persönlich. Werden Beschäftigte oder Auftragnehmer eingesetzt, werden diese **vor Aufnahme der Tätigkeit in Textform** zur Vertraulichkeit verpflichtet und im Umgang mit personenbezogenen Daten unterwiesen.

3. **Sicherheit der Verarbeitung** — die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO zu treffen und aufrechtzuerhalten. Die Maßnahmen dürfen fortentwickelt werden, sofern das Schutzniveau nicht unterschritten wird.

4. **Unterauftragsverarbeiter** — Dritte nur nach Maßgabe von § 5 einzusetzen.

5. **Betroffenenrechte** — den Verantwortlichen bei der Erfüllung von Betroffenenanfragen nach Kapitel III DSGVO zu unterstützen. Der Verantwortliche kann Auskunft, Berichtigung, Löschung und Export weitgehend selbst in der Anwendung vornehmen; soweit dies nicht ausreicht, unterstützt der Auftragsverarbeiter auf Anfrage. Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst.

6. **Unterstützungspflichten** — den Verantwortlichen bei der Einhaltung der Art. 32 bis 36 DSGVO zu unterstützen, insbesondere bei einer Datenschutz-Folgenabschätzung, und ihm die dafür erforderlichen Informationen zur Verfügung zu stellen.

7. **Löschung und Rückgabe** — nach Beendigung des Vertrags gemäß § 10 zu verfahren.

8. **Nachweise** — dem Verantwortlichen die zum Nachweis der Einhaltung dieses Vertrags erforderlichen Informationen zur Verfügung zu stellen und Überprüfungen nach § 7 zu ermöglichen.

§ 4 Verletzung des Schutzes personenbezogener Daten

1. Der Auftragsverarbeiter informiert den Verantwortlichen **unverzüglich nach Kenntniserlangung, spätestens innerhalb von 72 Stunden**, über jede Verletzung des Schutzes personenbezogener Daten, die die Kundendaten betrifft.

2. Die Meldung erfolgt in Textform an die vom Verantwortlichen hinterlegte E-Mail-Adresse und enthält, soweit bekannt: - eine Beschreibung der Art der Verletzung sowie der betroffenen Datenkategorien und der ungefähren Zahl betroffener Personen und Datensätze, - die wahrscheinlichen Folgen, - die ergriffenen oder vorgeschlagenen Maßnahmen zur Abhilfe und Schadensbegrenzung, - eine Kontaktstelle für Rückfragen.

3. Sind zum Zeitpunkt der ersten Meldung nicht alle Angaben verfügbar, meldet der Auftragsverarbeiter zunächst den bekannten Sachverhalt und ergänzt die Angaben unverzüglich.

4. Die **Meldung an die Aufsichtsbehörde** und gegebenenfalls an die betroffenen Personen (Art. 33, 34 DSGVO) obliegt dem **Verantwortlichen**. Der Auftragsverarbeiter unterstützt ihn dabei.

§ 5 Unterauftragsverarbeiter

1. Der Verantwortliche erteilt hiermit die **allgemeine Genehmigung** nach Art. 28 Abs. 2 DSGVO zum Einsatz von Unterauftragsverarbeitern. Die derzeit eingesetzten Unterauftragsverarbeiter sind in **Anlage 1,**

Abschnitt D namentlich mit Sitz, Verarbeitungsort und Zweck benannt und werden hiermit genehmigt.

2. Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die den in diesem Vertrag vereinbarten **im Wesentlichen entsprechen** (Art. 28 Abs. 4 DSGVO).

3. **Beabsichtigte Änderungen** teilt der Auftragsverarbeiter dem Verantwortlichen **mindestens 14 Tage vorher in Textform an die hinterlegte E-Mail-Adresse** mit. Als Änderung gilt - die **Hinzuziehung** eines neuen oder der **Austausch** eines bestehenden Unterauftragsverarbeiters sowie - eine **wesentliche Änderung des Verarbeitungsorts** oder der **Konzernzugehörigkeit** eines bestehenden Unterauftragsverarbeiters.

Zusätzlich kann die Änderung in der Anwendung angezeigt werden; maßgeblich ist die Mitteilung per E-Mail.

