Supplemental agreement for contract data processing pursuant to Article 28 GDPR

Between

Name: _____

Street: _____

Post Code/City: _____

Country: _____

- Controller within the meaning of Art. 4(7) GDPR, hereinafter referred to as the "**Controller**" -

and

OpenProject GmbH

Karl-Liebknecht-Str. 5

D-10178 Berlin

Germany

- Processor within the meaning of Art. 4(8) GDPR, hereinafter referred to as the "**Processor**" -

Preamble

This contract data processing agreement governs the obligations of the contracting parties with regard to data protection arising under the service agreement, including product descriptions.

Product: OpenProject Cloud Edition

Customer number: _____

Contract number (URL): _____

Contract date: _____

This agreement applies to all activities related to the primary contract in which employees of the Processor or agents of the Processor may come into contact with personal data of the Controller. The Processor will collect, process and otherwise use personal data for the Controller exclusively within the scope of this contract data processing agreement in accordance with Art. 28 GDPR.

§ 1 Scope and responsibilities

(1) The subject, type and purpose of the contract are activities whose specification is based on the service contract referred to above and the associated product descriptions.

(2) The Processor shall not use data provided to them for processing for any other purposes. Copies and/or duplicates may not be made without the knowledge of the Controller. This does not include backup copies, to the extent necessary to ensure proper data processing, and data required to comply with the statutory retention obligations.

(3) The Controller is solely responsible for assessing the lawfulness of the collection, processing and use of personal data by the Processor within the framework of their contractual relationship with regard to the provisions of the European General Data Protection Regulation (GDPR) and other relevant laws and regulations concerning data protection.

§ 2 Location of the intended data processing

The contractually agreed upon data processing shall take place exclusively within a Member State of the European Union or in another state that is party to the Agreement on the European Economic Area (EEA). The transfer of personal data to entities domiciled neither in a Member State of the European Union nor any other contracting state to the Agreement on the European Economic Area (so-called “third country”) requires the consent of the Controller and may only take place if the special requirements of Art. 44 ff. GDPR have been satisfied.

§ 3 Type of data processed and categories of data subjects

(1) The personal data undergoing processing pursuant to this agreement includes the following data types/categories (list/description of data categories):

- First and last name
- E-mail address
- Telephone number (optionally for sending 2FA one-time-passwords)
- Profile picture (avatar image)

(2) The categories of data subjects affected by the processing include:

- Employees of the Controller
- Customers of the Controller
- Suppliers of the Controller

For billing purposes the Processor collects the following information from the Controller:

- Company name
- Billing address
- Bank details
- VAT ID

§ 4 Technical and organisational measures

The Processor shall structure their internal organisation in such a way that they will meet the special requirements applicable to data protection. The measures implemented by the Processor are set out in Annex 1 to this contract data processing agreement. The Processor shall keep their documentation of technical and organisational measures up to date at all times.

§ 5 Rectification, restriction and erasure of data

The Processor may only rectify, erase or restrict the processing of data as processed pursuant to this contract if instructed to do so by the Controller. If a data subject contacts the Processor directly in this context, the Processor shall forward this request to the Controller.

§ 6 Obligations of the Controller

(1) The Controller is responsible for all data, automated procedures and data processing equipment within their area of responsibility as well as for safeguarding the rights of data subjects.

(2) The Controller shall arrange for the technical and organisational measures necessary to ensure data protection and data security in connection with the contract data processing. The nature and scope of the work and the powers of the staff employed by the Processor must be specified in sufficient detail. The costs of such technical and organisational measures, which must be implemented at the Processor's business owing to special requirements of the Controller, shall be borne by the Controller.

(3) The Controller has the right to issue instructions concerning the type, scope and sequence of the work. All such instructions must be issued in writing. Oral instructions must be confirmed by the Controller in writing without undue delay.

(4) Persons who are authorised to issue instructions, take receipt of consignments and perform monitoring must be named in writing. They must identify themselves when performing their functions.

§ 7 Duties of the Processor

(1) In addition to complying with the provisions of this agreement, the Processor shall comply with the statutory obligations set out in Articles 28 to 33 GDPR. Without limitation, the Processor shall ensure compliance with the following requirements:

(1) Written appointment of a data protection officer who will perform their duties in accordance with Articles 38 and 39 GDPR. The contact details for the data protection officer are set out in Annex 1.

