Vertrag zur Auftragsverarbeitung (AVV)

gemäß Art. 28 DSGVO – Anlage zu den Verträgen der ScaliRo GmbH

zwischen

dem Kunden gemäß Hauptvertrag – nachfolgend „**Verantwortlicher**“ –

und

ScaliRo GmbH, Eduard-Rüber-Straße 7, 83022 Rosenheim – nachfolgend „**Auftragsverarbeiter**“ –

1 Geltungsbereich

1.1 Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien, soweit der Auftragsverarbeiter bei der Erbringung seiner Leistungen personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Er gilt für folgende Verträge (jeweils „**Hauptvertrag**“):

- Lizenzvereinbarung FleetEngine (Software-as-a-Service),
- Lizenzvereinbarung FleetEngine Flottenmanager (On-Premise), soweit der Kunde dabei vom Auftragsverarbeiter betriebene Online-Dienste nutzt (z. B. Anmeldung), über die personenbezogene Daten verarbeitet werden; die Online-Lizenzvalidierung allein fällt nicht darunter,
- Wartungs- und Supportverträge, soweit der Auftragsverarbeiter dabei Zugriff auf personenbezogene Daten erhält (z. B. Fernwartung, Übergabe von Daten zur Fehleranalyse),
- Dienstleistungsaufträge (z. B. Simulations- und Projektleistungen), soweit dabei personenbezogene Daten des Verantwortlichen verarbeitet werden.

1.2 Dieser Vertrag wird mit Abschluss des jeweiligen Hauptvertrags Vertragsbestandteil, ohne dass es einer gesonderten Unterzeichnung bedarf (Art. 28 Abs. 9 DSGVO).

1.3 Bestellt ein Zwischenhändler im Auftrag des Kunden, ist Verantwortlicher im Sinne dieses Vertrags der Kunde, der die Leistungen nutzt. Der Zwischenhändler stellt sicher, dass dem Kunden dieser Vertrag zur Kenntnis gebracht wird.

1.4 Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes dem Hauptvertrag vor.

2 Gegenstand, Art und Zweck der Verarbeitung

Merkmal	**Beschreibung**
Gegenstand	Bereitstellung und Betrieb der Plattform FleetEngine/FleetPortal sowie damit verbundene Support- und Dienstleistungen gemäß Hauptvertrag
Art der Verarbeitung	Erheben, Speichern, Anzeigen, Übermitteln innerhalb der Plattform, Sichern, Löschen
Zweck	Ermöglichung der Nutzung der Plattform durch die Nutzer des Verantwortlichen, Benutzer- und Rechteverwaltung, Fehleranalyse und Support

Merkmal	Beschreibung
Kategorien von Daten	Benutzerdaten (Name, E-Mail-Adresse, Organisationszugehörigkeit, Rollen); Nutzungs- und Protokolldaten (z. B. Anmeldezeitpunkte, IP-Adressen, durchgeführte Aktionen); Kommunikationsinhalte in der Plattform (z. B. Kommentare, Erwähnungen); personenbezogene Inhalte, die der Verantwortliche in Projekten ablegt
Betroffene Personen	Beschäftigte und Beauftragte des Verantwortlichen, die die Plattform nutzen; ggf. in Projektdaten genannte Personen
Dauer	Laufzeit des Hauptvertrags zuzüglich der Fristen nach Ziffer 9
Ort der Verarbeitung	Rechenzentren in der EU (überwiegend Deutschland); Unterauftragsverarbeiter gemäß Anlage 2

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der Verarbeitung. Der Verantwortliche stellt keine solchen Daten in die Plattform ein.

3 Weisungen

3.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist gesetzlich zu einer Verarbeitung verpflichtet. In diesem Fall teilt er dem Verantwortlichen die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Gesetz dies nicht verbietet.

3.2 Die Weisungen ergeben sich aus dem Hauptvertrag, dieser Vereinbarung und der Nutzung der Plattform durch den Verantwortlichen (z. B. Anlegen und Löschen von Nutzern und Projekten). Weitere Weisungen erteilt der Verantwortliche in Textform.