4. Der Verantwortliche kann der Änderung innerhalb der Frist **aus einem wichtigen datenschutzrechtlichen Grund** in Textform widersprechen. Kommt keine Einigung zustande, kann **jede Partei** den Hauptvertrag zum Zeitpunkt des Wirksamwerdens der Änderung außerordentlich kündigen; bereits im Voraus gezahlte Entgelte werden anteilig erstattet. Widerspricht der Verantwortliche nicht fristgerecht, gilt die Änderung als genehmigt.

5. Bei **unmittelbarer Gefahr für die Verfügbarkeit oder Sicherheit** des Dienstes darf der Auftragsverarbeiter einen Unterauftragsverarbeiter vorübergehend ohne Vorlauf austauschen. Er informiert den Verantwortlichen in diesem Fall unverzüglich nachträglich; die Rechte aus Absatz 4 bleiben unberührt.

6. **Änderungen der Anlage 1, Abschnitt D, die auf einem Wechsel von Unterauftragsverarbeitern beruhen, richten sich ausschließlich nach diesem Paragraphen**; § 9 Abs. 2 findet auf sie keine Anwendung.

7. Nicht als Unterauftragsverarbeitung gelten **Nebenleistungen** ohne Bezug zur eigentlichen Datenverarbeitung, etwa Telekommunikationsdienste, Domainregistrierung oder die Zahlungsabwicklung des Hauptvertrags.

§ 6 Verarbeitungsorte und Drittländer

1. Die Verarbeitung der Kundendaten findet **innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums** statt. Die Verarbeitungsorte sind in **Anlage 1, Abschnitt D** je Unterauftragsverarbeiter angegeben.

2. **Ausnahme Schweiz:** Das E-Mail-Postfach des Auftragsverarbeiters wird von der Proton AG mit Sitz in der Schweiz betrieben. Für die Schweiz besteht ein **Angemessenheitsbeschluss** der Europäischen Kommission; eine Übermittlung dorthin bedarf keiner zusätzlichen Garantien nach Art. 46 DSGVO. Über dieses Postfach läuft die Korrespondenz mit dem Verantwortlichen. **Der Auftragsverarbeiter übermittelt von sich aus keine Inhalte aus dem Dienst dorthin.**

3. **Konzernstrukturen der Anbieter:** Einzelne der in Anlage 1, Abschnitt D genannten Unternehmen gehören Unternehmensgruppen an oder setzen Technologiepartner ein, die ihren Sitz außerhalb der EU haben und deren administrativer Zugriff auf die jeweilige Plattform nicht an den Standort der Rechenzentren gebunden ist. Die betreffenden Anbieter sind in Anlage 1, Abschnitt D **gekennzeichnet**. Die datenschutzrechtliche Absicherung dieser Konstellation obliegt dem jeweiligen Anbieter. Der Auftragsverarbeiter legt sie offen, damit der Verantwortliche sie in seiner eigenen Risikobetrachtung

berücksichtigen kann. **Unberührt bleiben die Pflichten des Auftragsverarbeiters aus § 5 Abs. 2 und § 8 Abs. 2.**

4. Soweit eine Übermittlung in ein Drittland erforderlich wird, erfolgt sie nur auf Grundlage eines Angemessenheitsbeschlusses oder geeigneter Garantien nach Art. 46 DSGVO. Der Auftragsverarbeiter informiert den Verantwortlichen darüber nach § 5 Abs. 3.

§ 7 Kontrollrechte und Nachweise

1. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage die zum Nachweis der Einhaltung dieses Vertrags erforderlichen Informationen zur Verfügung, insbesondere die Beschreibung der technischen und organisatorischen Maßnahmen (**Anlage 2**) und die von den Unterauftragsverarbeitern vorgelegten Nachweise, Zertifikate und Prüfberichte, soweit deren Weitergabe zulässig ist.

