Vertragsanlage über die Auftragsverarbeitung personenbezogener Daten

i.S.d. Art. 28 DSGVO

zwischen
Plattformanbieter
– nachfolgend „**Auftragnehmer**“ genannt –

und
Plattformnutzer
– nachfolgend „**Auftragsgeber**“ genannt –

(gemeinsam „Parteien“)

---

§ 1 Gegenstand, Dauer und Ort der Verarbeitung

1. **Gegenstand.** Der Auftragnehmer **Chester Roussos (Einzelunternehmen)** stellt dem Auftragsgeber eine SaaS-Plattform zur Einbindung eines KI-gestützten Chatbots auf den Webseiten des Auftragsgebers bereit.
   Im Rahmen dieses Vertrages verarbeitet der Auftragnehmer personenbezogene Daten **im Auftrag und nach Weisung** des Auftragsgebers zum Betrieb des Chatbots (Widget), des Dashboards (Konfiguration, Statistiken), der Wissensbasis (Datei-Uploads, Unternehmens- und Produktinformationen) sowie hierfür erforderlicher Systemfunktionen (z. B. Authentifizierung, transaktionale E-Mails, Zahlungsabwicklung via beauftragte Unterauftragsverarbeiter).
   Eine Nutzung der Daten zu eigenen Zwecken des Auftragnehmers findet nicht statt.

2. **Beginn und Ende.** Dieser Vertrag zur Auftragsverarbeitung tritt **mit Abschluss des Nutzungsverhältnisses über die Plattform des Auftragnehmers** in Kraft und gilt **für die Dauer der Nutzung**. **Die Beendigung der Nutzung der Plattform durch Kündigung oder Löschung des Accounts führt automatisch auch zur Beendigung dieses Vertrages.** Eine **gesonderte Kündigung** des Auftragsverarbeitungsvertrags ist **nicht erforderlich**.

3. **Verarbeitungsort.** Die Verarbeitung erfolgt grundsätzlich in der EU/des EWR. Soweit Unterauftragsverarbeiter außerhalb der EU/des EWR eingesetzt werden, geschieht dies ausschließlich unter Beachtung von **Kapitel V DSGVO** (vgl. § 10 und **Anlage 1**).

---

§ 2 Art, Zweck und Umfang der Verarbeitung; Daten- und Personenkategorien

1. **Art der Verarbeitung:** Erheben, Erfassen, Organisieren, Speichern, Anpassen/Verändern, Auslesen, Verwenden, Übermitteln (an Unterauftragsverarbeiter), Abgleichen, Einschränken, Löschen/Vernichten.
2. **Zweck:** Bereitstellung und Betrieb der SaaS-Plattform „Chatvise“ sowie der damit verbundenen Funktionen, insbesondere

   - Einbindung und Betrieb des KI-gestützten Chatbots auf den Webseiten des Auftragsgebers,
   - Konfiguration, Steuerung und Auswertung über das Dashboard,
   - Verarbeitung und Speicherung von durch den Auftragsgeber bereitgestellten Wissens-, Unternehmens- und Produktinformationen zur Erweiterung der Chatbot-Wissensbasis,
   - Durchführung systemischer Prozesse wie Authentifizierung, Benachrichtigungen und Zahlungsabwicklung,
   - Qualitätssicherung, Stabilität und Verbesserung der Dienstleistung.

   Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers (z. B. Marketing, Analyse, eigenständiges KI-Training) findet nicht statt.
3. **Kategorien personenbezogener Daten** (je nach Nutzung/Konfiguration durch den Auftragsgeber):

   - **Chat-Inhalte** (Freitexteingaben der Webseitenbesucher),
   - **optional**: E-Mail-Adresse des Webseitenbesuchers (falls durch den Auftragsgeber aktiviert),
   - **Meta-/Prozessdaten** (z. B. interne Chat-IDs, Zeitstempel von Einwilligungen/Popups, Antwortzeiten, Übergaben),
   - **Kundendaten des Auftragsgebers** (z. B. Name, E-Mail, Login-/Geräteinformationen),
   - **Abrechnungsdaten** (z. B. Zahlungs-ID/Transaktionsdaten beim Zahlungsdienst),
   - **Wissensbasis-Dokumente** (z. B. vom Auftragsgeber bereitgestellte PDFs, Textdaten oder Produktinformationen zur Bereitstellung der Wissensbasis und kontextbezogenen Antwortgenerierung).
4. **Kategorien betroffener Personen:** Webseitenbesucher des Auftragsgebers (Endnutzer), beim Auftragsgeber autorisierte Nutzer (Admin/Agent), Ansprechpartner beim Auftragsgeber.

