

Data Processing Contract

Between

fodjan GmbH, Großenhainer Str. 101, 01127 Dresden

- Contractor -

and

[Company name, street House number, zip code City]

- Principal -

Preamble

The Principal wants to engage the Contractor to render the performances specified in section 3. The implementation hereof includes personal data processing. In particular, Art. 28 GDPR imposes certain requirements on such processing. To meet these requirements, the parties conclude the following agreement, fulfilment of which will not be remunerated separately unless explicitly agreed.

Section 1 Definition of Terms

The definitions result from Art. 4 GDPR.

Section 2 Subject Matter of the Agreement

- (1) The Contractor shall render software as a service performances for the Principal based on a separate contract ("Main Contract") via the 'fodjan smart feeding' web platform. The software allows to manage different data of the Principal's customers. In doing so, the Contractor shall be granted access to and shall process Personal Data exclusively on behalf of and in line with the Principal's instructions.
- (2) The specific object of Processing, the type and purpose of Processing, the type of Personal Data and the categories of Data Subjects shall be governed by **appendix 1** hereto. Assessment of the admissibility of data Processing shall be incumbent upon the Principal.
- (3) To put their mutual rights and obligations under data protection law in concrete terms, the parties conclude this agreement. In case of doubt, the provisions hereunder shall prevail over the regulations of the Main Contract.
- (4) The provisions hereof shall be applicable to all activities associated with the Main Contract where the Contractor and its employees or agents of the Contractor deal with Personal Data originating from or collected for the Principal.
- (5) The term hereof shall be governed by the term of the Main Contract, unless farther-reaching obligations or rights of termination arise from the provisions below.

Section 3 Right to Issue Instructions

- (1) The Contractor may collect, process or use Personal Data only under the Main Contract and in line with the Principal's instructions. This shall apply, in particular, in relation to the transfer of Personal Data

to a third country or an international organisation. If the Contractor is obliged to perform further Processing activities on account of the laws of the European Union or of the Member States it is subject to, it shall notify the Principal of such legal requirements before Processing.

(2) Initially, the Principal's instructions shall be defined hereby and may subsequently be modified, amended or replaced by the Principal by individual instructions in text form ("Individual Instruction"). The Principal shall be entitled to issue relevant instructions at any time. This shall include instructions regarding the rectification, erasure and blocking of Personal Data. The persons entitled to issue instructions shall be governed by appendix 1. In case of any replacement or any longer-term unavailability of the designated persons, the contracting partner must be immediately notified of the successors or representatives in text form.

(3) All issued instructions must be documented by both the Principal and the Contractor. Instructions beyond the performance agreed in the Main Contract shall be treated as a Performance Changes request.

(4) If the Contractor takes the view that any instruction of the Principal violates provisions under data protection law, it shall immediately notify the Principal thereof. The Contractor shall be entitled to suspend implementation of the relevant instruction until it is confirmed or changed by the Principal. The Contractor may refuse implementation of any instruction that is obviously unlawful.

Section 4 Contractor's Protection Measures

(1) The Contractor shall be obliged to observe the legal provisions on data protection and to neither disseminate to third parties nor suspend access to the information obtained from the Principal's sphere. Documents and Personal Data must be protected against access by unauthorised parties, taking into account the state of the art.

(2) The Contractor shall set up the internal organisation in its sphere of responsibility in such a way that it meets the special requirements of data protection. It shall take all technical and organisational measures required to ensure reasonable protection of the Principal's Personal Data acc. to Art. 32 GDPR, especially, as a minimum, the measures specified in appendix 2:

- a) entry control
- b) admission control
- c) access control
- d) separation
- e) pseudonymisation and encryption
- f) input control
- g) dissemination control
- h) availability and resilience of the systems and services
- i) process for regularly testing, assessing and evaluating

Any change to the security measures taken shall remain reserved to the Contractor, who shall ensure that the contractually agreed level of protection will not be undercut.