2. Der Verantwortliche kann darüber hinaus **einmal je Kalenderjahr** sowie anlassbezogen bei einem konkreten Verdacht eine Überprüfung durchführen oder durch einen von ihm beauftragten, nicht mit dem Auftragsverarbeiter im Wettbewerb stehenden Prüfer durchführen lassen. Überprüfungen sind **mindestens vier Wochen vorher** in Textform anzukündigen, auf die üblichen Geschäftszeiten zu legen und so durchzuführen, dass der Betrieb nicht unverhältnismäßig beeinträchtigt wird. Der Prüfer ist zur Verschwiegenheit zu verpflichten.

3. Für den Aufwand einer über Absatz 1 hinausgehenden Überprüfung kann der Auftragsverarbeiter eine angemessene Vergütung verlangen, sofern die Prüfung keine erheblichen Mängel zutage fördert.

4. **Vor-Ort-Prüfungen in den Rechenzentren** kann der Auftragsverarbeiter nicht gewähren, da er die Rechenzentren nicht selbst betreibt. An deren Stelle treten die Nachweise nach Absatz 1.

5. Rechte der Aufsichtsbehörden nach Art. 58 DSGVO bleiben unberührt und sind nicht an die Voraussetzungen dieses Paragraphen gebunden.

§ 8 Haftung

1. Für die Haftung der Parteien untereinander gelten die Regelungen des Hauptvertrags.

2. **Unberührt bleiben Art. 82 DSGVO sowie Art. 28 Abs. 4 S. 2 DSGVO**, wonach der Auftragsverarbeiter dem Verantwortlichen für die Einhaltung der Datenschutzpflichten der von ihm eingesetzten Unterauftragsverarbeiter haftet. Im Innenverhältnis tragen die Parteien den Schaden in dem Umfang, der ihrem Anteil an der Verantwortung für den schadensverursachenden Umstand entspricht.

3. Der Verantwortliche stellt den Auftragsverarbeiter von Ansprüchen Dritter frei, die darauf beruhen, dass der Verantwortliche Daten ohne ausreichende Rechtsgrundlage in den Dienst eingegeben oder eine unzulässige Weisung erteilt hat.

§ 9 Änderungen der Rechtslage und dieses Vertrags

1. Ändern sich die anwendbaren Datenschutzvorschriften oder wird dieser Vertrag durch eine Entscheidung einer Aufsichtsbehörde oder eines Gerichts in Teilen unwirksam, verpflichten sich die Parteien, den Vertrag unverzüglich so anzupassen, dass er den Anforderungen entspricht.

2. Der Auftragsverarbeiter kann diesen Vertrag anpassen, soweit dies aufgrund geänderter Rechtslage, geänderter Rechtsprechung oder geänderter technischer Gegebenheiten erforderlich ist. Änderungen werden dem Verantwortlichen **mindestens 30 Tage vor Wirksamwerden** in Textform mitgeteilt. Widerspricht er nicht innerhalb dieser Frist, gelten die Änderungen als angenommen; auf dieses Recht wird in der Mitteilung hingewiesen. Widerspricht er, kann jede Partei den Hauptvertrag zum Wirksamwerden der Änderung kündigen. **Für Änderungen der Anlage 1, Abschnitt D gilt ausschließlich § 5.**

3. Die jeweils geltende Fassung dieses Vertrags ist mit **Fassungsnummer und Datum** öffentlich abrufbar; frühere Fassungen bleiben abrufbar.

4. Änderungen und Ergänzungen bedürfen der Textform. Das gilt auch für die Abbedingung dieses Formerfordernisses.

§ 10 Laufzeit, Beendigung, Löschung

1. Dieser Vertrag beginnt mit der Aufnahme der Nutzung des Dienstes und endet mit dem Hauptvertrag, ohne dass es einer gesonderten Kündigung bedarf. Er kann nicht unabhängig vom Hauptvertrag gekündigt werden.

2. **Nach Wahl des Verantwortlichen** gibt der Auftragsverarbeiter die Kundendaten nach Beendigung des Hauptvertrags **zurück oder löscht sie** (Art. 28 Abs. 3 lit. g DSGVO). Teilt der Verantwortliche seine Wahl nicht innerhalb der Frist nach Absatz 3 mit, werden die Daten gelöscht.

