Supplementary agreement on contract data processing

Name: _____

Street: _____

City, postcode: _____

Country: _____

- Client -

and

OpenProject GmbH

Karl-Liebknecht-Str. 5

10178 Berlin

Germany

- Contractor -

conclude the following agreement on the processing of the Client's data by the Contractor:

Preamble

This Agreement, together with its appendices, specifies the contracting parties' data protection obligations resulting from the contract data processing described in detail in the service or framework agreements. It applies for all activities directly or indirectly related to the service or framework agreements.

§ 1. Area of application and responsibility

(1) The object of the contract is activities specified in the service agreement and the product descriptions.

(2) It is possible that the Contractor may be able to view the Client's data while performing maintenance or other work as part of hosting the OpenProject software. This data may be so-called personal data, which by law is subject to special confidentiality and must be treated confidentially by the Contractor.

(3) The Client's customers, employees, contacts, suppliers, etc. are affected by the data processing, depending on the scale on which the Client processes data with the OpenProject software.

(4) The Client is solely responsible for evaluating whether the collection, processing and use of personal data by the Contractor within the bounds of the contractual relationship is legally admissible under the provisions of the Bundesdatenschutzgesetz [German Federal Data Protection Act] (BDSG) and other applicable data protection regulations.

§ 2. Type of data and group of persons affected

(1) This data protection agreement is being concluded between the Client and the Contractor because access to personal data and data regarding operations and business process (hereinafter referred to as data) is sometimes required for the purpose of the agreed services or cannot be ruled out.

(2) This Agreement governs the protection of data while executing contracts in special consideration of the requirements of the German Federal Data Protection Act. The type of data and the group of persons affected depends on the service agreements concluded.

§ 3. The Client's duties

(1) The Client is responsible for all data, automated procedures and data processing equipment within its remit; it is also responsible for safeguarding the rights of the persons affected.

(2) The Client must take the technical and organisational measures required to guarantee data protection and data security while executing the contract. The nature and scale of the work as well as the authorisation granted to the Contractor's personnel must be adequately defined.

(3) The Client has the right to give instructions on the nature, scale and sequence of the work; they must be given in writing. Oral instructions must be confirmed immediately in writing.

(4) The Client will monitor the implementation of this Agreement and inform the Contractor immediately of any errors or irregularities they identify.

(5) The Client must inform the Contractor in writing of the persons authorised to give instructions, the authorised recipients and those authorised to perform inspections. These parties must prove their identity when exercising their authority.

§ 4. The Contractor's duties

(1) The Contractor shall render the contractually agreed services properly and in accordance with data protection requirements. The Contractor is only permitted to use the data within the bounds of the contract stated in Section 1 (1), in line with the Client's written instructions and in accordance with data protection

regulations. The Contractor shall amend, delete or block personal data in accordance with this Agreement or when instructed to do so by the Client.

(2) The Contractor shall inform the Client immediately of enquiries made by regulatory bodies, persons affected and other third parties, if these affect the Client. The Contractor shall forward all enquiries to the Client and assist the Client with handling these enquiries.

(3) In accordance with Section 4f BDSG, the Contractor must appoint a company data protection officer and provide his contact details to the Client immediately in Appendix 2 (Appendix 2: the data protection officer's contact details). If the data protection officer changes, notification must be given immediately in writing. To maintain the skills required to perform his role, the data protection officer must undergo adequate training at regular intervals.

(4) The Contractor acknowledges and understands that the Client and their relevant regulatory bodies may, using the means specified in Section 38 (3) to (5) BDSG, check or commission a third party to check that the provisions relating to data protection are being complied with and that additional instructions are being followed, if it is necessary to do so during the contract in order to monitor data protection. Checks may be performed within the Contractor's normal business hours with ten (10) working days' notice in advance. The dates will be set by mutual arrangement between the parties. The Client shall bear the costs of any commissioned third parties. By mutual agreement, an on-site inspection by the Client may be replaced by presenting an inspection report.

(5) To act in accordance with the contract and perform the tasks required to fulfil the contract specified in Section 1, the Contractor shall only appoint persons who have pledged in writing to observe data privacy in accordance with Section 5 BDSG; it is advised that a breach of data privacy may result in criminal liability. The letter of undertaking must be provided at the Client's request. The Contractor shall also ensure that its personnel are carefully selected and also adequately informed and briefed with regard to data protection regulations. In particular, the Contractor must ensure that persons who obtain information pertaining to the Client do not pass this on to third parties or use it in any other way.

