Data processing agreement

in accordance with Art. 28

of the General Data Protection Regulation (DSGVO)

between

much. GmbH   Name
Marcel-Breuer-Straße 17   Street Number
80807 München   ZIP City

and

–Contractor–   –Customer–

1.   **Subject and duration of the contract**

The subject and duration of the order shall be determined by the contract concluded between the parties (hereinafter referred to as the "Main Contract").

2.   **Scope, nature and purpose of data processing**

The activity of the Contractor serves the purpose of providing the Customer with various services regarding the hosting of the ERP platform Odoo as well as services thereon and shall be provided by the Contractor to the extent agreed in the main contract. In this context, the Contractor shall provide the following services:

(Please tick)

☐   Hosting of an Odoo platform

☐   Services on the client's Odoo systems

3.   **Data types**

In principle, all types of data processed by means of the client's IT systems may be affected by the assignment. This applies in particular, but not conclusively, to the following types of data:

- Name
- Email
- Address & Location
- Usage behavior
- Purchases & Payments
- Salary
- Device Information
- Communications Data
- Phone number
- any other data stored on the client's Odoo platform, if applicable

4.   **Groups of affected persons**

In principle, all persons whose personal data is processed by means of the Client's IT systems may be affected by the data processing. This applies in particular, but not conclusively, to the following persons:

- Employees of the client
- Customers of the client
- Users of the client
- Interested parties of the client
- Suppliers of the client
- all other persons whose personal data may be stored on the client's Odoo platform

5. Subject of contract

Within the scope of the provision of services under the Main Agreement, it is necessary for the Contractor to handle personal data of third parties for which the Customer acts as the responsible body within the meaning of the data protection regulations (hereinafter referred to as "**Customer Data**"). This contract specifies the rights and obligations of the parties under data protection law as well as those resulting from the special position of the Client as a professional secrecy holder in connection with the Contractor's handling of Client Data for the fulfillment of the main contract.

6. Scope of the assignment

6.1.   The Contractor shall process the Client Data on behalf of and in accordance with the instructions of the Client within the meaning of Art. 28 DSGVO (commissioned processing). The Client shall remain the responsible party in the sense of data protection law.

6.2.   The processing of the Client Data by the Contractor shall take place within the Federal Republic of Germany. The Contractor is nevertheless permitted to process Client Data outside the EEA in compliance with the provisions of this Agreement if it informs the Client in advance of the location of the data processing and the requirements of Art. 44 - 48 DSGVO are met or an exception pursuant to Art. 49 DSGVO applies.

7. Directive authority of the client

7.1.   The Contractor may process the Client Data exclusively on behalf of and in accordance with the instructions of the Client, unless the Contractor is required by law to process them otherwise. In the latter case, the Contractor shall notify the Client of such legal requirements prior to processing, unless the relevant law prohibits such notification due to an important public interest.

7.2.   The Customer shall have a comprehensive right to issue instructions to the Contractor regarding the type, scope, purpose and procedure of the processing of Customer Data. The Client's instructions shall generally be given in writing or text form. If necessary, the Customer may also issue instructions orally or by telephone. However, instructions given orally or by telephone shall require immediate confirmation by the Customer in writing or text form. The Contractor shall be obliged to document all instructions of the Customer.

7.3.   Instructions shall generally be provided by the Client's project contact person(s) to the Contractor's project contact person(s). In urgent cases, however, any other employee of the Client may also issue corresponding instructions to any other employee of the Contractor, provided that the project contact person on the side of the Contractor was not available.

7.4.   The Contractor shall carry out the Customer's instructions without delay. The Customer shall be entitled to set the Contractor a reasonable deadline for this in each individual case.

7.5.   The Contractor warrants that it will process the Customer Data in accordance with the provisions of this Agreement and the Customer's instructions. If the Contractor is of the justified opinion that an instruction of the Customer violates this Agreement or the applicable

data protection law, it shall notify the Customer thereof without undue delay. The Contractor shall be entitled to suspend the execution of the instruction until confirmation or amendment of the instruction by the Customer after giving the Customer at least 14 days' prior notice.

7.6. If it is unreasonable for the Contractor to carry out an instruction of the Client, the Contractor shall be entitled to terminate the main contract and this contract extraordinarily.

8. Responsibility of the customer

8.1. The Customer shall be responsible for the lawfulness of the processing of the Customer Data and for safeguarding the rights of the data subjects. Should third parties assert claims against the Contractor based on the processing of Customer Data in accordance with this Agreement, the Customer shall indemnify the Contractor against all such claims.

