Order according to Art. 28 DS-GVO

agreement

between

XXXX

- hereinafter referred to as the principal -

and

Continux GmbH,
Landshuter Allee 10,
80637 Munich

- hereinafter referred to as contractor –

1. Subject and duration of the contract
The subject matter and the duration of the contract are determined in their entirety according to the information given in the respective contractual relationship.

The contractor processes personal data for the client i.S.v.Art.4 Nr.2 and Art.28 DS-GVO on the basis of this order.

2. Scope, nature and purpose of the collection, processing or use of data
The scope, nature and purpose of any collection, processing or use of personal data, the nature of the data and the circle of data subjects shall be described to the contractor by the contracting authority in accordance with Annex 1 completed by the contracting entity, insofar as this does not result from the contract in paragraph 1.

The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another Contracting State to the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 et seq. DS-GVO are met.

3. Technical-organizational measures according to Art. 32 DS-GVO (Art. 18 (3) sentence 2 lit.c DS-GVO)
(1) The contractor shall document the implementation of the technical and organizational measures set out prior to the award of the contract and prior to processing, in particular with regard to the specific execution of the contract, and submit them to the client for review (see Annex 2). If accepted by the client, the documented measures become the basis of the order.
(2) The contractor has the security gem. Art. 28 (3) sentence 2 lit.c, 32 DS-GVO
in particular in conjunction with Article 5 (1) (2) DS-GVO. Overall, the actions to be taken are data security measures and to ensure a level of protection appropriate to the level of risk with regard to the confidentiality, integrity, availability and resilience of the systems. In this context, the state of the art, the implementation costs and the type, scope and purpose of the processing as

well as the different probability and severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 DS-BER must be taken into account.

(3) The technical and organizational measures are subject to technical progress and further development. In that regard, the contractor is allowed to implement alternative adequate measures. At the same time, the safety level of the specified measures must not be undershot. Significant changes must be documented.

4. Correction, blocking and deletion of data
(1) The contractor shall not delete or restrict the processing of the data processed in the order on its own initiative. Insofar as an affected person directly addresses the contractor in this regard, the contractor will immediately forward this request to the client.

(2) Insofar as included in the scope of services, the contractor shall ensure the cancellation concept, right to be forgotten, rectification, data portability and information according to the client's documented instructions.

5. Quality assurance and other obligations of the contractor
The contractor has in addition to the compliance with the regulations of this contract legal obligations according to Art. 28 to 33 DS-GVO; In particular, it ensures compliance with the following requirements:

• The preservation of confidentiality pursuant to Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR.
The contractor only employs employees when carrying out the work one committed to the confidentiality and previously with the relevant for them Privacy Policy. The contractor and any person subject to the contractor who has access to personal information Data may only be used in accordance with the instructions of the Client, including those granted in this Agreement Powers, unless they are required by law to process.

• The implementation and compliance with all necessary for this order technical and organizational measures comply with Art. 28 para. 3 sentence 2 lit. c, 32 DSGVO and Annex 2.

• The client and the contractor work with the Supervisory authority in the performance of their duties together.

• The immediate information of the client about control actions and Measures taken by the supervisory authority insofar as they relate to this mandate. This shall also apply, to the extent that a competent authority contributes to the processing of personal data in the context of an administrative offense or criminal proceedings order processing at the contractor.

• If the principal for its part is subject to inspection by the supervisory authority, a Administrative offense or criminal proceedings, the liability claim of an affected party Person or a third party or other claim in connection with the Order processing is suspended at the contractor, the contractor has him

to support to the best of our ability.

• The contractor regularly checks the internal processes as well as the technical and organizational measures to ensure that the Processing in his area of responsibility in accordance with the requirements of the applicable data protection legislation and the protection of the rights of the data subjects Person is guaranteed.