---

§ 3 Rollen; Weisungsrecht

1. Der **Auftragsgeber** ist **Verantwortlicher** i. S. d. Art. 4 Nr. 7 DSGVO. Der **Auftragnehmer** ist **Auftragsverarbeiter**.
2. Der Auftragnehmer verarbeitet personenbezogene Daten **ausschließlich auf dokumentierte Weisung** des Auftragsgebers; hierunter fallen insbesondere Einstellungen im Dashboard. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.
3. Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Auftragsgeber unverzüglich.
4. **Suspendierungsrecht:** Der Auftragnehmer ist berechtigt, die Umsetzung rechtswidriger oder unklarer Weisungen **bis zur Klärung auszusetzen**. Der Auftragnehmer haftet nicht für Verzögerungen/Leistungseinschränkungen, die auf ausgesetzte, rechtswidrige oder unklare Weisungen zurückzuführen sind.

---

§ 4 Pflichten des Auftragnehmers

1. **Rechtskonforme Organisation:** Interne Prozesse sind so auszugestalten, dass die Anforderungen der DSGVO, insbesondere Art. 28 und Art. 32, eingehalten werden.
2. **Vertraulichkeit:** Personen, die beim Auftragnehmer Daten verarbeiten, sind **vertraulich verpflichtet**.
3. **Technische und organisatorische Maßnahmen (TOMs):** Der Auftragnehmer implementiert und unterhält die in **Anlage 2** beschriebenen TOMs. Anpassungen sind zulässig, sofern das Schutzniveau **nicht unterschritten** wird.
4. **Unterstützungspflichten:** Angemessene Unterstützung des Auftragsgebers bei **Betroffenenrechten** (Art. 12–22), **Meldungen** von Verletzungen (Art. 33/34), **DSFA** (Art. 35) und ggf. **Konsultationen** (Art. 36).
5. **Nachweise/Protokolle:** Geeignete Nachweise zur Einhaltung (z. B. Informationen zur Rechenzentrums-Sicherheit, Policies) stellt der Auftragnehmer auf Anfrage bereit.
6. **Datenminimierung/Privacy by Design:** Verarbeitung nur im erforderlichen Umfang; Pseudonymisierung/Maskierung, wo zweckmäßig (z. B. Richtung KI-API).
7. **Drittlandtransfers:** Nur nach Maßgabe von **Kapitel V DSGVO** (vgl. § 10).

---

§ 5 Pflichten und Garantien des Auftragsgebers

1. Der Auftragsgeber garantiert, dass für alle im Rahmen dieses Vertrages verarbeiteten personenbezogenen Daten eine **geeignete Rechtsgrundlage** besteht und **Informationspflichten** ordnungsgemäß erfüllt sind (z. B. Hinweis auf KI-Interaktion, Datenschutzhinweise/Popup).
2. Der Auftragsgeber ist allein verantwortlich für **Inhalte**, die er oder seine Nutzer bereitstellen (einschließlich Trainingsdaten, Uploads, Freitexteingaben, Konfigurationen).
3. Weisungen sind rechtmäßig, eindeutig und **dokumentiert** zu erteilen.
4. Die Plattform wird **rechtskonform** konfiguriert (u. a. E-Mail-Abfrage nur mit Rechtsgrundlage; passende **Löschintervalle**; **Rollen/Zugriffsrechte**).
5. Verletzungen dieser Pflichten gehen **zu Lasten des Auftragsgebers** (Innenverhältnis).

---

§ 6 Sicherheitsvorfälle (Art. 33/34 DSGVO)

1. Der Auftragnehmer informiert den Auftragsgeber **unverzüglich** über bekannt gewordene **Verletzungen des Schutzes personenbezogener Daten**.
2. Die Mitteilung enthält, soweit möglich: Art des Vorfalls, betroffene Datenkategorien/Anzahl, voraussichtliche Folgen, ergriffene/geplante Abhilfemaßnahmen.
3. Der Auftragnehmer unterstützt den Auftragsgeber bei Bewertung, Meldung an die Aufsichtsbehörde und Benachrichtigung Betroffener.
4. Die Kommunikation mit Behörden/Betroffenen erfolgt durch den Auftragsgeber; der Auftragnehmer handelt hierbei nur auf Weisung.