3. Die Instanz des Verantwortlichen bleibt nach Beendigung des Hauptvertrags **30 Tage ausschließlich zum Zweck des Datenexports erreichbar**. Der Auftragsverarbeiter unterstützt den Verantwortlichen auf Anfrage beim Export.

4. Nach Ablauf dieser Frist wird die Instanz abgeschaltet und werden die Kundendaten gelöscht.

5. **Sicherungskopien:** Kundendaten befinden sich zusätzlich in turnusmäßigen Sicherungen. Diese werden nicht gezielt bereinigt, sondern laufen nach den regulären Aufbewahrungsfristen aus. Die vollständige Entfernung aus allen Sicherungsbeständen ist spätestens **sieben Monate nach Beendigung des Hauptvertrags** abgeschlossen. Bis dahin bleiben die Sicherungen verschlüsselt, unterliegen unverändert den Maßnahmen der Anlage 2 und werden **ausschließlich zum Zweck der Wiederherstellung** vorgehalten.

6. Der Auftragsverarbeiter bestätigt die Löschung auf Anfrage in Textform.

7. Eine über die Beendigung hinausgehende Aufbewahrung erfolgt nur, soweit gesetzliche Aufbewahrungspflichten entgegenstehen. Diese betreffen Rechnungs- und Vertragsdaten, nicht die Inhalte aus dem Dienst.

§ 11 Schlussbestimmungen

1. Sollte eine Bestimmung dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

2. Es gilt **österreichisches Recht** unter Ausschluss des Kollisionsrechts und des UN-Kaufrechts. Zwingende Vorschriften der DSGVO und des jeweiligen nationalen Datenschutzrechts des Verantwortlichen bleiben

unberührt.

3. Ausschließlicher Gerichtsstand für Streitigkeiten aus diesem Vertrag ist — soweit gesetzlich zulässig — der Sitz des Auftragsverarbeiters.

Anlage 1 — Einzelheiten der Verarbeitung

A. Gegenstand, Art und Zweck

Gegenstand: Bereitstellung und Betrieb des KI-Arbeitsplatzes „algonice mit Ody" als Software-Dienst, betrieben in einer dem Verantwortlichen eigens zugewiesenen Instanz.

Art der Verarbeitung: Erheben, Speichern, Ordnen, Auslesen, Verwenden, Übermitteln an die unter D genannten Unterauftragsverarbeiter, Löschen.

Zweck: Erfüllung des Hauptvertrags, namentlich

- Bereitstellung der Chat- und Assistenzfunktionen einschließlich der Weitergabe von Anfragen an die Anbieter der Sprachmodelle,
- Speicherung der vom Verantwortlichen angelegten Inhalte (Gespräche, Dokumente, Dateien),
- Durchsuchbarkeit eigener Dokumente über eine Vektor-Indexierung,
- Erzeugung von Bildern auf Anforderung,
- Betrieb, Absicherung, Fehlerbehebung und Datensicherung des Dienstes.

Dauer: für die Laufzeit des Hauptvertrags, im Übrigen nach § 10.

B. Kategorien betroffener Personen

- Beschäftigte, Auftragnehmer und sonstige vom Verantwortlichen berechtigte Nutzer der Instanz
- Dritte, deren personenbezogene Daten der Verantwortliche in den Dienst eingibt — insbesondere Kunden, Interessenten, Lieferanten, Korrespondenzpartner
- Personen, die in vom Verantwortlichen hochgeladenen Dokumenten genannt sind

> Der Kreis der betroffenen Personen wird allein durch den Verantwortlichen bestimmt.