3.3 Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, weist er den Verantwortlichen unverzüglich darauf hin.

4 Pflichten des Auftragsverarbeiters

4.1 **Vertraulichkeit:** Alle Personen, die Zugang zu den Daten haben, sind zur Vertraulichkeit verpflichtet.

4.2 **Sicherheit:** Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO gemäß **Anlage 1**. Er darf diese an den Stand der Technik anpassen, sofern das Schutzniveau nicht unterschritten wird.

4.3 **Unterstützung:** Der Auftragsverarbeiter unterstützt den Verantwortlichen im angemessenen Umfang bei der Erfüllung der Rechte der betroffenen Personen (Kapitel III DSGVO) sowie bei den Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung).

4.4 **Datenschutzverletzungen:** Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden nach deren Bestätigung, mit den ihm vorliegenden Angaben nach Art. 33 Abs. 3 DSGVO.

4.5 **Betroffenenanfragen:** Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter.

4.6 **Ansprechpartner Datenschutz:** Patrick Burkart, E-Mail: datenschutz@scaliro.de. Ein Datenschutzbeauftragter ist gesetzlich nicht zu benennen (§ 38 BDSG).

5 Unterauftragsverarbeiter

5.1 Der Verantwortliche genehmigt die in **Anlage 2** aufgeführten Unterauftragsverarbeiter.

5.2 Der Auftragsverarbeiter informiert den Verantwortlichen mindestens **4 Wochen** vor dem Einsatz eines neuen oder dem Austausch eines Unterauftragsverarbeiters in Textform. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Kommt keine Einigung zustande, kann jede Partei den betroffenen Teil des Hauptvertrags außerordentlich kündigen.

5.3 Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieses Vertrags entsprechen.

5.4 Eine Verarbeitung außerhalb der EU/des EWR erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss, EU-Standardvertragsklauseln).

6 Nachweise und Kontrollen

6.1 Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage die zum Nachweis der Einhaltung dieses Vertrags erforderlichen Informationen zur Verfügung, insbesondere eine aktuelle Beschreibung der technischen und organisatorischen Maßnahmen sowie Zertifikate seiner Unterauftragsverarbeiter.

6.2 Reichen diese Nachweise nicht aus, kann der Verantwortliche nach Ankündigung mit einer Frist von mindestens 30 Tagen höchstens einmal pro Kalenderjahr eine Prüfung während der üblichen Geschäftszeiten durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen. Anlassbezogene Prüfungen nach einer Datenschutzverletzung bleiben unberührt.

6.3 Der Verantwortliche trägt die Kosten der Prüfung, es sei denn, die Prüfung deckt einen wesentlichen Verstoß des Auftragsverarbeiters auf.

7 Eigene Verarbeitungen des Auftragsverarbeiters

Nicht Gegenstand dieses Vertrags sind Verarbeitungen, die der Auftragsverarbeiter für eigene Zwecke in eigener Verantwortung durchführt, insbesondere:

- Vertragsabwicklung, Abrechnung und Kommunikation mit Ansprechpartnern des Kunden,
- Prüfung und Verwaltung von Lizenzen,
- Gewährleistung der IT-Sicherheit und Missbrauchsabwehr,
- Bearbeitung von Support-Anfragen.

Hierüber informiert der Auftragsverarbeiter in seiner Datenschutzerklärung.

8 Pflichten des Verantwortlichen

8.1 Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Rechtsgrundlage und die Information der betroffenen Personen (z. B. seiner Nutzer) nach Art. 13 und 14 DSGVO.

8.2 Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

8.3 Daten zur Fehleranalyse (z. B. Protokolldateien, Projektstände) übermittelt der Verantwortliche nach Möglichkeit ohne Personenbezug oder pseudonymisiert.

9 Löschung und Rückgabe

9.1 Nach Ende des Hauptvertrags löscht der Auftragsverarbeiter die personenbezogenen Daten des Verantwortlichen einschließlich der Datensicherungen spätestens nach **4 Wochen**, sofern keine gesetzliche Aufbewahrungspflicht besteht.