8.2. The Customer shall be responsible for providing the Contractor with the Customer Data in a timely manner for the performance of services under the Main Agreement and shall be responsible for the quality of the Customer Data. The Client shall inform the Contractor without undue delay if it discovers errors or irregularities with regard to data protection provisions or its instructions during the review of the Contractor's order results.

8.3. If the Contractor is under an obligation to a government agency or person to provide information about the processing of Client Data or to otherwise cooperate with such agencies, the Client shall assist the Contractor in providing such information or in fulfilling other obligations to cooperate.

9. Processing security

9.1. In accordance with Article 32 of the DSGVO, the Contractor shall take the necessary, appropriate technical and organizational measures, which are required taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing of the Client Data and the varying likelihood and severity of the risk to the rights and freedoms of the data subjects, in order to ensure a level of protection for the Client Data that is appropriate to the risk. The technical organizational measures of the Contractor used at the time of the conclusion of the contract are detailed in Annex 2.

9.2. The Contractor is permitted to change or adapt technical and organizational measures during the term of the contract as long as they continue to meet the legal requirements.

10. Use of other processors

10.1. The Customer hereby grants the Contractor general approval to involve further processors with regard to the processing of Customer Data. The further processors involved at the time of conclusion of the contract are shown in Annex 1. Contractual relationships with service providers which have as their object the testing or maintenance of data processing procedures or systems by other bodies or other ancillary services are generally not subject to approval, even if access to Customer Data cannot be excluded in the process, as long as the Contractor makes appropriate arrangements to protect the confidentiality of the Customer Data.

10.2. The Contractor shall inform the Customer of any intended changes with regard to the involvement or replacement of further processors. In individual cases, the Customer shall have the right to object to the commissioning of a potential additional processor. An objection may only be raised by the Customer for good cause to be proven to the Contractor. If the Customer does not raise an objection within 30 days after receipt of the notification, its right of objection with regard to the corresponding commissioning shall expire. If the Customer raises an objection, the Contractor shall be entitled to terminate the main contract and this contract with a notice period of 3 months.

10.3. The contract between the contractor and the additional processor must impose the same obligations on the latter as are imposed on the contractor by virtue of this contract. The parties agree that this requirement is met if the contract has a level of protection corresponding to this contract or if the obligations set out in Article 28(3) of the DSGVO are imposed on the further processor.

11. Data subject rights

11.1. The Contractor shall support the Customer with technical and organizational measures in fulfilling its obligation to respond to requests to exercise the rights of data subjects to which they are entitled.

11.2. Insofar as a data subject asserts a request to exercise the rights to which he or she is entitled directly against the Contractor, the Contractor shall forward this request to the Customer.

11.3. The Contractor shall provide the Customer with information about the stored Customer Data, the recipients of Customer Data to whom the Contractor passes it on in accordance with the order, and the purpose of the storage, insofar as the Customer does not have this information itself or is unable to obtain it itself.

11.4. The Contractor shall enable the Customer to correct, delete or restrict the further processing of the Customer Data or, within the scope of what is reasonable and necessary, to carry out the correction, blocking or restriction of further processing itself at the request of the Customer against reimbursement of the expenses and costs to be proven incurred by the Contractor as a result, if and to the extent that this is impossible for the Customer itself.

11.5. Insofar as the data subject has a right to data portability with respect to the Customer Data pursuant to Art. 20 DSGVO, the Contractor shall support the Customer within the scope of what is reasonable and necessary in providing the Customer Data in a common and machine-readable format in exchange for reimbursement of the efforts and costs incurred by the Contractor in this regard, if the Customer cannot obtain the data otherwise.

12. Notification and support obligations of the Contractor

12.1. Insofar as the Customer is subject to a statutory obligation to report or notify a breach of the protection of Customer Data (in particular pursuant to Art. 33, 34 DSGVO), the Contractor shall inform the Customer of any reportable events in its area of responsibility. The Contractor shall support the Customer in fulfilling the reporting and notification obligations at the Customer's request within the scope of what is reasonable and necessary in return for

reimbursement of any expenses and costs to be proven incurred by the Contractor in this regard.

12.2. The Contractor shall support the Customer within the scope of what is reasonable and necessary against reimbursement of the expenses and costs to be proven incurred by the Contractor in connection with any data protection impact assessments to be carried out by the Customer and any subsequent consultations with the supervisory authorities pursuant to Art. 35, 36 DSGVO.

