Appendix 3 Data Processing Agreement pursuant to Art. 28 GDPR ("DPA")

between

Leadtime Labs GmbH, Yorckstr. 22, 93049 Regensburg

- Processor, hereinafter referred to as: Contractor -

and

- controller, hereinafter referred to as: client -

- hereinafter also jointly referred to as "Parties" and individually
referred to as "Party" -

Preamble

This agreement sets out the rights and obligations of the Contractor and the Client in the context of the processing of personal data on behalf of the Client in accordance with Art. 28 of the EU General Data Protection Regulation ("GDPR"). This agreement applies to all activities in which the Contractor, its employees, or subcontractors commissioned by it process personal data of the Client.

§ 1 Subject matter and duration of processing

(1) The subject matter of the processing is set out in the contract for the provision of IT services ("IT project contract"), which is referred to below (hereinafter referred to as the "main contract").

(2) The duration of this agreement (term) corresponds to the term of the main contract.

(3) If the term of the main contract has ended, this agreement shall remain in force, notwithstanding the preceding paragraph, for as long as the contractor processes the client's personal data (including backups).

§ 2 Type of data and purpose of processing

(1) The contractor shall provide the client with IT services in accordance with the main contract, in particular the following services: operation of a "Leadtime Workspace". In addition, the provider shall provide maintenance and support services for the client, which may involve access to the types of personal data listed below.

(2) The following types/categories of data may be subject to processing:

- General personal data (name, title, academic degree, date of birth)
- Communication data (address, telephone number, email)
- Payment data (bank details)
- Health data (employee sick days, medical certificates)
- Social data (health insurance number, pension insurance, social security number, income tax bracket)

(3) The categories of persons affected by the processing include the following:

- Employees of the client
- Freelancers
- Customers and prospective customers of the client.

§ 3 Obligations of the contractor

(1) The contractor assures that it is familiar with the relevant, applicable data protection regulations and that it complies with the principles of proper processing of personal data at all times. This agreement does not release the contractor from compliance with other provisions of the GDPR.

(2) The contractor shall only process personal data on the basis of documented instructions from the client, unless it is obliged to do so under the law of the Member State or under Union law. The initial instructions of the client are set out in this

The contractor shall inform the client immediately if it believes that an instruction violates applicable data protection regulations.

(3) The contractor shall not use the data for any purposes other than those specified.

(4) The contractor undertakes to maintain confidentiality when processing the data and shall only employ staff who are bound to confidentiality and have been familiarized with the relevant data protection provisions prior to providing their services.

(5) The parties shall cooperate with the supervisory authority in the performance of its duties upon request.

(6) The contractor shall immediately inform the client of any control activities and measures taken by the supervisory authority insofar as they relate to this agreement and the processing of the client's data. This shall also apply if a competent authority investigates the contractor in the context of administrative or criminal proceedings relating to the processing of personal data under this agreement.

(7) The contractor shall regularly monitor internal processes and technical and organizational measures to ensure that processing within its area of responsibility is carried out in accordance with the requirements of applicable data protection law and that the rights of data subjects are protected.

(8) The contractor shall report violations of personal data protection to the client immediately after becoming aware of them in such a way that the client can fulfill its legal obligations, in particular in accordance with Articles 33 and 34 of the GDPR. The contractor shall prepare documentation on the entire process, which it shall forward to the client upon request for information and further action.

(9) The contractor undertakes to support the client in its area of responsibility and, as far as possible, within the scope of existing information obligations towards supervisory authorities and data subjects, and to provide the client with all relevant information in this context.

(10) If the client is obliged to carry out a data protection impact assessment, the contractor shall support the client at the client's expense, taking into account the nature of the processing and the information available to it. This applies equally to any obligation to consult the competent data protection supervisory authority. The parties shall agree on the terms and conditions in each individual case in writing or in text form.

§ 4 Technical and organizational measures ("TOMs")

(1) The contractor undertakes to take all necessary technical and organizational measures within its area of responsibility in accordance with Art. 32 GDPR to protect the personal data processed on behalf of the client. The documentation of the technical and organizational measures shall be bindingly agreed between the parties in Appendix 1 at the time of conclusion of the contract.

(2) The technical and organizational measures described in Appendix 1 are subject to technical progress and further development. In this respect, the contractor is permitted to implement appropriately adapted measures in the future, provided that the security level of the measures specified herein is not compromised. The contractor shall document all changes and inform the client immediately of any significant changes.