---

§ 7 Betroffenenrechte und Auskunftsersuchen

1. Gehen Betroffenenanfragen beim Auftragnehmer ein, leitet er diese – soweit zuordenbar – **ohne unangemessene Verzögerung** an den Auftragsgeber weiter.
2. Unterstützung des Auftragsgebers bei der Beantwortung im erforderlichen und zumutbaren Umfang.

---

§ 8 Nachweise, Audits, Inspektionen

1. Der Auftragnehmer stellt **angemessene Nachweise** zur Verfügung (z. B. Informationen zur Rechenzentrums-Sicherheit, TOM-Übersichten).
2. **Audits/Inspektionen** durch den Auftragsgeber oder beauftragte Prüfer: nach vorheriger Ankündigung, zu üblichen Geschäftszeiten, unter Wahrung von Vertraulichkeit und Betriebsabläufen. Vor-Ort-Audits sind nur erforderlich, wenn andere geeignete Nachweise **nicht ausreichen**.
3. Audits können an Bedingungen (Geheimnisschutz, keine Wettbewerber als Prüfer) geknüpft werden. Erforderliche Unterstützung wird – soweit nicht gesetzlich zwingend – angemessen vergütet.

---

§ 9 Löschung und Rückgabe von Daten

1. **Wahlrecht des Auftragsgebers:** Nach Beendigung des Nutzungsverhältnisses kann der Auftragsgeber die im Auftrag verarbeiteten personenbezogenen Daten innerhalb der vom Auftragnehmer vorgesehenen Frist über die bereitgestellten Exportfunktionen abrufen. Soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen und keine anderweitige dokumentierte Weisung des Auftragsgebers vorliegt, löscht der Auftragnehmer die Daten nach Ablauf dieser Frist.
2. **Löschfunktion während der Laufzeit (Dashboard):** Der Auftragnehmer stellt im Dashboard eine Funktion bereit, mit der der Auftragsgeber die **Löschung sämtlicher personenbezogener Daten** (soweit technisch möglich und nicht aufbewahrungspflichtig) beauftragen kann; die Löschung erfolgt **unverzüglich** nach Auftragseingang.
3. **Optionale automatisierte Löschung:** Die Pflicht zur Löschung/Anonymisierung der im Auftrag verarbeiteten Chat-Daten liegt ausschließlich beim Auftragsgeber. Der Auftragnehmer stellt hierfür optional eine Funktion zur automatisierten Löschung bereit; die Intervalle werden allein vom Auftragsgeber konfiguriert (30/60/90/180/360 Tage). Ohne entsprechende Konfiguration erfolgt keine automatisierte Löschung; in diesem Fall nimmt der Auftragsgeber die Löschung eigenverantwortlich über das Dashboard vor
4. **Backups:** Gelöschte Datensätze können für die Dauer der **Backup-Rotation** in Sicherungen enthalten sein; Backups dienen ausschließlich **Integritäts-/Wiederherstellungszwecken** und werden nach Ablauf der Rotation **überschrieben**. Im Restore-Fall werden zuvor gelöschte Datensätze erneut entfernt.

---

§ 10 Unterauftragsverhältnisse (Subprozessoren)

1. Die aktuell eingesetzten Unterauftragsverarbeiter sind in **Anlage 1** aufgeführt; der Auftragsgeber **stimmt** diesen zu.
2. Der Auftragnehmer informiert den Auftragsgeber **vorab** über die Einbindung/Änderung weiterer Subprozessoren (z. B. per E-Mail/Dashboard-Hinweis). Der Auftragsgeber kann innerhalb einer angemessenen Frist **aus wichtigem datenschutzrechtlichen Grund** widersprechen.
3. Der Auftragnehmer verpflichtet Subprozessoren **schriftlich** auf ein Datenschutzniveau, das diesem Vertrag entspricht (Art. 28 Abs. 4 DSGVO).
4. **Drittländer:** Bei Verarbeitung außerhalb des EU/EWR-Raums stellt der Auftragnehmer geeignete Garantien nach **Kapitel V DSGVO** sicher (z. B. EU-Standardvertragsklauseln, Angemessenheitsbeschluss).
5. Unterstützende Nebenleistungen ohne spezifischen Datenzugriff (z. B. Reinigung) gelten **nicht** als Unterauftragsverhältnisse; angemessenes Schutzniveau wird dennoch sichergestellt.
6. Der Auftragnehmer haftet **nicht** für Leistungsstörungen von Subprozessoren, die auf **höhere Gewalt, flächendeckende Störungen** oder **behördliche Anordnungen** beruhen. Ansprüche gegenüber Subprozessoren werden – soweit möglich – an den Auftragsgeber **abgetreten**.