C. Kategorien personenbezogener Daten

Kategorie	Inhalt	Aufbewahrung
Kontodaten	Anzeigename, Benutzername bzw. E-Mail-Adresse, Passwort (nur als kryptografischer Hash), Rolle, Spracheinstellung	bis zur Löschung durch den Verantwortlichen, im Übrigen nach § 10
Inhaltsdaten	Gesprächsverläufe, angelegte Dokumente und Notizen, hochgeladene Dateien, Dateien im Arbeitsbereich, erzeugte Bilder	ebenso
Abgeleitete Daten	Vektor-Repräsentationen (Embeddings) der eigenen Dokumente für die Suchfunktion	ebenso
Anbindungsdaten	Zugangs-Token für vom Verantwortlichen selbst angebundene externe Dienste	bis zur Trennung der Verbindung durch den Verantwortlichen
Zugriffsprotokolle	IP-Adresse, Zeitstempel, aufgerufene Adresse, Browserkennung, Sitzungskennung	**30 Tage**
Technische Systemprotokolle	Fehler- und Betriebsmeldungen der beteiligten Dienste	**90 Tage**
Nutzungs- und Verbrauchsdaten	Anzahl der Anfragen, verwendetes Modell, Umfang der verarbeiteten Texteinheiten (Token), Anzahl erzeugter Bilder — jeweils mit Zeitstempel, zur Durchsetzung des vereinbarten Leistungsumfangs	bis zum **Ende des auf die Nutzung folgenden Kalendermonats**. Danach ist der zeitliche Verlauf unwiederbringlich gelöscht; davon unberührt bleiben die zur Abrechnung erforderlichen **Verbrauchssummen je Kundenkonto ohne Zeitbezug**, die der Auftragsverarbeiter als **Verantwortlicher** auf Grundlage des Vertragsverhältnisses und der gesetzlichen Aufbewahrungspflichten speichert
Sicherheits- und Missbrauchsdaten	Bei abgelehnten Bildanfragen die **Ablehnungskategorie** (z. B. Gewaltdarstellung, Fälschung amtlicher Dokumente) zusammen mit der Kundenkennung. **Der Anfragetext selbst wird nicht gespeichert.** Zweck ist ausschließlich der Jugendschutz und die Abwehr missbräuchlicher Nutzung	**30 Tage**; danach bleibt nur der Vermerk „abgelehnt" ohne Kategorie

> **Zu allen Fristen dieser Tabelle:** Sicherungskopien werden längstens nach 14 Tagen überschrieben; bis dahin kann gelöschter Datenbestand dort noch enthalten sein.
>
> **Nicht erfasst sind Protokolle, die die Anwendung innerhalb der Instanz des Verantwortlichen schreibt.** Sie sind Teil seines Datenbestands, liegen in seinem Datenverzeichnis und unterliegen seiner eigenen Löschung bzw. § 10 — nicht den vorstehenden Fristen. Der Auftragsverarbeiter greift dort nicht ein.

Nicht vorgesehen: besondere Kategorien nach Art. 9 DSGVO und Daten nach Art. 10 DSGVO (§ 2 Abs. 5).

Nicht Gegenstand dieses Vertrags — Vertragsdaten des Verantwortlichen selbst: Für die Begründung und Abwicklung des Hauptvertrags verarbeitet der Auftragsverarbeiter **Name, Anschrift und E-Mail-Adresse** des Verantwortlichen. **Zahlungsdaten** erhält er nicht; die Zahlungsabwicklung erfolgt über einen eigenständigen Anbieter. Für diese Vertragsdaten ist der Auftragsverarbeiter **selbst Verantwortlicher**; Einzelheiten regelt die Datenschutzerklärung.