(3) The following person has been appointed operational point of contact for data protection at the Contractor's:

Alexander, Weidenhammer
DID Dresdner Institut für Datenschutz
Hospitalstraße 4
01097 Dresden

Tel.: (0)351 / 655 772-0
E-Mail: datenschutz@fodjan.de

(4) The persons employed for data processing by the Contractor shall be prohibited from collecting, processing or using Personal Data without authorisation. The Contractor shall obligate all persons entrusted by it with the handling and fulfilment hereof (hereinafter referred to as "Employees") accordingly (confidentiality obligation, point (b) of Art. 28(3) GDPR) and shall ensure compliance with such obligation with all due care. Such obligations must be defined such that they continue to apply even after the end hereof or of the employment relationship between the Employee and the Contractor. Upon request, the Principal must be provided with appropriate evidence of such obligations.

Section 5 Contractor's Information Obligations

(1) In case of disruptions, suspected data breaches or violations of contractual obligations of the Contractor, suspected security-relevant incidents or other irregularities in the Processing of the Personal Data by the Contractor, persons employed by it within the scope of the assignment or by third parties, the Contractor shall immediately inform the Principal in text form. The same shall apply to audits of the Contractor by the data protection Supervisory Authority. The notification of a Personal Data breach shall at least:

- a) describe the nature of the Personal Data breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
- b) describe the measures taken or proposed to be taken by the Contractor to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(2) The Contractor shall immediately take the measures required to back up the Personal Data and to mitigate possible adverse effects on the persons concerned, inform the Principal thereof and request further instructions.

(3) In addition, the Contractor shall be obliged to provide the Principal with information at any time where its Personal Data is affected by a breach pursuant to (1).

(4) If the Principal's Personal Data at the Contractor's is jeopardised due to attachment or seizure, insolvency or settlement proceedings or other events or measures of third parties, the Contractor shall notify the Principal thereof immediately, unless it is prohibited from doing so by an order issued by a court or by official order. In this context, the Contractor shall immediately inform all competent bodies of the decision-making authority for the Personal Data resting exclusively with the Principal as "Controller" within the meaning of the GDPR.

(5) The Contractor must immediately notify the Principal of significant changes to the security measures pursuant to section 4 (2).

(6) Any replacement of the operational point of contact for data protection is to be communicated to the Principal without delay.

(7) The Contractor and, where applicable, its representative shall maintain a record of all categories of Processing activities carried out on behalf of the Principal, containing all information acc. to Art. 30(2) GDPR. The record must be provided to the Principal upon request.

(8) The Contractor must contribute to the compilation of the process record by the Principal to a reasonable extent. It must provide the Principal with the respective necessary information in an appropriate manner.

Section 6 Control Rights of the Principal

(1) Prior to commencing data processing and subsequently at regular intervals, the Principal shall convince itself of the Contractor's technical and organisational measures. To that end, it may, for ex., obtain information from the Contractor, have existing attestations of expert witnesses, certifications or internal reviews presented to it or personally review itself or have a qualified third party review the Contractor's technical and organisational measures after timely coordination during normal business hours, unless such third party competes with the Contractor. The Principal shall perform controls only to the extent required, not disrupting the Contractor's business operations disproportionately.

(2) The Contractor undertakes to provide the Principal, upon the latter's verbal or written request (text form sufficient) and within a reasonable deadline, with all information and evidence required to control the Contractor's technical and organisational measures.

(3) The Principal shall document and notify the Contractor of the control result. In case of errors or irregularities identified by the Principal, especially when reviewing assignment results, it shall immediately inform the Contractor. If any facts requiring changes in the ordered process sequence to be avoided in the future are discovered during the control, the Principal shall immediately notify the Contractor of the necessary process changes.

(4) Upon request, the Contractor shall provide the Principal with an extensive and up-to-date data protection and security concept for data processing and on persons having rights of access.

(5) The Contractor shall furnish evidence of the Employees' commitment pursuant to section 4 (4) upon request.

Section 7 Deployment of Subcontractors

(1) The contractually agreed performances or the partial performances described below shall be rendered by involving the subcontractors specified in appendix 3. Within the scope of its contractual obligations, the Contractor shall be authorised to establish further subcontracting relationships with subcontractors ("Subcontractor Relationship") where it notifies the Principal thereof in advance and the latter has agreed to the engagement of the subcontractor in text form beforehand.

A refusal of consent requires an appropriate justification of the Principal (in text form) from a data protection point of view.

