Agreement on the processing of personal data

As an **attachment to the Terms of Service**.

Between the

Customer

as User

- hereinafter User -

and

Planubo, Christoph Drechsler & Michael Tenzer GbR

Am Hirtengarten 2

77743 Neuried

as Contractor

- hereinafter Contractor -

the following agreement on the processing of personal data is concluded:

1 Introduction, scope, definitions

(1) This Agreement governs the rights and obligations of the User and the Contractor (hereinafter referred to as the "Parties") in the context of processing personal data on behalf of the User.

(2) Terms used in this contract are to be understood according to their definition in the EU General Data Protection Regulation. In this sense, the User is the "responsible party", the contractor is the "processor". Insofar as declarations in the following are to be made "in writing", the written form according to § 126 BGB is meant. Otherwise, declarations may also be made in another form, provided that appropriate verifiability is ensured.

2 Subject and duration of processing

2.1 Subject

The subject matter of the agreement is the rights and obligations of the parties within the scope of the provision of services according to the order, the service description and Terms of Service (hereinafter referred to as the main contract), insofar as a processing of personal data takes place by the Contractor as a processor for the User pursuant to Art. 28 DSGVO. This includes all activities which the Contractor carries out to fulfill the order and which constitute commissioned processing. This also applies if the order does not expressly refer to this agreement on commissioned processing.

2.2 Duration

Processing shall commence on the Start Date agreed in the Order and shall continue indefinitely until termination of this agreement or the main contract by either Party.

3 Nature, purpose and data subjects of the data processing:

3.1 Type of processing

The type of processing includes all types of processing within the meaning of the GDPR to fulfill the order.

3.2 Purpose of processing

Purposes of processing are all purposes necessary for the provision of the contracted service.

3.3 Type of data

The following data will be processed:

- The type of data processed is determined by the User through the configuration and through the use of the services. The data to be processed may include, but is not limited to, first and last name, email address, IP address, address, event data, billing data and profile settings.

3.4 Categories of data subjects

Affected by the processing are:

- The categories of data subjects are determined by the User through the configuration and through the use of the Services. Data subjects may include customers of the User, interested parties of the User, and employees of the User.

4 Duties of the contractor

(1) The Contractor shall process personal data exclusively as contractually agreed, unless the Contractor is legally obliged to perform a specific processing. If such obligations exist for the Contractor, the Contractor shall notify the User thereof prior to processing, unless the Contractor is prohibited by law from such notification.

(2) The Contractor confirms that it is aware of the relevant general data protection regulations. It shall observe the principles of proper data processing.

(3) The Contractor undertakes to strictly maintain confidentiality during processing.

(4) Persons who may obtain knowledge of the data processed in the order must undertake in writing to maintain confidentiality, insofar as they are not already subject to a relevant confidentiality obligation by law.

(5) The Contractor warrants that the persons employed by it for processing have been familiarized with the relevant provisions of data protection and this Agreement prior to the start of processing. Corresponding training and awareness-raising measures shall be repeated on an appropriate regular basis. The Contractor shall ensure that persons deployed for commissioned processing are appropriately instructed and monitored on an ongoing basis with regard to compliance with data protection requirements.

(6) In connection with the commissioned processing, the Contractor shall support the User to the extent necessary in fulfilling its obligations under data protection law, in particular in creating and updating the list of processing activities, in carrying out the data protection impact assessment and any necessary consultation with the supervisory authority. The required information and documentation shall be kept available and provided to the User upon request. The Contractor shall be entitled to demand reasonable remuneration from the User for these services.

(7) If the User is subject to control by supervisory authorities or other bodies or if data subjects assert rights against it, the Contractor undertakes to support the User to the extent necessary, insofar as the processing on behalf is affected. The Contractor shall be entitled to demand reasonable remuneration from the User for these services.

(8) The Contractor may only provide information to third parties or the person concerned with the prior consent of the User. The Contractor shall immediately forward any inquiries addressed directly to it to the User.

(9) To the extent required by law, the Contractor shall appoint a competent and reliable person as data protection officer. The contact details of the data protection officer are published on the Contractor's website.

5 Processing safety

(1) The Contractor shall take appropriate technical and organizational measures in its area of responsibility to ensure that the processing is carried out in compliance with the requirements of the GDPR and to ensure the protection of the rights and freedoms of the data subject. The Contractor shall take appropriate technical and organizational measures in its area of responsibility in accordance with Article 32 of the GDPR to permanently ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the Processing.

(2) The Contractor's current technical and organizational measures can be viewed in Annex 1. The Contractor clarifies that the technical and organizational measures listed in the Annex are merely descriptions of a technical nature and are not to be considered part of this Agreement.