D. Unterauftragsverarbeiter

Fassung 1.0, Stand 2. August 2026

Nr.	Unternehmen	Sitz	Verarbeitungsort	Zweck	Daten, die dorthin gelangen
1	**IP-Projects GmbH & Co. KG**, Am Vogelherd 14, 97295 Waldbrunn, Deutschland (AG Würzburg HRA 6798)	Deutschland	Deutschland (Frankfurt, Eschborn, Würzburg)	Bereitstellung der Server, auf denen der Dienst läuft — hier liegen die Kundendaten gespeichert	alle unter C genannten Kategorien (als Speicherort)
2	**Hetzner Online GmbH**, Industriestr. 25, 91710 Gunzenhausen, Deutschland (AG Ansbach HRB 6089)	Deutschland	Deutschland (Falkenstein)	Aufbewahrung der Datensicherungen	alle unter C genannten Kategorien, **vor der Übertragung clientseitig verschlüsselt**
3 ⚑	**Infercom SCS**, 29 Boulevard Grande-Duchesse Charlotte, 1331 Luxemburg (RCS Luxembourg B298727)	Luxemburg	Deutschland (München)	Ausführung des Standard-Sprachmodells und der Vektor-Indexierung	Inhalt der jeweiligen Anfrage bzw. des zu indexierenden Textes; **keine Kontodaten**
4 ⚑	**TensorX Ltd.**, Unit 25, Classon House, Dundrum Business Park, Dublin 14, D14N2F6, Irland — CRO-Nr. **796387**, USt-ID IE4482721SH	Irland	Irland (Dublin) und Finnland (Helsinki)	Ausführung der zusätzlich wählbaren Sprachmodelle	Inhalt der jeweiligen Anfrage; **keine Kontodaten**
5	**Verda Cloud Oy** (bis 16.01.2026: DataCrunch Oy), Töölönlahdenkatu 2, 00100 Helsinki, Finnland — Y-tunnus **2886809-8**	Finnland	Finnland (Helsinki)	Bilderzeugung; zugleich Betreiber des Rechenzentrums für Nr. 4	Bildbeschreibung (Prompt) und erzeugtes Bild; **zusätzlich liegen die von Nr. 4 verarbeiteten Anfrageinhalte physisch auf Hardware dieses Anbieters**
6	**Proton AG**, Route de la Galaise 32, 1228 Plan-les-Ouates, Genf, Schweiz (CHE-354.686.492)	**Schweiz** (Angemessenheitsbeschluss)	Schweiz	Betrieb des E-Mail-Postfachs support@algonice.eu	Korrespondenz mit dem Verantwortlichen sowie Fehlermeldungen aus der Anwendung (Instanz, Zeitpunkt, Version, Modell, **Betriebsart**, Sitzungskennung — **kein Gesprächsinhalt**)

⚑ **Kennzeichnung nach § 6 Abs. 3:** Bei diesen Anbietern bestehen Konzernbeziehungen oder Technologiepartnerschaften mit Unternehmen außerhalb der EU, deren administrativer Zugriff auf die jeweilige Plattform nicht an den Standort der Rechenzentren gebunden ist.

Vertragsgrundlagen: Mit Nr. 1 und 2 bestehen gesonderte Verträge zur Auftragsverarbeitung. Bei Nr. 3, 4, 5 und 6 sind die Datenschutzbestimmungen Bestandteil der jeweiligen Nutzungs- bzw. Geschäftsbedingungen.

Zusicherungen zur Inferenz (Nr. 3, 4 und 5): Die Anbieter sagen zu, dass **Ein- und Ausgaben nicht dauerhaft gespeichert und nicht zum Training** von Modellen verwendet werden — bei Nr. 3 im Auftragsverarbeitungsvertrag, bei Nr. 4 und 5 in den jeweiligen Nutzungsbedingungen. Davon unberührt bleiben **technische Protokolldaten** (etwa Verbindungs- und Abrechnungsdaten), die bei den Anbietern anfallen und dort eigenen Aufbewahrungsfristen unterliegen.

Derzeit nicht eingesetzt: Ein GPU-Server der **Trooper.ai**, Niederlande, steht als technischer Rückfallweg bereit, verarbeitet gegenwärtig jedoch **keine Kundendaten**. Vor einer Reaktivierung wird diese Anlage um den vollständigen Rechtsträger ergänzt und die Änderung nach § 5 Abs. 3 angekündigt.

E. Übermittlungen, die keine Auftragsverarbeitung sind

1. **Websuche im Chat.** Ist die Websuche aktiviert, wird die Suchanfrage über einen eigenen Suchvermittler des Auftragsverarbeiters an externe Suchmaschinen weitergeleitet. Dabei werden **keine Kontodaten, keine Kennung des Verantwortlichen und keine Cookies** übertragen. Die Suchmaschinen sind insoweit **eigenständig Verantwortliche**. Die Funktion kann in den Einstellungen deaktiviert werden.

2. **Vom Verantwortlichen selbst angebundene externe Dienste.** Verbindet der Verantwortliche den Dienst mit einem Drittanbieter, entscheidet **er** über diese Übermittlung und ihre Rechtsgrundlage. Der Auftragsverarbeiter stellt die technische Schnittstelle bereit und speichert das Zugangs-Token. Solche Anbieter sind **nicht** Unterauftragsverarbeiter des Auftragsverarbeiters.