§ 5 Handling of the rights of data subjects

(1) The contractor shall support the client in its area of responsibility and, as far as possible, by means of appropriate technical and organizational measures in responding to and implementing requests from data subjects regarding their data protection rights.

(2) The contractor shall only disclose, correct, delete, or restrict the processing of data processed on behalf of the client in accordance with the contractual agreement or the client's instructions. If a data subject contacts the contractor directly in exercising their data protection rights, the contractor shall forward this request to the client without delay.

§ 6 Use of subcontractors

(1) The contractor is entitled to use subcontractors as additional processors in the context of the processing of personal data. The client permits the use of the subcontractors listed in Appendix 2.

(2) Outsourcing to additional subcontractors and any change of subcontractors listed in Appendix 2 shall be permitted provided that:

(a) the contractor notifies the client of such outsourcing or change in writing or in text form with four weeks' advance notice, and

(b) the client does not object to the planned outsourcing in writing or in text form to the contractor within two weeks of receiving the notification, and

(c) a contractual agreement in accordance with Art. 28 (2) - (4) GDPR exists with the subcontractor.

(3) In the event of an objection by the client to such outsourcing or to the change of a subcontractor, the contractor shall have the right to terminate this agreement and the main contract for good cause.

(4) The contractor shall check compliance with and implementation of the technical and organizational measures at the subcontractor, taking into account the respective risk, before the processing of personal data begins and then on a regular basis. The contractor shall make the results of the checks available to the client upon request.

(5) If the subcontractor provides the agreed service outside the EU/EEA, the contractor shall ensure compliance with data protection law by taking appropriate measures, in particular by providing adequate data protection guarantees.

(6) Any further outsourcing by the subcontractor requires the express consent of the main contractor in writing or in text form.

(7) Within the meaning of the above provisions, subcontracting relationships refer to services that relate directly to the performance of the main contract. . This does not include ancillary services such as telecommunications services, postal/transport services, cleaning services, or security services. The contractor is obliged to enter into appropriate and legally compliant contractual agreements to ensure data protection and data security, even for outsourced ancillary services. Maintenance and testing services constitute a subcontracting relationship if they are provided for IT systems that are related to a service provided by the contractor under this agreement.

§ 7 Rights and obligations of the client

(1) The client is solely responsible for assessing the permissibility of order processing and for safeguarding the rights of data subjects.

(2) The client has comprehensive authority to issue instructions regarding the processing of personal data on behalf of the client. To this end, the parties designate the following persons, who are exclusively authorized to issue and accept instructions:

Authorized persons at	Client	Contractor
Last name, first name	Ebner, Lukas	
Email	lukas@leadtime.de	
Phone	+49 941 463 900 42	

(3) Any changes to authorized persons and/or their contact details must be communicated to the other party immediately in writing or in text form.

(4) The client is obliged to issue all orders, partial orders, or instructions in documented form, i.e., at least in text form. Instructions may only be given verbally in urgent exceptional cases; such instructions must be confirmed by the client immediately and documented in an appropriate manner.

(5) The client undertakes to inform the contractor immediately if and to the extent that it discovers errors or irregularities in the course of order processing.

(6) The client is entitled to verify compliance with data protection regulations and contractual agreements, in particular the complete implementation of the specified technical and organizational measures and their effectiveness, at the contractor's premises to an appropriate extent, either itself or through a representative

agreements, in particular the complete implementation of the specified technical and organizational measures and their effectiveness, either itself or through an auditor to be appointed in each individual case. Checks are possible in particular by obtaining information and inspecting the stored data and data processing programs. The contractor is obliged to provide the necessary information and evidence required to carry out a check.

§ 8 Data processing outside the EU/EEA

(1) If it is necessary to transfer personal data to a third country or to an international organization, the contractor shall ensure compliance with the requirements for the transfer of personal data to third countries in accordance with Chapter 5 of the GDPR.

(2) The client authorizes the transfer of data to a third country to the recipients listed in Appendix 2. The appendix sets out the measures approved by the client to ensure an adequate level of protection in accordance with Art. 44 ff. GDPR in the context of subcontracting.

(3) If the client instructs the transfer of data to third parties in a third country, it shall be solely responsible for compliance with the provisions of Chapter 5 of the GDPR.

§ 9 Termination of processing on behalf of the client

(1) Upon termination of the cooperation, the contractor shall, at the request of the client, hand over the personal data to the client in accordance with the agreed retention period and then delete it from the servers. The customer must exercise this request within one (1) month of the termination of the cooperation. The deletion shall be carried out in such a way that restoration is impossible with reasonable effort.