• Documentation of the technical and organizational measures taken towards the client also available on the website

6. Subcontracting
For the purposes of this regulation, subcontracting means such services that directly relate to the provision of the main service. This does not include ancillary services provided by the contractor, e.g. as telecommunication services, postal / transport services, maintenance and user service as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing facilities. The contractor is however committed to ensuring the privacy and data security of the data of the client even with outsourced ancillary services to take appropriate and legally compliant contractual arrangements and control measures.

7. Control rights of the client
(1) The client shall have the right to carry out inspections in consultation with the contractor or to have them carried out by examiners to be named in individual cases. He has the right to satisfy himself of the compliance of this agreement by the contractor in his business through spot checks, which are usually to be registered in good time.

(2) The contractor shall ensure that the client can satisfy himself of the compliance with the obligations of the contractor in accordance with Art. 28 DS-GVO. The contractor undertakes to provide the client with the necessary information upon request and, in particular, to prove the implementation of the technical and organizational measures.

(3) The proof of such measures, which do not concern only the concrete order, Optionally, it can be done by following approved behavioral rules Art. 40 DS-GVO, the certification according to an approved certification procedure according to Art. 42 GDPR, current certificates, reports or report extracts of independent bodies (eg auditors, auditors, data protection officers, IT security department, privacy auditors, quality auditors) and / or a suitable certification by IT security or data protection audit (eg according to BSI) basic protection).

(4) The contractor may assert a claim for compensation in order to allow controls by the client.

8. Notification in case of violations of the contractor

1. The contractor shall assist the contracting authority in complying with the obligations on security of personal data, reporting of data breaches, data protection impact assessments and prior consultations, as referred to in Articles 32 to 36 of the GDPR. These include u.a.

(a) ensuring an adequate level of protection through technical and technical means; organizational measures affecting the circumstances and purposes of the processing as well as the predicted probability and severity of a possible Infringement due to security vulnerabilities and immediate Enable detection of relevant injury events
(b) the obligation to immediately disclose personal data breaches to the Client to report
c) the obligation to the client in the context of his duty to inform to assist the person concerned and him in this context to provide all relevant information without delay
d) the client's support for their privacy impact assessment
(e) the assistance of the contracting authority in the context of prior consultations with the supervisory authority

(2) For services that are not included in the terms of reference or are not the result of a wrongdoing by the contractor, the contractor may claim a fee.

9. Authorization of the client
(1) Verbal instructions are confirmed immediately by the client (at least in text form).

(2) The contractor must inform the client immediately if he believes that an instruction violates data protection regulations. The contractor is entitled to suspend the execution of the relevant instruction until it has been confirmed or changed by the client.

10. Deletion and return of personal data
(1) Copies or duplicates of the data are not created without the knowledge of the client. This does not include backup copies, to the extent necessary to ensure proper data processing, and data required for compliance with statutory retention requirements.
(2) After the conclusion of the contractually agreed work or sooner upon request by the client - at the latest upon termination of the service agreement - the contractor shall have received all documents, processing and utilization results as well as data sets which are related to the contract To hand over client or destroy it after prior consent in accordance with data protection. The same applies to test and scrap material. The contractor will inform the client on request about the nature and the time of deletion.

(3) Documentation that proves the orderly and proper
Data processing shall be retained by the contractor according to the respective retention periods beyond the end of the contract. He can hand them over to the client for discharge at the end of the contract.

11. Other agreements

11.1. charges
A fee for this order is not required.

Insofar as the client requires support according to Section 4 for answering inquiries from those

affected, he shall reimburse the costs incurred as a result. Insofar as the client exercises control rights in accordance with clause 7, the amount of the fee to be agreed in advance shall be based on a fixed hourly rate of the employee assigned to the contractor for support.

If the client issues instructions to the contractor in accordance with Section 9, he must reimburse costs incurred by this instruction.

11.2. Contract duration
This Agreement is dependent on the existence of a Principal Contractual Relationship pursuant to Number 1. The termination or other termination of the Principal Contractual Relationship pursuant to Number 1 shall terminate this Agreement at the same time.

