Data Processing Agreement (DPA)

pursuant to Art. 28 GDPR – Annex to the agreements of ScaliRo GmbH

between

the Customer under the Main Agreement – hereinafter "**Controller**" –

and

ScaliRo GmbH, Eduard-Rüber-Straße 7, 83022 Rosenheim, Germany – hereinafter "**Processor**" –

1 Scope

1.1 This Agreement sets out the data protection obligations of the parties insofar as the Processor processes personal data on behalf of the Controller when providing its services. It applies to the following agreements (each a "**Main Agreement**"):

- License Agreement FleetEngine (Software-as-a-Service),
- License Agreement FleetEngine Fleet Manager (on-premise), insofar as the Customer uses online services operated by the Processor (e.g. sign-in) through which personal data is processed; online license validation alone is not covered,
- maintenance and support agreements, insofar as the Processor obtains access to personal data (e.g. remote maintenance, provision of data for error analysis),
- service orders (e.g. simulation and project services), insofar as personal data of the Controller is processed.

1.2 This Agreement becomes part of the respective Main Agreement upon its conclusion without requiring a separate signature (Art. 28(9) GDPR).

1.3 If a reseller places an order on behalf of the Customer, the Controller within the meaning of this Agreement is the Customer who uses the services. The reseller shall ensure that this Agreement is brought to the Customer's attention.

1.4 In the event of conflicts, this Agreement takes precedence over the Main Agreement in matters of data protection.

2 Subject Matter, Nature and Purpose of the Processing

Item	**Description**
Subject matter	Provision and operation of the FleetEngine/FleetPortal platform and related support and other services under the Main Agreement
Nature of the processing	Collection, storage, display, transfer within the platform, backup, erasure
Purpose	Enabling the Controller's users to use the platform, user and permission management, error analysis and support
Categories of data	User data (name, e-mail address, organisational affiliation, roles); usage and log data (e.g. sign-in times, IP addresses, actions performed); communication content within the platform (e.g. comments, mentions); personal content stored by the Controller in projects

Item	Description
Data subjects	Employees and agents of the Controller who use the platform; where applicable, persons named in project data
Duration	Term of the Main Agreement plus the periods under Section 9
Place of processing	Data centres in the EU (predominantly Germany); sub-processors as listed in Annex 2

Special categories of personal data (Art. 9 GDPR) are not subject to the processing. The Controller shall not enter any such data into the platform.

3 Instructions

3.1 The Processor processes personal data only on documented instructions from the Controller, unless required to do so by law. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits such information.

3.2 The instructions result from the Main Agreement, this Agreement and the Controller's use of the platform (e.g. creating and deleting users and projects). Further instructions shall be given by the Controller in text form.

3.3 If the Processor considers that an instruction infringes data protection provisions, it shall inform the Controller without undue delay.

4 Obligations of the Processor

4.1 **Confidentiality:** All persons with access to the data are bound to confidentiality.

4.2 **Security:** The Processor implements the technical and organisational measures pursuant to Art. 32 GDPR as set out in **Annex 1**. It may adapt them to the state of the art, provided that the level of protection is not reduced.

4.3 **Assistance:** The Processor assists the Controller to a reasonable extent in fulfilling data subjects' rights (Chapter III GDPR) and the obligations under Art. 32 to 36 GDPR (security, notification of personal data breaches, data protection impact assessment).

4.4 **Personal data breaches:** The Processor notifies the Controller of a personal data breach without undue delay, at the latest within 24 hours after its confirmation, providing the information available to it pursuant to Art. 33(3) GDPR.

4.5 **Data subject requests:** If a data subject contacts the Processor directly, the Processor forwards the request to the Controller without undue delay.

4.6 **Data protection contact:** Patrick Burkart, e-mail: datenschutz@scaliro.de. The appointment of a data protection officer is not required by law (Section 38 BDSG).

5 Sub-processors

5.1 The Controller approves the sub-processors listed in **Annex 2**.

5.2 The Processor informs the Controller in text form at least **4 weeks** before engaging a new sub-processor or replacing a sub-processor. Within this period, the Controller may object for an important reason relating to data protection. If no agreement is reached, either party may terminate the affected part of the Main Agreement for cause.

5.3 The Processor contractually binds sub-processors to data protection obligations equivalent to those of this Agreement.

5.4 Processing outside the EU/EEA only takes place if the requirements of Art. 44 et seq. GDPR are met (e.g. adequacy decision, EU standard contractual clauses).