The Contractor shall be obliged to select subcontractors with due care based on their qualifications and reliability. When involving subcontractors, the Contractor shall obligate them according to the regulations hereunder, ensuring that the Principal may exercise its rights herefrom (especially its auditing and control rights) directly vis-à-vis the subcontractors. If any involvement of subcontractors in a third country is intended, the Contractor must ensure that an appropriate level of data protection is ensured at the relevant subcontractor's (e.g. by concluding an agreement based on the standard EU data protection clauses). Upon request, the Contractor shall furnish the Principal with evidence on the conclusion of the aforementioned agreements with its subcontractors.

(2) A Subcontractor Relationship within the meaning of these provisions shall not exist if the Contractor has engaged third parties to render any performances that are to be considered purely ancillary services in nature. This shall include, for ex., mail, transport and dispatch services, cleaning services, telecommunication services not specifically related to performances rendered by the Contractor for the Principal and security services. Maintenance and inspection services shall be Subcontractor Relationships requiring consent where they are rendered for IT systems also used in connection with performances rendered for the Principal.

Section 8 Data Subject Requests and Rights

(1) The Contractor shall support the Principal, where possible, with appropriate technical and organisational measures to ensure fulfilment of the latter's obligations pursuant to Art. 12 to 22 and 32 to 36 GDPR.

(2) If a Data Subject asserts rights, such as right of access, right to rectification or erasure regarding his/her Personal Data, immediately vis-à-vis the Contractor, the latter shall not respond autonomously, but shall immediately refer the Data Subject to and shall await the instructions of the Principal.

Section 9 Liability

(1) Where exclusions or reliefs of liability to the benefit of either party or both contracting partners are agreed in the Main Contract, they shall not apply in relation to damages claims asserted by a person concerned on account of any unauthorised or incorrect data processing or use under data protection law as part of data processing.

(2) The parties release each other from liability if either party demonstrates that it is not responsible in any way for the circumstance having caused the damage to a person concerned.

Section 10 Right of Extraordinary Termination

The Principal may terminate the Main Contract without notice in full or in part if the Contractor fails to meet its obligations herefrom, violates GDPR provisions by wilful intent or gross negligence or is not able or willing to execute any instruction of the Principal. In case of ordinary violations, i.e. caused by neither wilful intent nor gross negligence, the Principal shall set the Contractor a reasonable deadline, within which the Contractor may remedy the violation.

Section 11 End of the Main Contract

(1) After the end of the Main Contract or at any time upon the Principal's request, the Contractor shall return to the Principal or, where desired by the Principal, shall erase all documents, Personal Data and data carriers surrendered to it, unless it is obligated to retain the Personal Data according to the laws of the European Union or of the Federal Republic of Germany. This shall also relate to any data backups at the Contractor's. The Contractor shall furnish the documented proof of proper erasure of any Personal Data still existing. Documents to be disposed of must be destroyed using a paper shredder pursuant to DIN 66399. Data carriers to be disposed of shall be destroyed pursuant to DIN 66399.

(2) The Principal shall have the right to check in an appropriate manner that the Personal Data at the Contractor's is returned or erased in full and in line herewith.

(3) The Contractor shall be obliged to keep confidential, also beyond the end of the Main Contract, any Personal Data of which it has gained knowledge in connection with the Main Contract. This agreement shall remain in full force and effect beyond the end of the Main Contract as long as the Contractor has available Personal Data forwarded to it by or collected by it for the Principal.

Section 12 Final Provisions

(1) The parties agree that the defence of the right of retention by the Contractor w. t. m. of Section 273 BGB (German Civil Code) regarding the Personal Data to be processed and the associated data carriers shall be excluded.

(2) Modifications and amendments hereto shall require written form. This shall also apply to the waiver of this formal requirement. This shall not affect the priority of individually agreed terms.

(3) If individual provisions hereof are or become legally ineffective or unenforceable in whole or in part, this shall not affect the validity of the relevant remaining provisions.

(4) This agreement shall be subject to German law. Place of exclusive jurisdiction shall be, where legally permissible, the Contractor's registered office.

(5) The following appendices shall be subject matters hereof:

Appendix 1 - Subject Matter of the Assignment

Appendix 2 - Technical and Organisational Measures of the Contractor

Appendix 3 - Approved Subcontractors

-Contractor-

Dresden,

Place, Date

fodjan GmbH

Carsten Gieseler and Michael Schütze

Managing Directors

[Signature, Stamp]

-Principal-

Place, Date

Name Principal

First name Name

Position

[Signature, Stamp]

Appendix 1 - Subject Matter of the Assignment

1. Processing Object and Purpose

The Principal's assignment to the Contractor shall include the following activities and/or performances: fodjan smart feeding is a software as a service offering. The offering allows to manage and evaluate data of an agricultural holding. Such data can be used to optimise the processes of the holding. Fodder trading is supported. CRM functionalities are included in the performances as well.