(2) The contractor shall also ensure deletion vis-à-vis its subcontractors, insofar as this is contractually possible and legally permissible.

(3) The contractor is obliged to provide evidence of proper deletion in accordance with the law and will submit this to the client accordingly.

and shall submit this to the client accordingly. The contractor is entitled to retain documentation serving as proof of proper data processing in accordance with the respective retention periods, even beyond the term of the agreement.

§ 10 Final provisions

(1) This agreement shall take precedence, even if other agreements between the client and the contractor contain other provisions on the protection of personal data, unless the parties have expressly agreed otherwise.

(2) This agreement thus replaces all verbal or written agreements previously made between the parties with regard to the subject matter of the processing.

(3) No further verbal or written side agreements to this agreement have been made.

(4) Amendments and supplements to this agreement must be made in writing, unless an individual agreement has been made. This also applies to the waiver of this written form requirement.

(5) Should any provision of this agreement be or become invalid or unenforceable in whole or in part, this shall not affect the validity of the agreement or the remaining provisions. The parties shall endeavor to agree on a valid and enforceable provision that comes as close as possible to the economic purpose of the invalid or unenforceable provision. This shall apply equally in the event of a loophole.

(6) The appendices to this agreement listed below are an integral and essential part of the contract:

Appendix 3 – Annex 1
Technical and organizational measures ("TOMs") at the contractor

The technical and organizational measures listed below to ensure data protection and data security are currently in place at the contractor and/or its subcontractors:

No	Area	Description
0	**Organization**	
	How is data protection implemented?	An external data protection officer is appointed to perform the advisory and supervisory functions required by the GDPR.
	Name and contact details of the data protection officer	Wojtek Dragon Projekt 29 GmbH & Co. KG Ostengasse 14 93047 Regensburg anfrage@projekt29.de
	How are employees trained in the implementation of the agreed technical and organizational measures that apply to this processing?	The training concept includes both data protection instruction at the start of employment and constant awareness-raising through monthly data protection newsletters and specialist web training courses.
	Is the processing documented in terms of data protection law compliance?	The data flows are documented in the internal procedure directory and the admissibility of processing and use in accordance with the GDPR is verified. Any necessary prior checks are already integrated at the planning stage.
1	**Confidentiality (Art. 32 (1) (b) GDPR)**	
1.1	**Access control**	
	How are the buildings in which processing takes place secured against unauthorized access?	The building is equipped with a security locking system.
	How are the rooms/offices where processing takes place secured against unauthorized access?	The rooms are also secured by the security locking system.
	How are the processing facilities protected against unauthorized access?	DigitalOcean's data centers are located in inconspicuous buildings that are physically constructed, managed, and monitored around the clock to protect data and services from unauthorized access and environmental threats. All data centers are surrounded by a fence and access is restricted by ID-controlled gates.
	How are the access control measures implemented tested for suitability?	The access control measures are also reviewed as part of the checks carried out by the external data protection officer.
1.2	**Access control**	
	How is user access granted?	User accounts are only granted on a very selective basis and only after approval by management. Access to commercial documents and communication information is protected by strong passwords.
	How is the validity of user accounts checked?	All rights are granted in accordance with the principle of minimal access and are only extended when necessary. All access rights are revoked upon termination of employment.
	How is it ensured that the number of administrative accounts is reduced to the necessary minimum and that only professionally and personally suitable personnel are assigned to them?	Decisions on the assignment of rights strictly adhere to the relevant guidelines, data avoidance, and data minimization.
	Is it possible to access the systems/applications from outside the company (home workstations, service providers, etc.) and how is access organized?	The use of home workstations is governed by a home office policy. Employees are required to maintain the same measures at home as they do at work.
1.2	**Access control**	
	How is it ensured that passwords are only known to the respective user?	Passwords are assigned by the respective employee themselves. Strict system settings enforce a high level of password complexity. Passwords are not stored or written down in plain text.
	What are the requirements for password complexity?	The specifications and recommendations of the BSI serve as a model for the above-mentioned system settings.