(3) The data security measures can be adapted in line with technical and organizational developments, as long as the level of protection agreed here is not undercut.

6 Rules for the correction, deletion and blocking of data

(1) The Contractor shall only correct, delete or block data processed within the scope of the order in accordance with the contractual agreement reached or in accordance with the User's instructions.

7 Subcontracting relationships

(1) The User grants the Contractor general authorization to use further subcontractors within the meaning of Art. 28 GDPR for the performance of the Contract.

(2) The subcontractors currently used can be found at the following link: https://planubo.com/privacy-policy/. The User will be regularly informed about changes there. The User agrees to their use.

(3) It must also be possible to effectively exercise the rights of the User against the subcontractor.

(4) The responsibilities of the contractor and the subcontractor must be clearly delineated.

(5) The Contractor shall carefully select the subcontractor, paying particular attention to the suitability of the technical and organizational measures taken by the subcontractor.

(6) If the Contractor awards contracts to other Processors, it shall be the Contractor's responsibility to transfer its data protection obligations under this Agreement to the other Processor.

(7) Subcontracting relationships within the meaning of this contract are only those services that have a direct connection with the provision of the main service. Ancillary services, such as transport, maintenance and cleaning as well as the use of telecommunications services or user services are not covered. The obligation of the Contractor to ensure compliance with data protection and data security in these cases shall remain unaffected.

8 Rights and obligations of the User

(1) The User alone is responsible for assessing the permissibility of the commissioned processing and for safeguarding the rights of data subjects.

(2) The User shall issue all orders, partial orders or instructions in documented form. In urgent cases, instructions may be issued verbally. The User shall confirm such instructions immediately in a documented manner.

(3) The User shall inform the Contractor without undue delay if it discovers errors or irregularities in the examination of the results of the order or irregularities with regard to provisions under data protection law.

(4) In the event of termination, the User undertakes to delete the personal data stored in the Services before the termination of the Contract.

(5) At the request of the Contractor, the User shall appoint a contact person for data protection issues.

9 Requests from affected persons

(1) If a data subject approaches the Contractor with a request for correction, deletion or information, the Contractor shall refer the data subject to the User, provided that an assignment to the User is possible according to the information provided by the data subject. The Contractor shall immediately forward the request of the data subject to the User. The Contractor shall support the User

within the scope of its possibilities. The Contractor shall not be liable if the request of the data subject is not answered by the User, not answered correctly or not answered in time.

10 Instructions

(1) Within the scope of this Agreement, the User shall be solely responsible for compliance with the statutory provisions of the data protection laws, in particular for the lawfulness of the transfer of data to the Contractor as well as for the lawfulness of the data processing ("Controller" within the meaning of Art. 4 No. 7 DSGVO). This also applies with regard to the purposes and means of processing regulated in this agreement.

(2) The User shall issue all instructions in documented form. In urgent cases, instructions may be issued verbally. The User shall confirm such instructions immediately in a documented manner.

(3) Instructions not provided for in the contract shall be treated as a request for a change in performance. In the case of proposed changes, the Contractor shall inform the User of the effects on the agreed services. If the Contractor cannot reasonably be expected to carry out the instruction, the Contractor shall be entitled to terminate the processing.

(4) The contractually agreed data processing usually takes place predominantly in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area, unless the transfer of data to third countries is necessary for the provision of the service. In the event that a transfer to a third country takes place, the Contractor shall ensure that the requirements pursuant to Art. 44 et seq. DSGVO are fulfilled.

11 Liability and compensation

(1) In the event that a data subject asserts a claim for damages pursuant to Art. 82 GDPR, the parties undertake to assist each other and to contribute to the clarification of the underlying facts.

(2) The liability provision agreed between the parties in the main contract for the provision of services shall also apply to claims arising from this commissioned processing agreement and, in the internal relationship between the parties, to claims by third parties pursuant to Art. 82 of the GDPR, unless expressly agreed otherwise.

(3) The parties shall each release themselves from liability if / to the extent that a party proves that it is not responsible in any respect for the circumstance by which the damage occurred to an affected person.

(4) Unless otherwise provided above, liability under this Agreement shall be the same as under the main contract.

12 Remuneration

The Contractor's remuneration is conclusively regulated in the main contract.

13 Special right of termination

(1) The User may terminate the main contract and this agreement at any time without notice ("Extraordinary Termination") if there is a serious breach of data protection regulations or the provisions of this Agreement by the Contractor, the Contractor cannot or will not carry out a lawful instruction of the User or the Contractor refuses control rights of the User in breach of the Agreement.