(2) Maintaining confidentiality in accordance with Articles 28(3)(b), 29, 32(4) GDPR. In carrying out their work, the Processor shall exclusively use employees who are bound to maintain confidentiality and who have previously been familiarised with the relevant data protection provisions. The Processor and any person under their authority who has access to personal data of the Controller may only process such data exclusively in accordance with instructions from the Controller, including the authority granted in this agreement, unless they are legally obliged to process such data.

(3) The implementation and compliance with all technical and organisational measures required for the respective contract data processing in accordance with Articles 28(3)(c), 32 GDPR. The technical and organisational measures are documented in Annex 1 to this agreement.

(4) Notification of the Controller regarding control procedures and measures taken by the supervisory authority in so far as they relate to the underlying contractual relationship.

(5) The Processor may only provide information to data subjects or third parties concerning the underlying contractual relationship with the consent of the Controller unless they are legally obliged to do so.

§ 8 Subcontractors

(1) Subcontracting relationships within the meaning of this provision shall be understood to mean those services which relate directly to the provision of the principal service. This does not include ancillary services used by the Processor, e.g. telecommunications services, postal/transport services, maintenance and user services or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software used in data processing systems. However, the Processor shall be obliged to undertake appropriate and legally binding contractual agreements and control measures to ensure the data protection and the data security of the Controller's data, including in relation to outsourced ancillary services.

(2) The Processor may only engage subcontractors to process personal data of the Controller if they are located in a Member State of the European Union or in another country which is a signatory to the Agreement on the European Economic Area (EEA). Forwarding, storing and processing data using automated data processing systems outside the EU or the EEA is not permitted.

(3) The Controller agrees to the engagement of the subcontractors named by the Processor in Annex 2 to this agreement on condition of a contractual agreement in accordance with Art. 28(2)-(4) GDPR.

(4) Outsourcing to further subcontractors or the change of an existing subcontractor is permissible provided that:

- The Processor will notify the Controller in writing or in text form of outsourcing to such subcontractors prior to the start of processing by the respective subcontractor. The Controller's right of objection extends for two weeks after notification, and notice must likewise be given in writing or in text form.
- A contractual agreement in accordance with Art. 28(2)-(4) GDPR serves as the basis for the engagement.

(5) The Processor shall regularly check the subcontractor's compliance with data protection requirements.

(6) The transfer of personal data from the Controller to the subcontractor, and their commencement of work, are only permitted if all requirements for subcontracting are met.

§ 9 Control rights of the Controller

(1) Upon appropriate advance notice, the Controller is entitled to have inspections performed by auditors to be appointed on a case-by-case basis. The Processor shall ensure that the Controller can satisfy themselves of the Processor's compliance with the obligations in accordance with Art. 28 GDPR. The Processor shall grant the Controller access to the Processor's property and business premises upon prior arrangement of an appointment during normal local operating and business hours. The Processor is required to furnish the necessary information to the Controller on request and to demonstrate, in particular, the implementation of the technical and organisational measures.

(2) Proof of such measures, which do not only relate to a specific engagement, may be provided in the form of compliance with approved rules of conduct in accordance with Art. 40 GDPR; certification according to an approved certification procedure pursuant to Art. 42 GDPR; current certificates, reports or report extracts from independent bodies (e.g. auditor, internal audit department, data protection officer); suitable certification by IT security or data protection audit (e.g. according to BSI Basic Protection).

§ 10 Notification of breaches by the Processor

(1) The Processor shall inform the Controller of violations of the protection of personal data, disturbances, breaches of data protection regulations or the specifications made in a specific agreement by the Processor or persons employed by them or engaged by them. This is especially the case with regard to any legal obligations of the Controller to notify data subjects or the supervisory authorities.

(2) To the extent possible, the Processor shall assist the Controller in complying with the obligations set out in Articles 30 to 36 GDPR concerning the security of personal data, notification obligations in the event of personal data breaches, data protection impact assessments and prior consultations. This includes, in particular:

- Subdivision of the facility into individual security areas;
- Ensuring an adequate level of protection by means of technical and organisational measures that consider the circumstances and purposes of the processing, as well as the predicted likelihood and severity of a possible infringement due to vulnerabilities and that make immediate identification of relevant violations possible;
- The obligation to report personal data breaches to the Controller;
- The obligation to support the Controller in connection with their duty to inform data subjects;
- Supporting the Controller in connection with their obligations to carry out data protection impact assessments;
- Supporting the Controller in connection with prior consultations with the supervisory authority.