13. Data deletion

13.1. The Contractor shall delete the Customer Data 30 days after termination of this Agreement, unless the Contractor is legally obliged to continue storing the Customer Data. If the Customer has commissioned the Contractor with hosting services, the Customer shall have the option at any time beforehand to download all data processed by the Contractor and covered by the contract in the so-called self-service.

13.2. Documentation that serves as proof of the proper processing of customer data in accordance with the contract may be retained by the contractor even after the end of the contract.

14. Proofs and verifications

14.1. The Contractor shall provide the Customer, upon the Customer's request, with all information necessary and available to the Contractor to demonstrate compliance with its obligations under this Agreement.

14.2. The Customer shall be entitled to check the Contractor with regard to compliance with the regulations of this Agreement, in particular the implementation of the technical and organizational measures; including by means of inspections.

14.3. In order to carry out inspections in accordance with Section 14.2, the Customer shall be entitled to enter the Contractor's business premises where Customer Data are processed during normal business hours (Monday to Friday from 10 a.m. to 6 p.m.) after timely advance notice in accordance with Section 14.5 at its own expense, without disrupting operations and subject to strict confidentiality of Contractor's trade and business secrets.

14.4. The Contractor shall be entitled, at its own discretion, taking into account the Customer's legal obligations, not to disclose information which is sensitive with regard to the Contractor's business or if the Contractor would violate legal or other contractual regulations by disclosing it. The Customer shall not be entitled to have access to data or information on other customers of the Contractor, to information regarding costs, to quality review and contract management reports and to any other confidential data of the Contractor which is not directly relevant for the agreed review purposes.

14.5. The Customer shall inform the Contractor in good time (as a rule at least two weeks in advance) of all circumstances connected with the performance of the inspection. The customer may carry out one inspection per calendar year. Further inspections shall be carried out against reimbursement of costs and after coordination with the Contractor.

14.6. If the Customer commissions a third party to carry out the inspection, the Customer shall oblige the third party in writing in the same way as the Customer is obliged towards the Contractor on the basis of this Clause 14 of this Agreement. In addition, the Customer shall oblige the third party to maintain secrecy and confidentiality, unless the third party is subject to a professional confidentiality obligation. Upon request of the Contractor, the Customer shall immediately submit to the Contractor the obligation agreements with the third party. The Customer may not commission any competitor of the Contractor with the inspection.

14.7. At the Contractor's discretion, proof of compliance with the obligations under this Agreement may also be provided by the submission of a suitable, up-to-date attestation or report by an independent body (e.g., auditor, audit, data protection officer, IT security department, data protection auditors or quality auditors) or a suitable certification by IT security or data protection audit - e.g., in accordance with BSI-Grundschutz - ("audit report") instead of an inspection, if the audit report reasonably enables the Customer to satisfy itself of compliance with the contractual obligations.

15. Contract duration and termination

The term and termination of this Agreement shall be governed by the provisions governing the term and termination of the Main Agreement, unless otherwise provided in this Agreement. Termination of the main contract shall automatically result in termination of this contract. An isolated termination of this contract is excluded.

16. Liability

16.1. The exclusions and limitations of liability pursuant to the main contract shall apply to the Contractor's liability under this contract. Insofar as third parties assert claims against the Contractor which have their cause in a culpable breach by the Customer of this Agreement or of one of its obligations as a data protection officer, the Customer shall indemnify the Contractor against these claims upon first request.

16.2. The Customer undertakes to indemnify the Contractor also against any fines imposed on the Contractor to the extent that the Customer bears a share of the responsibility for the violation sanctioned by the fine.

16.3. **Miscellaneous**

16.4. If individual provisions of this contract are or become invalid or contain a loophole, this shall not affect the remaining provisions. The parties undertake to replace the invalid provision with a legally permissible provision that comes as close as possible to the purpose of the invalid provision and meets the requirements of Article 28 of the DSGVO.

16.5. In case of contradictions between this contract and other agreements between the parties, in particular the main contract, the provisions of this contract shall prevail.