6 Evidence and Audits

6.1 Upon request, the Processor provides the Controller with the information necessary to demonstrate compliance with this Agreement, in particular a current description of the technical and organisational measures and certificates of its sub-processors.

6.2 If such evidence is not sufficient, the Controller may, with at least 30 days' notice and no more than once per calendar year, carry out an audit during normal business hours or have it carried out by an auditor bound to confidentiality. Audits following a personal data breach remain unaffected.

6.3 The Controller bears the costs of the audit unless the audit reveals a material breach by the Processor.

7 Processing by the Processor for Its Own Purposes

This Agreement does not cover processing that the Processor carries out for its own purposes under its own responsibility, in particular:

- contract performance, invoicing and communication with the Customer's contact persons,
- verification and management of licenses,
- ensuring IT security and preventing misuse,
- handling support requests.

The Processor provides information on this in its privacy policy.

8 Obligations of the Controller

8.1 The Controller is responsible for the lawfulness of the processing, in particular for the legal basis and for informing the data subjects (e.g. its users) pursuant to Art. 13 and 14 GDPR.

8.2 The Controller informs the Processor without undue delay if it detects errors or irregularities in the processing.

8.3 The Controller shall, where possible, provide data for error analysis (e.g. log files, project states) without personal reference or in pseudonymised form.

9 Erasure and Return

9.1 After termination of the Main Agreement, the Processor erases the Controller's personal data, including backups, at the latest after **4 weeks**, unless a statutory retention obligation applies.

9.2 Until then, the Controller may back up its data itself using the platform’s export functions.

9.3 Upon request, the Processor confirms the erasure in text form.

10 Liability and Final Provisions

10.1 Liability is governed by Art. 82 GDPR. Otherwise, the liability provisions of the Main Agreement apply to the extent permitted by law.

10.2 This Agreement ends with the Main Agreement. The obligations under Section 9 and confidentiality continue to apply thereafter.

10.3 Amendments to this Agreement require text form. The current version is available at https://www.scaliro.de/avv.

10.4 Should any provision be invalid, the validity of the remaining provisions shall remain unaffected.

10.5 This Agreement is governed by German law, excluding the UN Convention on Contracts for the International Sale of Goods (CISG). Place of jurisdiction is Rosenheim, Germany, to the extent permitted by law.

10.6 In the event of discrepancies between the German version of this Agreement and a translation, the German version shall prevail.

Annex 1 – Technical and Organisational Measures (Art. 32 GDPR)

A detailed description is contained in the security concept of ScaliRo GmbH, which is provided upon request.

Area	**Measures**
Physical access control	Hosting in ISO/IEC 27001-certified data centres of Hetzner Online GmbH in Germany (access control, video surveillance, alarm systems); ScaliRo does not operate its own data centres
System access control	Sign-in via Microsoft Entra ID (OpenID Connect) with enforced multi-factor authentication; personal accounts; administration only via encrypted connections (SSH, HTTPS)
Data access control	Role-based permission model (organisation, space, project), server-side verification of every request; permissions granted on a need-to-know basis; regular review of privileged access
Separation control	Dedicated virtual server and dedicated database per customer project; separation of development, test and production environments
Transfer control	Encrypted transmission (TLS) between users and platform and to service providers; databases accessible only via private networks
Input control	Logging of application and security events; traceability of changes through versioning and release processes
Availability control	Regular project backups separate from production data for operational security (without entitlement of the Controller; its obligation to back up its own data under the Main Agreement remains unaffected); redundant database (replica set); DDoS protection by the hosting provider; emergency and recovery planning
Processor control	Selection of sub-processors based on security criteria; agreements pursuant to Art. 28 GDPR
Organisational measures	Information security policy and security guidelines; confidentiality obligation of employees; awareness training; defined process for security incidents; secure software development with vulnerability testing

Annex 2 – Approved Sub-processors

Sub-processor	Service	Place of processing
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany	Hosting of the platform (servers, network, storage, backups)	Germany
Microsoft Ireland Operations Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland	Sign-in (Entra ID), sending of invitations (Microsoft Graph), container registry and development platform (Azure)	EU (EU Data Boundary): Microsoft 365 currently Germany, Azure Container Registry Germany (Germany West Central), Azure DevOps Netherlands (West Europe), Entra ID EU data centres; third-country reference USA, safeguarded by the EU-US Data Privacy Framework or standard contractual clauses