3. **Vom Nutzer aufgerufene Inhalte.** Ruft der Dienst auf Wunsch des Nutzers eine Webseite ab, handelt es sich um einen Zugriff auf ein fremdes Angebot, nicht um eine Auftragsverarbeitung.

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

Fassung 1.0, Stand 2. August 2026. Die Maßnahmen werden fortlaufend überprüft und dürfen fortentwickelt werden, solange das Schutzniveau nicht unterschritten wird.

> **Zur Darstellungstiefe:** Diese Anlage beschreibt die Maßnahmen so, dass ihre Eignung nach Art. 32 DSGVO beurteilt werden kann. Einzelheiten der Umsetzung — etwa konkrete Schwellenwerte, Adressen, Systembezeichnungen oder Aufbewahrungsstaffeln — werden bewusst **nicht** genannt: Ihre Veröffentlichung würde die Wirksamkeit der Maßnahmen selbst beeinträchtigen. Im Rahmen einer Überprüfung nach § 7 werden sie dem Verantwortlichen oder einem von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer offengelegt, soweit dies ohne Gefährdung der Sicherheit möglich ist.

1. Vertraulichkeit

1.1 Zutrittskontrolle (physischer Zugang)

Der Auftragsverarbeiter betreibt **keine eigenen Rechenzentren**. Die Server stehen in Rechenzentren der unter Anlage 1 D genannten Anbieter. Dort gelten unter anderem:

- Zutritt über biometrische Kontrolle und Chipkarten, Personenschleusen, Unterteilung in gesonderte Sicherheitsbereiche
- Videoüberwachung und Protokollierung der Zu- und Ausgänge, Personal rund um die Uhr
- redundante Stromversorgung mit USV und Netzersatzanlage, Brandfrüherkennung, Klimatisierung

Für den Anbieter der Datensicherung sind diese Maßnahmen durch ein **ISO-27001-Zertifikat**, ein **BSI-C5-Typ-2-Testat** sowie einen **Prüfbericht des TÜV Rheinland mit Ortsbegehungen** belegt.

1.2 Zugangskontrolle (Systemzugang)

Maßnahme	Umsetzung
Administrativer Serverzugang	ausschließlich **schlüsselbasiert**; eine Anmeldung mit Passwort ist serverseitig nicht vorgesehen
Beschränkung der Herkunft	administrative Zugänge sind auf **autorisierte Herkunftsadressen** beschränkt; übrige Verbindungsversuche werden bereits auf Netzwerkebene verworfen
Automatische Sperre	wiederholte Fehlversuche führen zu einer **automatischen zeitweiligen Sperre** der Herkunftsadresse
Kundenzugang	über HTTPS mit persönlichem Konto und Passwort; Passwörter werden ausschließlich als **kryptografischer Hash** gespeichert, nicht im Klartext
Öffentliche Registrierung	in den Kundeninstanzen **deaktiviert** — Konten legt allein der Verantwortliche an
Transportverschlüsselung	ausschließlich **TLS**, per HSTS erzwungen; unverschlüsselte Verbindungen werden umgeleitet

1.3 Zugriffskontrolle (Rechte innerhalb des Systems)

- Innerhalb der Instanz gilt das Rollen- und Rechtekonzept der Anwendung; der Verantwortliche vergibt die Rollen selbst.
- Der administrative Zugriff des Auftragsverarbeiters ist auf den technischen Betrieb beschränkt und erfolgt anlassbezogen (Betrieb, Sicherung, Fehlerbehebung, Aktualisierung).
- Betriebsroutinen laufen unter einem **eigens reservierten technischen Konto**, nicht unter einem Kundenkonto.
- Zugangsdaten zu Anbietern werden je Kunde vergeben und nicht zwischen Kunden geteilt.