(6) In accordance with the annex to Section 9 BDSG, technical and organisational measures have been defined and are described in Appendix 1 (Appendix 1: Technical and organisational measures) of this document. The Contractor has enclosed the measures taken by it as Appendix 1. The Client reserves the right to examine the measures specified and stipulate additional measures which the Contractor must implement. The Contractor shall ensure that the agreed organisational and technical measures will be complied with as stipulated.

(7) The Contractor will only use the data it obtains while executing the order to perform the contractually agreed tasks. It will not pass it on to third parties. It will store it securely, but only for as long as it is required to fulfil the contract stated under Section 1 (1). If there are legal retention periods which prevent the data

from being deleted, any use of it must be prevented and it must be deleted after the retention period expires without this being requested. The Client may stipulate provisions deviating from clauses 1 to 3 in writing.

(8) Sole ownership and usage rights over the data remain with the Client. When the contractual relationship is terminated or in accordance with relevant agreements in a particular case, the Contractor shall return to the Client all documents it has obtained and data which has been provided to it, together with the products of all processing and use, relating to the contractual relationship, in a format agreed upon with the Client. The Contractor's relevant data storage devices must then be physically cleared.

(9) The Contractor shall take suitable measures to ensure that only persons who are entrusted with the contractual performance of the work have access to the Client's data.

(10) The Contractor shall not produce any copies or duplicates of the data provided to it without the Client's knowledge or for any purposes other than those agreed by contract.

(11) The Contractor shall inform the Client immediately of any suspicion of data protection breaches or other irregularities which occur when performing the work. If the Customer's data which is held by the Contractor is put at risk by third-party actions (e.g. attachment or seizure), insolvency or composition proceedings or other events, the Contractor must inform the Customer of this immediately, if the security measures taken by the Contractor do not meet the Client's requirements. If the Contractor believes that an instruction given by the Client would lead to a violation of the law, it shall inform the Client accordingly. The instruction does not need to be followed until the Client has amended it or expressly confirmed it.

§ 5. Subcontractors

(1) The Contractor is permitted to commission subcontractors if the subcontractors are subject to the same contractual data protection provisions as the Contractor.

(2) The Contractor must select the subcontractors carefully and, before commissioning them, check that they are able to comply with the agreements made between the Client and the Contractor. In particular, the Contractor must check in advance and at regular intervals for the duration of the contract that the subcontractor has taken the technical and organisational measures required in accordance with Section 9 BDSG to protect personal data.

(3) Subcontracting within the context of this provision does not mean those services offered by third parties which the Contractor commissions as supplementary work to assist it with executing the contract. For example, this includes telecommunications services, cleaning and auditors. However, the Contractor is obligated to make reasonable and lawful contractual agreements and perform checks to ensure the protection and security of the Client's data, even for supplementary work contracted out externally.

§ 6. Confidentiality obligations

(1) Both parties undertake to indefinitely treat all information which they obtain in connection with executing this contract as confidential and to use it only to execute the contract. Neither of the parties may use this information, in full or in part, for purposes other than those just mentioned or disclose this information to third parties.

(2) This obligation does not apply to information if it can be proven that one of the parties has obtained this information from a third party where there is no obligation to maintain confidentiality or if this information is public knowledge.

§ 7. Duration of the contract

(1) This data protection agreement will remain in force for as long as the contracts stated under section 1 remain valid. The confidentiality obligation extends beyond the end of the contract.

(2) The breach of legal or contractual data protection provisions by the Contractor always constitutes good cause for the Client to exercise their right reserved in the contractual agreements to extraordinarily terminate the contract stated under section 1.

§ 8. Severability clause

(1) If one or more provisions of this agreement is/are or becomes/become wholly or partly invalid, this does not affect the validity of the remaining provisions of this agreement.

§ 9. Final provisions

(1) Amendments or additions to this Agreement must be made in writing and signed by both contracting parties. This also applies to the amendment of this written form clause. Email is not considered written form.

(2) The defence of right of retention pursuant to Section 273 BGB (Bürgerliches Gesetzbuch [German Civil Code]) with regards to the processed data and the associated data storage devices is excluded.

§ 10. Entry into force

(3) This Agreement will enter into force once it has been signed.