---

§ 11 Technische und organisatorische Maßnahmen (TOMs)

1. Die **TOMs** des Auftragnehmers sind in **Anlage 2** beschrieben und stellen das **vereinbarte Mindestschutzniveau** dar.
2. Anpassungen an technische/organisatorische Entwicklungen sind zulässig, sofern das Schutzniveau **mindestens gleichwertig** bleibt. **Wesentliche Änderungen** werden mitgeteilt.

---

§ 12 Haftung und Innenausgleich

1. **Zwingende Haftung:** Nichts in diesem Vertrag beschränkt die Haftung einer Partei für **Vorsatz**, **grobe Fahrlässigkeit**, **Schäden aus Verletzung von Leben, Körper oder Gesundheit** sowie Haftungstatbestände, die gesetzlich **nicht** beschränkbar sind (einschl. **Art. 82 DSGVO gegenüber Betroffenen**).
2. **Kardinalpflichten:** Bei leicht fahrlässiger Verletzung wesentlicher Vertragspflichten (Kardinalpflichten) ist die Haftung auf den **typischerweise vorhersehbaren Schaden** begrenzt.

3. **Haftungscap (Innenverhältnis):** Im Übrigen ist die vertragliche und deliktische Haftung des Auftragnehmers gegenüber dem Auftragsgeber auf den **Netto-Vergütungsbetrag der letzten zwölf (12) Monate** vor dem schadensauslösenden Ereignis **gedeckelt**. **Ausgenommen** vom Cap sind die Fälle nach Abs. 1 sowie Schäden, die durch einen **nachweislichen Verstoß gegen die in Anlage 2 festgelegten TOMs** entstanden sind.
4. **Ausschluss indirekter Schäden:** Mittelbare Schäden, entgangener Gewinn, Produktions- und Nutzungsausfall, Datenwiederherstellungskosten **außerhalb** regulärer Backuproutinen sowie Folgeschäden sind ausgeschlossen, soweit nicht Abs. 1 eingreift.
5. **Innenausgleich nach Art. 82 Abs. 5 DSGVO:** Soweit der Auftragnehmer Betroffenen gegenüber haftet, ohne den Schaden verursacht zu haben, hat der Auftragsgeber den Auftragnehmer im Innenverhältnis **entsprechend seinem Verantwortungsanteil** freizustellen.

---

§ 12a Freistellung (Indemnität)

1. Der Auftragsgeber stellt den Auftragnehmer von **Ansprüchen Dritter**, behördlichen Maßnahmen (einschließlich Bußgeldern, soweit rechtlich zulässig), **Schäden, Kosten und Aufwendungen** (einschließlich angemessener Rechtsverfolgungskosten) frei, die zurückzuführen sind auf:
   (a) **rechtswidrige oder fehlende Weisungen**,
   (b) **fehlende Rechtsgrundlagen**,
   (c) **vom Auftragsgeber oder dessen Nutzern bereitgestellte Inhalte/Daten**,
   (d) **nicht DSGVO-konforme Konfigurationen** oder
   (e) **Vertragsverletzungen** des Auftragsgebers.
2. Der Auftragnehmer informiert den Auftragsgeber unverzüglich über geltend gemachte Ansprüche und stimmt Abwehr-/Vergleichsmaßnahmen mit ihm ab.

---

§ 13 Schlussbestimmungen

1. Änderungen/Ergänzungen dieses Vertrages bedürfen der **Textform**.
2. Sollten einzelne Bestimmungen unwirksam sein/werden, bleibt der Vertrag im Übrigen wirksam; an die Stelle der unwirksamen Bestimmung tritt eine zulässige Regelung, die dem wirtschaftlichen Zweck am nächsten kommt.
3. Es gilt **deutsches Recht**. Soweit zulässig, ist Gerichtsstand der Sitz des Auftragnehmers.