§ 11 Confidentiality obligations

(1) Both parties agree that all information obtained in the course of executing this contract shall be treated as confidential for an indefinite period and shall be used exclusively to perform the tasks agreed herein. Neither party is entitled to use this information in whole or in part for any other purposes other than those referred to above or to disclose such information to third parties.

(2) The foregoing obligation does not apply to information which one of the parties has demonstrably received from third parties without being bound to maintain confidentiality or which is publicly known.

§ 12 Contract term

(1) The validity of this agreement for contract data processing ("term") corresponds to the term of the service agreement referred to in section 1. The confidentiality obligation survives the term of this contract.

(2) A violation of legal or contractual data protection provisions by the Processor represents good cause for the Controller to exercise their right of extraordinary termination as reserved in the service agreement referred to in section 1.

§ 13 Severability

(1) Should one or more provisions of this agreement be or become invalid or unenforceable, this shall not affect the validity of the remaining provisions of this agreement.

§ 14 Final provisions

(1) Amendments or supplements to this agreement must be made in writing and must be signed by both parties. This also applies to the amendment of this written form clause. E-mail does not satisfy the written form requirement.

(2) The assertion of a right of retention within the meaning of section 273 of the German Civil Code (BGB) is excluded with respect to the processed data and the associated data storage devices.

(3) This agreement is governed exclusively by the laws of the Federal Republic of Germany. The place of jurisdiction for all disputes arising under or in connection with this contract is Berlin.

§ 15 Effective date

This agreement is effective upon its signing.

§ 16 Annexes

The following Annexes are appended to this contract data processing agreement:

- Annex 1: Technical and organisational data security measures
- Annex 2: List of subcontractors in use

§ 17 Signatures

_____, dated _____	_____, dated _____
Place Date	Place Date
_____	_____
- Controller -	- Processor (OpenProject GmbH) -

Annex 1: Technical and organisational data security measures

The data security measures defined by the Processor in this Annex have been agreed as binding.

1. Confidentiality (Art. 32(1)(b) GDPR)

1.1. Entry control

Data processing by the Processor shall be performed in a secure computer centre. The computer centre is certified according to ISO 27001 concerning its information security management system. Access to the computer centre is secured by state-of-the-art control systems. This includes the following security measures and infrastructure:

- Subdivision of the facility into individual security areas;
- Physical access protection, for example through steel doors, windowless rooms or secured windows;
- Protection of security areas through an electronic access control system;
- Monitoring of the facility by security services and logging access to the facility;
- Video surveillance of all security-relevant security areas, such as entrances, emergency exits and server rooms;
- Central assignment and revocation of access authorisations;
- Identification of all visitors by means of identity card;
- Obligatory identification within the security areas for all employees and visitors;
- Visitors must be accompanied by employees at all times.

1.2. Access control

The Processor is required to prevent the intrusion by unauthorised persons into systems and applications used for the processing of personal data. The Processor ensures this by granting access to the data processing systems of the IaaS provider solely to explicitly authorised administrators. Login takes place exclusively via multi-factor authentication based on the login information stored in the respective personal user account. In addition, the Processor employs a differentiated rights system based on security groups and access control lists. It is only possible to log in via connections that are encrypted using state-of-the-art technology.

Individual services and components are divided into several network segments to further secure access. Isolation is provided by means of a hardware-based firewall systems and Virtual Private Clouds (VPC). Every access to systems and applications is documented, monitored and logged centrally.

The internal office network is protected against unauthorised access from outside by a hardware-based firewall. Access to computers in the Processor's offices is controlled via user accounts. The internal office network can only be accessed from outside the premises via an encrypted VPN connection (Virtual Private Network).

The Controller can only access their OpenProject instance via an encrypted connection (SSL/HTTPS).

1.3. Access controls

The Processor is required to prevent unauthorised activities within the data processing systems. Accordingly, only the respective Controller and a small group of individually-named administrators have access to the data. Technical measures shall ensure that a Controller cannot view, modify or erase data of other controllers. Within an OpenProject instance, access is controlled via a comprehensive role-based access control and authorisation concept. Within an OpenProject instance, rights are allocated by the Controller by assigning appropriate roles and rights. In addition, the Controller has the option of adapting the preconfigured roles and rights for their organisation to their needs via an administrative interface.