_____ , _____		_____ , _____	
Place	Date	Place	Date
_____		_____	
- Client -		- Contractor -	

Appendix 1: Technical and organisational data security measures

The data security measures defined by the Contractor in this appendix are considered binding.

a) Entry control

The Contractor processes data in a secure data processing centre. The data processing centre is certified in accordance with standard ISO 27001 for its information security management system. Entry to the data processing centre is secured by the latest control systems. This includes the following security measures and infrastructures:

- Division of the facilities into specific secure areas,
- Physical entry management, e.g. steel doors, windowless rooms or secured windows,
- Protection of secure areas by electronic access control system,
- Surveillance of the facility by security services and recording of access,
- Video surveillance of all security-related areas such as entrances, emergency exits and server rooms,
- Centralised granting and revocation of access rights,
- Identification of all visitors using personal ID,
- Identification requirement within secure areas for all employees and visitors,
- Constant supervision of visitors by employees.

b) Access control

The Contractor must prevent all unauthorised parties from accessing systems and applications which are used to process personal data. The Contractor guarantees this by giving only expressly authorised administrators access to the IaaS provider's data processing systems. Log-in is exclusively via multi-factor authentication using the log-in information stored in the relevant personal user account. A sophisticated rights system based on security groups and access control lists is also used. Log-in is only possible over connections which are encrypted using the latest technology.

To secure access further, the individual services and components are divided into multiple network segments. Isolation is enabled by hardware firewall systems and virtual private clouds (VPCs). All access to systems and applications is documented, monitored and recorded centrally.

The internal network is protected against unauthorised access from outside by a hardware firewall. Access to computers in the Contractor's premises is controlled via user accounts. The internal network can only be accessed from outside the premises via an encrypted VPN (virtual private network) connection.

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

c) Access control

The Contractor must prevent illegal activities within the data processing systems. As a result, only the client concerned and a small group of individually appointed administrators have access to the data. It is technologically ensured that one client cannot see, amend or delete another client's data. Within OpenProject, access is controlled using a comprehensive role and authorization concept. Rights are granted within OpenProject by the Client by assigning roles and rights. The Client also has the option to adapt the preconfigured roles and rights for their organisation via an administration interface to meet their needs.

Access to the Client's data for the Contractor's customer service staff is limited to basic data and billing data, which is required for them to perform their customer service duties and for billing for the hosting service. Customer service staff do not have access to customer data within OpenProject.

Customers' credit card details are only stored by the payment service providers; the Contractor does not have access to this data.

Administrators are only permitted to access customer data if there is a fault which cannot be resolved by the Client and/or the Contractor's customer service staff alone.

d) Disclosure control

Control over disclosure of the Client's data is guaranteed by various technical and organisational security measures. In principle, the Contractor does not process or store the Client's data outside of the data processing centre either. Employees of the data processing centre operator cannot enter the data processing centre or access customer data; they cannot view, delete or amend it either. Data backups are always encrypted. The Client's data is never transported on physical data storage devices. Billing data is transmitted via an encrypted connection to the Contractor's accounting systems for the purpose of billing for the service.

e) Input control

The Contractor must ensure that data processing is comprehensible and documented. For this purpose, all entries in the systems and applications are recorded by the Contractor. The records are archived and deleted once they have served their purpose or in accordance with legal requirements. The OpenProject application only supports the entry and amendment of data via a user interface intended for this purpose and interfaces in accordance with a detailed role and authorisation concept. For many objects, the Client can also see the revision history for data (e.g. work packages, wiki pages, SCM repositories) via the web interface.

f) Contract control

The Contractor shall process the data provided in accordance with the contract concluded and, by doing so, guarantees compliance with legal requirements and requirements defined by contract in line with the Client's instructions. The OpenProject platform has an administration interface via which the Client can manage their client account. The Client enters their own access details into their user account during initial set-up. Only those who have these access details can enter, amend or delete customer data with the assigned authorisation. Other tasks which the Client cannot perform themselves via the administration interface must be performed in writing.

g) Availability control

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

A comprehensive security and recovery concept has been implemented to prevent the loss of data. The Client's data is continuously backed up using a duplication mechanism in a separate availability zone. Full backups of all systems and data are also produced daily.

The systems and applications are continuously monitored with regard to availability, functionality, security and capacity. There is a written contingency plan to restore the backups in the event of loss or destruction.

h) Partitions

All data records which are collected, processed or used by the Contractor's systems and applications are explicitly and unambiguously assigned to the relevant client and technically separated from other data. The Contractor's data processing systems are specially geared towards purpose-specific and client-separate processing. Access to another client's data is thus technically impossible.

Appendix 2: Contact details of the company data protection officer

The company data protection officer is:

Mr Ingo Wolff
Tacticx GmbH
Walbecker Straße 53
47608 Geldern, Germany