2. Type(s) of Personal Data

The following data types are regularly objects of Processing:

- name, address
- access times and usage profiles
- free-text comments
- individual holding data on the production process of the holding of the Principal's customers
- economic situation of the holding (yields, costs, profit)

3. Data Subject Categories

Group of Data Subjects affected by data processing:

- Principal
- customers of the Principal
- Employees of the Principal's customer
- business partners of the Principal's customer (veterinarian, consultant...)

4. Persons Entitled to Issue Instructions at the Principal's

Name, First name: _____

Position: _____

Tel.: _____

E-Mail: _____

5. Persons Entitled to Receive Instructions at the Contractor's

Michael Schütze und Carsten Gieseler
Großenhainer Straße 101
01127 Dresden

Email: info@fodjan.de
Tel: +49 351 4188 6693

Appendix 2 - Technical and Organisational Measures of the Contractor

1. Confidentiality Art. 32 Abs. 1 lit. b GDPR

Entry Control = Nobody without authorization can enter the room in which the data processing system is located.	☒ Chip card/Transponder locking system ☒ Key control (e.g. key output) ☒ Careful selection of cleaning personnel
Server room Where is the server located?	☒ Serverlocker ☒ Cabinet locked? ☒ Data cables laid open? Other cables in the room? ☒ Electricity ☒ Water ☒ Server rooms not located under sanitary facilities or water-carrying pipes
Admission Control = No unauthorized use of the system	☒ Allocation of user rights ☒ Password policy incl. password length and composition ☒ Authentication with user name and password ☒ Demand different passwords for different services ☒ Passwordsave ☒ No unencrypted storage of passwords ☒ Screen lock or shutdown on inactivity ☒ Assignment of user profiles to IT systems ☒ Automatic locking in the event of multiple incorrect entries ☒ Lock external interfaces (USB) ☒ Restriction to company-owned mobile data carriers ☒ Using a software firewall ☒ Using a hardware firewall ☒ VPN (Virtual Privat Network) ☒ Use of anti-virus software

Access Control = No unauthorized reading, copying, modification or removal within the system.	☒ Right assignment according to the "need to know" principle: Delete, write, read... ☒ Logging of accesses to applications, in particular when entering, changing and deleting data ☒ Rights management by system administrator ☒ Number of administrators reduced to the "bare minimum" ☒ Separate password protection for individual, particularly sensitive DV applications ☒ Encryption of mobile data media ☒ Encryption of data carriers in notebooks ☒ Encryption of smartphone contents/tablets ☒ Physical deletion of data carriers before reuse ☒ Proper destruction of data carriers (DIN 32757) ☒ Use of document shredders or service providers ☒ Secure storage of data media Where? In the locked cabinet of managing director Mr. Schütze Rules? Only Mr. Schütze outputs the data carriers
Separation Control = Separate processing of data collected for different purposes.	☒ Physical separation ☒ Logical customer separation (software side) ☒ Creation of an authorization concept ☒ Sandboxing / separation of production and test system
Pseudonymisation (Art. 32 Abs. 1 lit. a GDPR; Art. 25 Abs. 1 GDPR) = The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without additional information, provided that such additional information is	☒ Use of pseudonymisation where possible (e.g. when passing on data) ☒ Appropriate choice of pseudonymization keys

kept separately and is subject to appropriate technical and organisational measures.	
--	--

2. Integrity (Art. 32 Abs. 1 lit. b GDPR)

Handover Control = No unauthorized reading, copying, modification or removal during electronic transmission or transport	☒ VPN ☒ E-Mail TLS encryption ☒ Encryption of mobile data media ☒ Encryption of data carriers in notebooks ☒ Encryption of smartphone contents/tablets ☒ Passing on of data in anonymized or at least pseudonymized form
Input Control = Determining whether and by whom personal data have been entered, altered or removed in data processing systems.	☒ Documentmanagement ☒ Allocation of rights to enter, change and delete data on the basis of an authorization concept