4. **Höhere Gewalt/Behördliche Anordnungen:** Keine Partei haftet für Verzögerungen/Leistungshindernisse infolge **höherer Gewalt**, **flächendeckender Störungen der Telekommunikations-/Cloud-Infrastruktur** oder **behördlicher Anordnungen**, sofern die Partei hierauf keinen Einfluss hat und zumutbare Maßnahmen trifft.

Anlage 1 – Unterauftragsverarbeiter (Stand: 28.03.2026)

Dienst	Zweck	Region / Transfermechanismus
Amazon Web Services (AWS)	Infrastruktur/Hosting (z. B. DB/Compute)	EU (Frankfurt, eu-central-1) – kein Drittlandtransfer bei ausschließlicher EU-Nutzung
Supabase	Authentifizierung / Plattform-Services	EU-Region (projektspezifisch) – ggf. SCC bei Supportzugriffen außerhalb der EU
OpenAI (API)	KI-Antwortgenerierung	Übermittlungen außerhalb der EU nach SCC/DPF; Zero-Data-Retention aktiviert
Stripe	Zahlungsabwicklung	Verarbeitung durch EU-Entität; etwaige Übermittlungen in die USA nach DPF/SCC
Resend	Versand transaktionaler E-Mails	Übermittlungen in die USA nach DPF/SCC
Uploadcare	Datei-Uploads (Wissensbasis)	Speicherung je nach Konfiguration EU/USA; Übermittlungen nach DPF/SCC

Anlage 2 – Übersicht der umgesetzten technischen und organisatorischen Maßnahmen (Art. 32 DSGVO) (Stand: 28.03.2026)

Maßnahmenbereich	Ziel der Maßnahme	Umgesetzte Maßnahme
Zutrittskontrolle	Verhinderung des physischen Zugriffs Unbefugter auf Server	Rechenzentrums-Sicherheit beim Hostinganbieter (AWS, Region EU); physische Zugangsbeschränkungen durch den Anbieter
Zugangskontrolle	Nur autorisierte Personen dürfen auf das System zugreifen	Passwortschutz + 2FA für Admin-/Agent-Zugänge; rollenbasierte Berechtigungen (RBAC)
Zugriffskontrolle (intern)	Beschränkung interner Zugriffe auf notwendige Daten (Need-to-know)	Serverseitig durchgesetztes RBAC (Admin/Agent); Nutzung eingeschränkter Service-Konten (kein Superuser im Produktivbetrieb)
Weitergabekontrolle (Übertragung)	Schutz bei Datenübertragungen	TLS/SSL für alle externen Verbindungen; HSTS; Schutz von API-Keys/Secrets auf Server-Seite
Eingabekontrolle / Protokolle	Nachvollziehbarkeit, wer was wann geändert hat	Änderungs-/Administrations-Logging in der Plattform (z. B. Rollen-, Konfig-, Löschaktionen); auditfähige Logs nach Erforderlichkeit
Auftragskontrolle	DSGVO-konformer Umgang mit Subdienstleistern	Abschluss von AV-Vereinbarungen mit Unterauftragsverarbeitern; veröffentlichte Subprozessor-Liste; Vorab-Information bei Änderungen
Verfügbarkeitskontrolle	Schutz vor Datenverlust / Ausfall	Nutzung von infrastrukturseitigen Backups/Redundanzen und Wiederherstellungsmechanismen des Hostinganbieters (AWS); Monitoring/Alerting
Trennungsgebot	Daten verschiedener Kunden dürfen nicht vermischt werden	Logische Mandantentrennung auf Datenbank-/Applikationsebene; getrennte Speicherbereiche für Wissensbasis-Uploads
Datensicherung	Wiederherstellbarkeit bei Ausfall	Automatisierte, verschlüsselte Backups auf Infrastruktur-Ebene (AWS-Rotation); im Restore-Fall erneute Löschung zuvor gelöschter Datensätze

Maßnahmenbereich	Ziel der Maßnahme	Umgesetzte Maßnahme
Privacy by Design/Default	Datenschutzfreundliche Voreinstellungen	Datenminimierung (E-Mail-Erfassung optional); Maskierung/Pseudonymisierung Richtung KI-API; konfigurierbare Löschintervalle für Chat-Daten (30/60/90/180/360 Tage)
Organisation/Prozesse	Geregelte Abläufe und Verantwortlichkeiten	Vertraulichkeitsbindung; dokumentierte Prozesse für Incident-Response sowie Bearbeitung von Weisungen und Betroffenenanfragen