Access to the Controller's data by the Processor's customer service representatives is limited to master data and billing data necessary for the performance of their customer service functions and invoicing hosting services. Customer service representatives do not have access to customer data within an OpenProject instance.

Credit card data of their controllers are exclusively stored by the payment service provider; the Processor has no access to this data.

Administrators are only allowed access to customer data if there is a fault that cannot be resolved by the Controller and/or the Processor's customer service alone.

1.4. Separation control

All data records that are collected, processed or used by the Processor's systems and applications are explicitly and clearly assigned to the respective Processor and technically separated from other data. The Processor's data processing systems are specially designed for data processing that is limited to a specific purpose and specific client. Access to the data of another client is thus technically impossible.

1.5. Pseudonymisation (Art. 32(1)(a) in conjunction with Art. 25(1) GDPR)

Pseudonymisation is intended to ensure that the identification of a data subject affected by data processing is not possible or is made considerably more difficult.

Data concerning deleted users in OpenProject are anonymised so that it is no longer possible to associate such data with the respective persons.

2. Integrity (Art. 32(1)(b) GDPR)

2.1. Transfer control

Control of the transfer of the Controller's data is ensured by various technical and organisational security measures. As part of these measures, the Processor never processes or stores the Controller's data outside the

computer centre. Employees of the computer centre operator have no physical or technical access to the Controller's data such that they can neither view, erase or modify such data. Data backups are only stored solely in encrypted form. The Controller's data are not transported on physical data carriers. For the purpose of invoicing for services, billing data is transferred to the Processor's accounting systems via an encrypted connection.

2.2. Input control

The Processor must guarantee the transparency and/or documentation of data processing. For this purpose, all entries made into the systems and applications are logged by the Processor. The logs are archived and erased once the purpose has been achieved or on the basis of legal requirements. The OpenProject application supports the entry and modification of its own data exclusively via user interfaces and interfaces provided for this purpose in accordance with a detailed role-based access control and authorisation concept. For many objects, the Controller may also view the change history for data via the web interface (e.g. work packages, wiki pages, SCM repositories).

3. Integrity (Article 32(1)(b) GDPR)

3.1. Availability control

The Processor must protect personal data against accidental destruction or loss. For this purpose, the architecture of the Processor's data processing systems, including network infrastructure, the power supply and the connection to the Internet must be designed redundantly.

A comprehensive backup and recovery concept must be in place to prevent data loss. The Controller's data is continuously backed-up in a separate availability zone via a replication mechanism. In addition, complete backups of all systems and data are made on a daily basis.

The systems and applications are continuously monitored with regard to availability, functionality, safety and utilisation. A written emergency plan is in place to restore the backups in the event of loss or destruction.

3.2. Rapid recoverability (Art. 32(1)(c) GDPR)

Measures must be taken to ensure that data can be recovered quickly in the event of data loss.

A combination of redundant systems and backup solutions is used to protect against the loss of the Controller's data. All data are backed up at least once a day. In case of data loss, this data can be recovered from the existing backups. Data are stored in geographically independent locations.

4. Availability and resilience (Art. 32(1)(b GDPR)

Resilience means the ability to resist attacks or to quickly bring systems back into working order after an attack.

The technical systems of the OpenProject platform are able to cope with expected disruptive events without their functionality being significantly impaired. IT systems are continuously hardened to protect against known attacks such as denial-of-service attacks.

In addition, each essential component is designed redundantly so that in the event of a fault, a switch to a defect-free component takes place automatically. Additional capacities can also be flexibly exchanged or expanded.

The OpenProject platform has modern, multitier architecture. As part of this architecture, access to the aspects via network disconnections is technically so limited that, for example, the database management system cannot be accessed from the Internet but rather only the load balancers.

Emergency plans exist which, in the event of a fault, provide precise instructions for restoring the desired condition. These emergency plans, and the protection concepts, are continuously reviewed and the relevant employees receive regular training in connection with their deployment.