Ort / Place: _____   Ort / Place: München

Datum / Date: _____   Datum / Date: _____

_____   _____

Contractor   Customer

List of Annexes:

Annex 1 Other processors

Annex 2 Technical and organizational measures according to Art. 32 DSGVO

Annex 1

Further processors

At the time of the conclusion of the Contract, the Contractor shall use the following (additional) Processors to provide its services:

Processor	Purpose of use	Location of the Processor
Hetzner Online GmbH Industriestr 25 91710 Gunzenhausen	Hosting and provision of data center services	Germany
Manvetipon - Unipessoal LDA, Av. Fontes Pereira de Melo 3, 1050-005 Lisboa, Portugal	Providing services according to the main contract	Portugal

Annex 2

Technical and organizational measures

according to Art. 32 DSGVO

At the time of the conclusion of the contract, the Contractor has implemented the following technical organizational measures.

Furthermore, all hosting offers are operated in data centers of Hetzner Online GmbH. Detailed information on access, access control, data carrier control, separation control, integrity, availability, resilience can also be found in Hetzner's ToMs at https://www.hetzner.com/AV/TOM.pdf.

I. Purpose limitation and separability
The following measures ensure that data collected for different purposes is processed separately:
- Logical client separation (on the software side) through virtual servers per customer Authorization concept
- Separation of productive and test system on different virtual servers

II. confidentiality and integrity

The following measures ensure the confidentiality and integrity of the Processor's systems:

1. encryption
The data or data carriers processed in the order shall be encrypted in the following manner: Use of Secure Sockets Layer for communication via the Internet, as long as this is supported by the Customer.

2. Pseudonymization
"Pseudonymization" means that personal data are processed in a way that excludes the identification of the data subject without the addition of further information (e.g., use of fantasy names that cannot be attributed to a specific person without additional information without additional information).
- No. The customer is responsible for the pseudonymization of his data in the applications himself.

3. the following measures have been taken to prevent unauthorized persons from gaining access to the data processing systems with which personal data are processed or used (access control):

In the data center at Hetzner Online GmbH:
- Electronic access control system with logging
- High security fence around the entire data center park
- Documented key assignment to employees and colocation customers for colocation racks
- Guidelines for escorting and tagging guests in the building
- 24/7 staffing of the data centers
- Video surveillance at entrances and exits, security gates and server rooms
- Access to the rooms for persons outside the company (e.g. visitors) is restricted as follows: only in the company of a Hetzner Online GmbH employee

In the office:
- Chip card/transponder locking system
- Video surveillance of the accesses
- Key control (key issue etc.)
- Careful selection of cleaning personnel

4. the following measures have been taken to prevent the use of the data systems by unauthorized third parties (access control):
- Assignment of user rights, assignment of user profiles to IT systems
- Creation of user profiles, authentication with user name / password, password assignment, password policies
- RSA encrypted SSH keys for servers
- Key regulation (key issuance etc.)
- Careful selection of cleaning personnel
- Use of anti-virus software
- Use of software firewall

5. the following measures have been taken to ensure that those authorized to use a data processing system can access only the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage (access control):
- Separation of customers into own virtual server
- Authorization concept
- Administration of rights by system administrator
- Regular checking and updating of access rights (especially when employees leave the company or similar)
- Number of administrators is reduced to the "bare minimum
- Password policy incl. password length

(6) The following measures can be used to check and determine retrospectively whether and by whom personal data have been entered into, modified or removed from data processing systems (input control).
- Assignment of rights to enter, change and delete data on the basis of an authorization concept

7. the following measures ensure that personal data processed on behalf of the customer can only be processed in accordance with the customer's instructions (order control).
- Selection of the processor under due diligence aspects (in particular with regard to data security).
- written instructions to the processor (e.g. by means of a processing contract)
- Obligation of the processor's employees to maintain data secrecy
- Processor has appointed data protection officer
- Ensuring the destruction of data after termination of the order

8. the following measures ensure that personal data cannot be obtained or viewed by unauthorized persons during transfer (physical and/or digital) (transport or transfer control):
- Use of SSH tunnels
- Encryption of physical data carriers at TransporteRecht24. All rights reserved.

III. availability, recoverability and resilience of the systems
The following measures ensure that the data processing systems used function properly at all times and that personal data are protected against accidental destruction or loss
- Regular updates of the operating systems and of our provided software.
- Daily backups with storage on the client's server and 2 other backup systems. At least five backups are kept at all times. The customer is responsible for making their own copies of the backups.
- Odoo backups are provided complete and installable

IV. Special data protection measures
No special data protection measures were taken.

V. Review, evaluation and adaptation of the present measures
The Processor shall review, evaluate and, if necessary, adapt the technical and organizational measures set forth in this Annex at its discretion or as required.