(2) A serious breach shall be deemed to have occurred in particular if the Contractor fails to fulfill or has failed to fulfill to a significant extent the obligations specified in this Agreement, in particular the agreed technical and organizational measures.

(3) In the event of insignificant violations, the User shall set the Contractor a reasonable deadline for remedial action. If the remedy is not provided in time, the User shall be entitled to extraordinary termination as described in this section.

14 Other

(1) Both parties are obligated to treat all knowledge of business secrets and data security measures of the respective other party obtained within the framework of the contractual relationship as confidential, even after the termination of the contract. If there is any doubt as to whether information is subject to the obligation of confidentiality, it shall be treated as confidential until it has been released in writing by the other party.

(2) If the property of the User with the Contractor is endangered by measures of third parties (for example by attachment or seizure), by insolvency or composition proceedings or by other events, the Contractor shall notify the User without delay.

(3) The User recognizes this agreement as part of the Terms of Service https://planubo.com/terms-of-service/ about the product booked by him.

(4) The Agreement shall commence upon its conclusion by the User. If a commissioned processing still takes place after the termination of this agreement, the provisions of this agreement shall apply until the actual end of the processing.

(5) The Contractor may amend the Contract at its own discretion with reasonable notice. In particular, the Contractor expressly reserves the right to unilaterally amend this Agreement if material legal changes occur with respect to this Agreement. The Contractor shall separately inform the User of the significance of the planned amendment and shall furthermore grant the User a reasonable period of time to declare an objection. The Contractor shall inform the User in the notice of amendment that the amendment will become effective if the User does not object within the set period. In the event of an objection by the User, the Contractor shall have an extraordinary right of termination.

(6) The exclusive place of jurisdiction for all disputes arising from and in connection with this contract shall be the Contractor's registered office. This shall apply subject to an exclusively statutory place of jurisdiction. This contract is subject to the statutory provisions of the Federal Republic of Germany.

(7) Should individual parts of this agreement be invalid, this shall not affect the validity of the remainder of the agreement.

Annex 1 - technical and organizational measures

The following specifies the order-related technical and organizational measures to ensure data protection and data security that the Contractor must at least establish and maintain on an ongoing basis. The aim is to ensure in particular the confidentiality, integrity and availability of the information processed in the order.

- Encryption (Art. 32 para. 1 lit. a DS-GVO)
  - Sensitive data, databases and media files that are uploaded are encrypted
- Confidentiality (Art. 32 para. 1 lit. b DS-GVO)
  - Access control: No unauthorized access to data processing equipment.
    - The Contractor's server and database are located in Germany with Strato AG
    - Images, invoices and uploads are stored on Amazon AWS S3 Buckets in Frankfurt
  - Access control: No unauthorized system use
    - Determination of the need for protection
    - Implementation of secure access procedures and strong authentication
    - Implementation of simple authentication via user name and password
    - Secure (encrypted) transmission of authentication secrets
    - Blocking in case of failed attempts and procedure for resetting blocked access IDs
    - Designation of authorized persons
    - Management of personal authentication media and access authorizations
    - Manual access blocking
  - Access control: no unauthorized reading, copying, modification or removal within the system
    - Implementation of access restrictions
    - Allocation of minimum authorizations
  - Segregation control: Separate processing of data collected for different purposes.
    - Data economy in the handling of personal data
    - Regular purpose control and deletion
    - Separation of test and development environment
- Integrity (Art. 32 para. 1 lit. b DS-GVO)
  - Transfer control: No unauthorized reading, copying, modification, or removal during electronic transmission or transport.
    - Determination of the persons authorized to receive/transmit data
    - Verification of the legality of the transfer abroad
    - Secure data transmission between server and User
    - Secure transmission to external systems
    - Secure storage of data, including backups
    - Data protection-compliant deletion and destruction process
  - Input control: Determining whether and by whom personal data have been entered into, modified or removed from data processing systems.
    - Logging of the inputs
- Availability and resilience (Art. 32 para. 1 lit. b DS-GVO)
  - Monitoring
  - Resource planning and provisioning
  - Defense against abuse of the system
  - Data backup concepts and implementation

- Recoverability (Art. 32 para. 1 lit. c DS-GVO)
  - Data backup concepts and implementation
- Data protection organization
  - Definition of responsibilities
  - Implementation and control of appropriate processes
  - Confidentiality obligation
  - Regulations for the internal distribution of tasks
- Procedures for regular review, assessment and evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)
  - Process for incident response management
    - Detection and investigation of security incidents
  - Data privacy-friendly default settings: If data is not required to achieve the purpose of use, the technical default settings are defined in such a way that data is only collected, processed, disclosed or published based on an action by the data subject.
  - Order control: selection of further contractors according to suitable guarantees