5. Data protection management

5.1. Contact details of the Processor(s) or the Processor's representative(s)

Mr Ingo Wolff (Data Protection Officer)

Tacticx GmbH

Walbecker Straße 53

D-47608 Geldern

5.2. Process for regular testing, assessment and evaluation (Art. 32(1)(d); Art. 25(1) GDPR)

A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing must be implemented.

This measure is to be implemented with the aid of a data protection management system. The effectiveness of the technical and organisational measures implemented is to be tested and optimised within the scope of a continuous improvement process. Regular audits are to be conducted by an external accredited expert as part of these efforts.

5.3. Incident response management; reporting channel

Measures must be in place to ensure that the Processor informs the Controller without undue delay in the event of a personal data breach or the suspicion of a personal data breach.

All contractual partners are contractually obliged to report data protection incidents within the legal deadlines. Internal processes ensure that the Data Protection Officer is involved in case of data protection incidents.

5.4. Data protection by default (Art. 25(2) GDPR)

Appropriate technical and organisational measures must be implemented for ensuring that, by default, only personal data that are necessary for each specific purpose of the processing are processed.

After expiration of the test phase, as well as after termination of the contractual relationship, customer data that have been collected must be erased within three months. In addition, the customer can independently delete individual users within its OpenProject installation. This results in the deletion of the following personal data:

- First and last name
- E-mail address
- Telephone number
- User name
- User profile picture (avatar image)

Data that has been created, such as comments on work packages, are assigned to an anonymous user after deletion.

5.5. Contractor control

The Processor processes data submitted to them in accordance with the applicable contract and, in doing so, ensures compliance with statutory provisions and requirements defined by contract within the scope of the instructions provided by the Controller. The OpenProject platform has an administration interface through which the Controller can manage their customer account. The Controller specifies their access data within their user account during the initial account creation process. Only persons who have such access data can enter, change or delete customer data within the scope of their assigned authorisations. The written form requirement applies to all other tasks that the Controller cannot perform independently via the administration interface.

Annex 2: List of subcontractors in use

The Controller consents to the use of the subcontractors listed below by the Processor.

Subcontractors	**Subject of the engagement**	**Statement concerning the guarantee of the requisite level of protection**
Amazon Web Services Inc. 410 Terry Avenue North, Seattle WA 98109-5210, USA	Infrastructure-as-a-Service	Standard data protection clauses (Art. 46 Abs. 2 litt. c und DSGVO)
Google Inc. 1600 Amphitheatre Parkway Mountain View CA 94043, USA	Analyse des Nutzer-Zugriffsverhaltens zur Produktoptimierung	Standard data protection clauses (Art. 46 Abs. 2 litt. c und DSGVO)
Cyril Rohr EIRL 99 rue de la rabine 35510 CESSON-SÉVIGNÉ, France	Consulting DevOps und Continuous Delivery, Erstellung von Software-Paketen	Standard data protection clauses (Art. 46 Abs. 2 litt. c und DSGVO)
Forkmerge SL C/ Guillem Massot, 44, Piso 3 07003 Palma de Mallorca, Spain	Consulting Software Entwicklung	Standard data protection clauses (Art. 46 Abs. 2 litt. c und DSGVO)
Thomas Gerstmann Saastraße 84 52062 Aachen, Germany	Consulting User Experience	Standard data protection clauses (Art. 46 Abs. 2 litt. c und DSGVO)
MessageBird B.V. Baarsjesweg 285-H 1058 AE Amsterdam, Netherlands	Übermittlung von Authentifizierungstoken per SMS oder Sprachanruf für die Zweifaktor-Authentifizierung	Standard data protection clauses (Art. 46 Abs. 2 litt. c und DSGVO)
Mailchimp The Rocket Science Group, LLC	Versand von E-Mail-Benachrichtigungen (Produktinformationen, Newsletter,	Standard data protection clauses (Art. 46 Abs. 2 litt. c

675 Ponce De Leon Ave NE Atlanta, GA 30308, USA	Sicherheits-Benachrichtigungen etc.)	und DSGVO)
PipeDrive 460 Park Ave South New York, NY 10016, USA	Verwaltung von Angebots-anfragen von Kunden	Standard data protection clauses (Art. 46 Abs. 2 litt. c und DSGVO)
Sendgrid Inc. 1801 California St Denver, CO 80202, USA	Versand von E-Mail-Benachrichtigungen	Standard data protection clauses (Art. 46 Abs. 2 litt. c und DSGVO)