1.4 Trennungskontrolle (Mandantentrennung)

Dies ist die zentrale Maßnahme des Betriebsmodells:

- **Je Verantwortlichem eine eigene Anwendungsinstanz** mit eigener Datenbank und eigenem Datenverzeichnis. Ein gemeinsamer Datenbestand mehrerer Kunden besteht nicht.
- **Je Verantwortlichem ein eigenes, isoliertes Container-Netz**; die Instanzen sind netzseitig voneinander getrennt.
- **Je Verantwortlichem ein eigenes Zugangs-Token** zum vorgelagerten Modell-Zugangsdienst; Freischaltung und Nutzungsgrenzen werden je Token geführt.
- Eigene Subdomain und eigenes Zertifikat je Instanz.

1.5 Datensparsamkeit

- Die Fehlermeldung aus der Anwendung überträgt **keine Gesprächsinhalte**, sondern ausschließlich Instanz, Zeitpunkt, Version, Modell, Betriebsart und eine Sitzungskennung, über die der Auftragsverarbeiter den Vorgang im eigenen Protokoll zuordnen kann. Was der Nutzer der Meldung von sich aus hinzufügt, bestimmt er selbst.
- Suchanfragen an externe Suchmaschinen werden ohne Kundenkennung und ohne Cookies gestellt (Anlage 1 E Nr. 1).

2. Integrität

2.1 Weitergabekontrolle

- Verbindungen zwischen Nutzer und Dienst sowie zwischen Dienst und den Anbietern nach Anlage 1 D erfolgen **verschlüsselt (TLS)**.
- **Datensicherungen werden vor der Übertragung an den Sicherungsanbieter clientseitig verschlüsselt**; der Sicherungsanbieter kann die Inhalte nicht lesen.
- Die Anwendung ist gegen das Ansprechen interner Netzadressen über nutzergesteuerte Adressen abgesichert (Schutz vor serverseitigen Anfragefälschungen).

2.2 Eingabekontrolle

- Zugriffe auf die Instanz werden mit Zeitpunkt, Herkunftsadresse und aufgerufener Adresse protokolliert; die Anwendung protokolliert technische Vorgänge zusätzlich.
- Änderungen an der Betriebskonfiguration werden versioniert geführt und sind nachvollziehbar.

3. Verfügbarkeit und Belastbarkeit

Ebene	Maßnahme
Tägliche Sicherung	die Daten des Verantwortlichen werden **automatisch täglich gesichert**
Auslagerung	die Sicherungen werden zusätzlich **verschlüsselt an einen räumlich getrennten Ort** übertragen und dort mehrstufig vorgehalten (Frist s. § 10 Abs. 5)
Schutz vor Manipulation	die ausgelagerten Bestände sind **vom Produktivsystem aus nicht veränder- oder löschbar**; sie überstehen damit auch eine Kompromittierung des laufenden Systems
Überwachung	fehlgeschlagene Sicherungen lösen **automatisch eine Meldung** aus
Erprobung	der Wiederherstellungsweg ist **erprobt**, einschließlich eines Abgleichs der Prüfsummen wiederhergestellter Dateien; die Lesbarkeit der ausgelagerten Bestände wird turnusmäßig stichprobenartig überprüft
Mehrere Ebenen	die Sicherung erfolgt auf mehreren voneinander unabhängigen Ebenen

4. Verfahren zur regelmäßigen Überprüfung

- **Auftragskontrolle:** Mit allen Unterauftragsverarbeitern bestehen Datenschutzvereinbarungen; die Nachweise werden gesammelt, mit Datum und Prüfsumme abgelegt und bei bekannt werdenden Änderungen erneut geprüft.
- **Sicherheitsüberprüfung:** Der Betriebsstand wird anlassbezogen und mindestens jährlich überprüft (Zugangshärtung, Firewall, offene Dienste, Rechtevergabe, Netztrennung). Befunde werden mit Maßnahme und Nachweis dokumentiert.
- **Aktualisierungen:** Software-Aktualisierungen werden auf einem gesonderten Testsystem erprobt, bevor sie auf Kundeninstanzen ausgerollt werden. Der eingesetzte Stand ist festgeschrieben und versioniert.
- **Datenschutz durch Voreinstellung:** Funktionen mit erhöhtem Risiko sind in der Standardauslieferung abgeschaltet.