	What organizational precautions are taken to prevent unauthorized access to personal data in the workplace?	Training and awareness-raising for employees. Instruction and regular training on the devices used.
	How is it ensured that access authorizations are granted in accordance with requirements and are time-limited?	See also point 1.2 on granting user access; the IT department checks the rights and user structure at regular intervals
	How is it ensured that access authorizations are not misused?	Everyone is assigned minimal rights to enable them to perform their tasks.
	How long are logs kept? Who has access to the logs and how often are they evaluated?	No fixed deadlines, mostly system parameters, exclusively the management
1.4	Pseudonymization	
	What organizational measures have been taken to ensure that the processing of personal data complies with the law?	All persons entrusted with the processing of personal data have been duly obligated. A data protection concept is implemented in the company and has been communicated to all employees. The training concept includes both data protection instruction at the start of employment and constant awareness-raising through monthly data protection newsletters and subject-specific web training. Attention has been drawn to the special features of handling pseudonymized data.
	What technical measures or tools are used for the pseudonymization of personal data?	Customer data is encrypted with TLS v1.2 during transmission between the customer's software application and our DigitalOcean data center.
2	**Integrity (Art. 32 (1) (b) GDPR)**	
2.1	**Transfer control**	
	How is integrity and confidentiality ensured when personal data is disclosed?	Where possible, no personal data of customers is transferred. This only occurs in the course of order processing, which is contractually secured by Art. 28 GDPR.
	Are encryption systems used when transferring personal data and, if so, which ones?	In the DigitalOcean data center, information is encrypted using the Advanced Encryption Standard (AES). Customer data stored by DigitalOcean is encrypted using TLS v1.2 during transmission between the customer's software application and DigitalOcean.
	How is the transfer of personal data documented?	Data processing agreements are concluded with the processors.
	How is the unauthorized disclosure of personal data restricted by technical measures?	Strict rights assignment protects the data from unauthorized access.
2.2	**Input control**	
	How can it be traced which activities were carried out on the relevant applications?	Role/rights concepts and various license models with different authorization concepts
	What measures are taken to ensure that processing by employees can only be carried out in accordance with the client's instructions?	Access control based on the role/rights concept for proper data processing and storage.
	What measures are taken to ensure that subcontractors also process the client's personal data exclusively to the agreed extent?	All subcontractors are subject to the same requirements as the contractor. Corresponding contracts have been concluded. The company's data protection officer is responsible for checking the subcontractors. He is also significantly involved in the selection of the contracted companies.
	How is the deletion/blocking of personal data at the end of the retention period ensured by subcontractors?	This is specified in the contract; if the purpose no longer applies, the data must also be deleted.
3	**Availability and resilience**	
3.1	**Availability control**	
	How is it ensured that the data carriers are protected against elemental influences (fire, water, electromagnetic radiation, etc.)?	Backed-up data is physically separated from productive data.
	What protective measures are used to combat malware, and how is their currency ensured?	We use constantly updated virus scanners and spam filters. The systems are updated regularly.

	How do you ensure that data carriers that are no longer needed or are defective are disposed of properly?	Physical deletion of functional data carriers and mechanical destruction of defective data carriers prior to disposal.
3.2	**Recoverability**	
	What organizational and technical measures are taken to ensure the availability of data and systems as quickly as possible, even in the event of damage? (Rapid recoverability in accordance with Art. 32 (1) (c) GDPR)	Regular backups, UPS, and a restart concept in the data center.
4.	**Procedures for regular review, assessment, and evaluation (Art. 32(1)(d) GDPR, Art. 25(1) GDPR)**	
	What procedures are in place for regular assessment/review to ensure the security of data processing (data protection management)?	The external data protection officer reviews compliance with technical and organizational measures on an annual basis. The DigitalOcean data center has developed and implemented a security control system to protect the confidentiality, integrity, and availability of customer systems. DigitalOcean's customer data usage policy governs the requirements for the use of customer data in accordance with various industry standards. The data center is ISO27001 certified.
	How are inquiries and problems handled (incident response management)?	Requests and problems can be reported directly to the team via the contact form or by email.
	What data protection-friendly default settings are there (Art. 25 (2) GDPR)?	No pre-selection by check marks; no pre-selections are made when logging into the system; users must enter their login information each time.
4.1	**Order control**	
	What procedures are in place for instructing and handling order processing (data protection management)?	The contract was designed in accordance with the current legal requirements for order processing. The external data protection officer performs the corresponding advisory and control duties.

Appendix 3 – Annex 2
Approved subcontractors

The client approves the use of the following subcontractors of the contractor:

Name of subcontractor	Address/Country	Scope of services	Information on appropriate safeguards for data transfers to third countries