9.2 Bis dahin kann der Verantwortliche seine Daten über die Exportfunktionen der Plattform selbst sichern.

9.3 Auf Anfrage bestätigt der Auftragsverarbeiter die Löschung in Textform.

10 Haftung und Schlussbestimmungen

10.1 Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags, soweit gesetzlich zulässig.

10.2 Dieser Vertrag endet mit dem Hauptvertrag. Die Pflichten nach Ziffer 9 und die Vertraulichkeit gelten darüber hinaus.

10.3 Änderungen dieses Vertrags bedürfen der Textform. Der jeweils aktuelle Stand ist unter https://www.scaliro.de/avv abrufbar.

10.4 Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

10.5 Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts (CISG). Gerichtsstand ist, soweit zulässig, Rosenheim.

10.6 Bei Widersprüchen zwischen der deutschen Fassung dieses Vertrags und einer Übersetzung ist die deutsche Fassung maßgeblich.

Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Die ausführliche Beschreibung enthält das Sicherheitskonzept der ScaliRo GmbH, das auf Anfrage bereitgestellt wird.

Bereich	**Maßnahmen**
Zutrittskontrolle	Hosting in ISO/IEC-27001-zertifizierten Rechenzentren der Hetzner Online GmbH in Deutschland (Zutrittskontrolle, Videoüberwachung, Alarmanlagen); ScaliRo betreibt keine eigenen Rechenzentren
Zugangskontrolle	Anmeldung über Microsoft Entra ID (OpenID Connect) mit erzwungener Mehr-Faktor-Authentisierung; personengebundene Konten; Administration nur über verschlüsselte Verbindungen (SSH, HTTPS)
Zugriffskontrolle	Rollenbasiertes Rechtemodell (Organisation, Space, Projekt), serverseitige Prüfung jeder Anfrage; Rechtevergabe nach Need-to-know; regelmäßige Überprüfung privilegierter Zugänge
Trennungskontrolle	Eigener virtueller Server und eigene Datenbank je Kundenprojekt; Trennung von Entwicklungs-, Test- und Produktivumgebung
Weitergabekontrolle	Verschlüsselte Übertragung (TLS) zwischen Nutzern und Plattform sowie zu Dienstleistern; Datenbanken nur über private Netzwerke erreichbar
Eingabekontrolle	Protokollierung von Anwendungs- und Sicherheitsereignissen; Nachvollziehbarkeit von Änderungen über Versionierung und Freigabeprozesse
Verfügbarkeitskontrolle	Regelmäßige Projekt-Backups getrennt von den Produktivdaten zur Betriebssicherheit (ohne Anspruch des Verantwortlichen; seine Pflicht zur eigenen Datensicherung nach dem Hauptvertrag bleibt unberührt); redundante Datenbank (Replica Set); DDoS-Schutz des Hosting-Anbieters; Notfall- und Wiederanlaufplanung
Auftragskontrolle	Auswahl von Unterauftragsverarbeitern nach Sicherheitskriterien; Verträge nach Art. 28 DSGVO
Organisatorische Maßnahmen	Informationssicherheitsleitlinie und Sicherheitsrichtlinien; Verpflichtung der Mitarbeitenden auf Vertraulichkeit; Sensibilisierung; geregelter Prozess für Sicherheitsvorfälle; sichere Softwareentwicklung mit Schwachstellenprüfung

Anlage 2 – Genehmigte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland	Hosting der Plattform (Server, Netzwerk, Speicher, Backups)	Deutschland
Microsoft Ireland Operations Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	Anmeldung (Entra ID), Versand von Einladungen (Microsoft Graph), Container-Registry und Entwicklungsplattform (Azure)	EU (EU-Datengrenze): Microsoft 365 derzeit Deutschland, Azure Container Registry Deutschland (Germany West Central), Azure DevOps Niederlande (West Europe), Entra ID EU-Rechenzentren; Drittlandbezug USA, abgesichert über EU-US Data Privacy Framework bzw. Standardvertragsklauseln