The right to isolated, extraordinary termination of this agreement and the exercise of legal rights of withdrawal specifically for the agreement remain unaffected.

11.3. choice of law
The law of the Federal Republic of Germany.

11.4. jurisdiction
The parties agree as the place of jurisdiction of the seat of the responsible for Munich Court.

Place and Date

Principal	Contractor

Annex 1 to the order pursuant to Art. 28 DS-GVO:

List of personal data and purpose of their processing

Type of data

Subject of the additional agreement are the following data types and data categories:

- Person master data
- communication data (e.g., telephone, e-mail)
- Contract master data
- log data

Circle of those affected

The circle of persons affected by this supplementary agreement includes:

- Clients and prospects of the client
- Employees and suppliers of the client

Annex 2 to the order according to Art. 28 DS-GVO:

Technical and organizational measures according to Art. 32 DS-GVO and Annex

I. Confidentiality

- Access control
    - Server in Nuremberg
        - documented key assignment to employees
        - 24/7 staffing of data centers
        - The access for non-employees (for example, visitors) to the rooms is limited as follows: only in the company of a employee

- Technical access control
    - Access is password protected, access is for authorized users only
    Employee; used passwords must have minimum length and be renewed at regular intervals
    - The password for the administration interface is assigned by the contractor himself - the passwords must fulfill predefined guidelines.

- Access control via application
    - in the Contractor's internal management systems
        - Through regular security updates (according to the current status of the Technology), the contractor ensures that unauthorized access be prevented.
    - Audit-proof, mandatory authorization procedure for Employees of the contractor
    - The responsibility of access control lies with the contractor.
    - For transmitted data / software, only the contractor is responsible for Security and updates in charge.
- volume control
    - Hard drives will be terminated after a defined procedure repeatedly overwritten (deleted). After verification, the Hard disks inserted again.
    - Defective hard disks that cannot be safely deleted destroyed ("shredded") irectly in the data center.
- separation control
    - Principals data is logically separated from other data saved.
    - Data backup is done on physically separate systems.
- Pseudonymization
    - The client is responsible for the pseudonymisation

II. Integrity (Article 32 (1) (b) of the GDPR)• Weitergabekontrolle
    - All employees are i. P. D. Instructed and obliged to comply with Article 32 (4) DS-GVO; the privacy-compliant handling of personal data sure.
    - Privacy-friendly deletion of the data after the order has been completed.
    - Possibilities for encrypted data transmission are within the scope of Service description of the main order provided.
- Input control

- The data are entered or recorded by the client himself.
- Changes to the data are logged.
- The responsibility of the input control lies with the client.

III. Availability and resilience (Art. 32 (1) (b) DS-BER)

- Availability control
  - Backup and recovery concept with daily backup of all relevant Dates.
  - Expert use of protection programs (virus scanners, firewalls, Encryption programs, SPAM filters).
  - Use disk mirroring on all relevant servers.
  - Monitoring of all relevant servers.
  - Use of uninterruptible power supply, emergency power system.

- Rapid recoverability (Article 32 (1) (c) DS-BER);
  - For all internal systems, an escalation chain is defined that specifies who should be informed in the event of a fault, to the system as soon as possible restore.

IV. Procedure for regular review, evaluation and evaluation (Article 32 (1) (d) of the GDPR, Article 25 (1) of the GDPR)

  - Incident management is in place.
  - Privacy-friendly presets are used in software development taken into account (Article 25 (2) of the GDPR).

- Order control
  - Employees are regularly involved in data protection law and they are familiar with the procedures and User policies for data processing on behalf, including with regard to to the authority of the client. The terms and conditions contain detailed Information on the type and extent of commissioned processing and use personal data of the client.
  - The terms and conditions contain detailed information on the earmarking of the personal data of the client.
  - Continux GmbH has a company data protection officer and an information security officer. Both are through the Privacy organization and information security management system in involved the relevant operational processes.