3. Availability and resilience (Art. 32 Abs. 1 lit. b GDPR)

Availability Control = Protection against accidental or deliberate destruction or loss / security.	☒ Mirrored hard disks (RAID) ☒ Mirrored systems/clusters ☒ Using a software firewall ☒ Using a hardware firewall ☒ Use of anti-virus software ☒ Regular updating of systems ☒ Creation of a backup & recovery concept (e.g. online/offline; on-site/off-site) ☒ Regular data recovery tests ☒ Storage of data backup in a secure, off-site location ☒ Fire and smoke detection systems ☒ Fire extinguishers in server rooms (CO2)
--	---

Rapid Recoverability (Art. 32 Abs. 1 lilt. c GDPR)	☒ Automated server setup
--	--

4. Procedures for periodic review, assessment and evaluation (Art. 32 Abs. 1 lit. d GDPR)

Data Protection-Management	☒ Appointment of a data protection officer ☒ List of processing activities ☒ Data protection impact assessments ☒ Training measure/awareness-raising measures with proof of completion ☒ Commitment to employee confidentiality ☒ Defined and documented processes ☒ Work instructions/policies with data protection background
Incident-Response-Management	☒ Definition of responsibilities and responsibilities for incidents (e.g. incident team) ☒ Defined reporting process ☒ Defined measures for relevant and conceivable incidents ☒ Defined escalation paths ☒ Current message and contact lists
Order Control No data processing within the meaning of Art. 28 GDPR without corresponding instructions from the Principal, e.g: Clear contract design, formalised order management, strict selection of the service provider, obligation to convince the client in advance, follow-up controls	☒ Selection of the contractor under due diligence aspects ☒ Ensuring the obligation of confidentiality by the contractor ☒ Contractor has appointed Data Protection Officer (if required by law) ☒ Contractual obligations and responsibilities ☒ Contract processing agreements ☒ Effective control rights vis-à-vis the contractor agreed ☒ Written instructions to the contractor (text form sufficient) ☒ Ensuring the destruction of data after completion of the order

Appendix 3 - Subcontractors

To ensure data processing on the Principal's behalf, the Contractor makes use of performances of third parties processing data on its behalf ("Subcontractors"). This relates to the following company/companies:

Subcontractors	Adress	Type of Service
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen Germany	Provider data center
Strato AG	Pascalstraße 10 10587 Berlin Germany	Provider data center
Loumaris UG (limited liability)	Mühlenstr. 6 06420 Könnern Germany	Server Administration Services
FastBill GmbH	Wildunger Str. 6 60487 Frankfurt am Main Germany	Accounting Software
HubSpot, Inc.	25 First Street Cambridge MA 02141 USA	CRM-System
Google Ireland Ltd	Gordon House Barrow Street Dublin	Crashreports in Firebase, Google Analytics, Google- Marketing-Services
1&1 IONOS SE	Elgendorfer Straße 57 56410 Montabaur Germany	Provider data center
Microsoft Ireland Operations, Ltd.	Attn: Data Protection One Microsoft Place South County Business Park Leopardstown, Dublin 18, D18 P521	Microsoft Online services, Azure Cloud, MS Office
Stripe Payments Europe Ltd.	1 Grand Canal Street Lower Grand Canal Dock Dublin	Payment provider

Subcontractors	Adress	Type of Service
Atlassian Pty Ltd.	Level 6, 341 George Street Sydney, NSW 2000 Australia	Software Service
Elbe Inkasso GmbH	Tiergartenstraße 8 01219 Dresden	Collection agency
DeepL GmbH	Maarweg 165 50825 Köln	Translation service provider
DSI GmbH Daten Service Informationssysteme	Carolinestraße 1 01097 Dresden	IT Service Provider
Adobe Systems Software Ireland Limited	4-6 Riverwalk City West Business Campus Saggart D24 Dublin Ireland	Adobe cloud services (Adobe sign)
Github Inc.	88 Colin P. Kelly Jr. Street San Francisco California 94107 USA	Online version management service for software development projects
Tempo Software Inc.	67 South Bedford Street Suite 400 West Burlington MA 01803 USA	Software Service
Pitch Software GmbH	Joachimstraße 7 10119 Berlin	Presentation Platform

You can view the continuously updated list of subcontractors on our homepage (<https://fodjan.com/en/order-processing-contract/>).