Data Processing Agreement

between

_____
_____
_____

as Data Controller (hereinafter referred to as the “Customer”)

and

foreknown GmbH
Brückenstr. 7
48231 Warendorf

as Data Processor (hereinafter referred to as the “Contractor”)

(The Customer and the Contractor together will hereinafter be referred to as the "Parties")

Preamble

The Customer wishes to commission the Contractor with the services specified in § 3, which include the processing of personal data. In particular, Art. 28 of the General Data Protection Regulation (GDPR) imposes certain requirements on commissioned processing, as is to be the subject of the services specified in § 3. To meet these requirements, the parties enter into the following agreement, the performance of which shall not be remunerated separately unless this is expressly agreed. The agreement serves to specify the mutual rights and obligations under data protection law.

§ 1 Definitions

Terms used in this Agreement which are defined by Article 4, 9 and 10 GDPR shall have the same meaning as those established by the relevant GDPR provision.

§ 2 Subject of the Agreement

(1) The Contractor shall provide services to the Customer in the field of consulting and development of software and shall be responsible for the

Terms of Use (foreknown) (“Main Contract”)

from _____ (Date: Conclusion of the Main Contract)

Service provider in the area of cloud computing. In this context, it offers the so-called "Software as a Service" model (SaaS model), i.e., it operates the software and IT infrastructure of the principal as an external IT service provider. In doing so, the Contractor obtains access to personal data and processes it exclusively on behalf of and according to the instructions of the Customer. The scope and purpose of the data processing by the Contractor result from the main contract.

(2) The Customer shall be responsible for assessing the permissibility of data processing. The parties conclude the present agreement to specify the mutual rights and obligations under data protection law. In case of doubt, the provisions of this Agreement shall take precedence over the provisions of the main contract.

(3) The provisions of this Agreement shall apply to all activities related to the main contract in which the Contractor and its employees or persons authorized by the Contractor come into contact with personal data originating from the Customer or collected for the Customer.

(4) The term of this contract shall be based on the term of the main contract, provided that the following provisions do not result in any obligations or rights of termination beyond this term.

§ 3 Right of Instruction

(1) The Contractor may only collect, process, or use data within the scope of the main contract and in accordance with the Customer’s instructions; this applies in particular with regard to the transfer of personal data to a third country or to an international organization. If the Contractor is required by the law of the European Union or of the Member States to which it is subject to carry out further processing, it shall notify the Customer of these legal requirements prior to processing.

(2) The Customer's instructions shall initially be determined by this Agreement and may thereafter be amended, supplemented, or replaced by individual instructions from the Customer's persons authorized to issue instructions, as set out in Annex 5, in writing or in text form vis-à-vis the Contractor (individual instructions). The Customer shall be entitled to issue corresponding instructions at any time. The instructions shall be confirmed in writing or in text form. They shall take into account a reasonable period of time for implementation at the Contractor's premises.

(3) The right to issue instructions includes instructions regarding the correction, deletion, and blocking of data. In the event of a change or long-term prevention of the persons named in Annex 5 who are authorized to issue instructions, the successor or representative shall be named to the contractual partner in text form without delay. Failure to immediately notify a change and its consequences shall not fall within the Contractor's sphere of risk but shall lie within the Customer’s sphere of risk.

(4) All instructions issued shall be documented by both the Customer and the Contractor. Instructions that go beyond the performance agreed in the main contract shall be treated as a request for a change in performance, which shall require acceptance by the Contractor.

(5) If the Contractor is of the opinion that an instruction of the Customer violates data protection provisions, it shall notify the Customer thereof without undue delay. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Customer.

(6) If there is an illegality in the contractor's sphere and if he would intentionally be involved in irregular or punishable actions, he may refuse the instruction with regard to the risk of punishment and liability.

(7) The Contractor may always refuse to carry out an obviously unlawful instruction. An instruction is obviously unlawful in particular if there is no legal basis for the processing activity, taking into account the relevant provisions of data protection law.

§ 4 Obligation to cooperate with the competent data protection supervisory authority

(1) The Client and the Contractor shall cooperate with the Supervisory Authority upon request in the performance of their duties.

(2) The competent supervisory authority for the Client is the State Commissioner for Data Protection _____.

(3) The competent supervisory authority for the Contractor is the State Commissioner for Data Protection of North Rhine-Westphalia.

§ 5 Type of Data processed and Group of affected Persons

(1) In the course of the performance of the Main Contract, the Contractor shall have access to the personal data specified in more detail in Appendix 1. These data comprise the special categories of personal data listed and marked as such in Appendix 1.

(2) The group of persons affected by the data processing is shown in Appendix 2.

§ 6 Protective Measures of the Contractor

(1) The Contractor is obliged to observe the statutory provisions on data protection and not to disclose information obtained from the Customer’s domain to third parties or expose it to their access. Documents and data are to be secured against knowledge by unauthorized persons, taking into account the state of technology.

(2) The Contractor shall design the internal organization in its area of responsibility in such a way that it meets the special requirements of data protection. It shall take all necessary technical and organizational measures to adequately protect the Customer's data pursuant to Art. 32 GDPR, in particular at least the measures of access control, access control, earmarking control, disclosure control, input control and availability control listed in Appendix 3. The Contractor reserves the right to change the security measures taken, while ensuring that the contractually agreed level of protection is not undercut.

(3) The contact persons for data protection are the managing directors of the contractor, Mr. Andreas grosse Austing and Mr. Bernfried Howe.

(4) The persons employed in data processing by the Contractor are prohibited from collecting, processing or using personal data without authorization. The Contractor shall oblige all persons entrusted by it with the processing and performance of this Agreement (hereinafter referred to as "Employees") accordingly (obligation of confidentiality, Art. 28 para. 3 lit. b GDPR) and shall ensure compliance with this obligation with due care. These obligations must be formulated in such a way that they remain in force even after the termination of this contract or the employment relationship between the employee and the contractor. The Customer shall be provided with appropriate evidence of the obligations upon request.

§ 7 Information Obligations of the Contractor

(1) In the event of disruptions, suspected data protection violations or violations of contractual obligations of the Contractor, suspected security-related incidents or other irregularities in the processing of personal data by the Contractor, by persons employed by it within the scope of the contract or by third parties, the Contractor shall inform the Customer without undue delay. The same shall apply to audits of the Contractor by the data protection supervisory authority.

(2) The Contractor shall immediately take the necessary measures to secure the data and to mitigate possible adverse consequences of the data subjects, inform the Customer thereof and request further instructions.

(3) In addition, the Contractor shall be obliged to provide the Customer with information at any time insofar as the Customer's data is affected by a breach pursuant to paragraph 1 above.

(4) If the Customer's data at the Contractor is endangered by seizure or attachment, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Customer thereof without undue delay, unless it is prohibited from doing so by court or administrative order. In this context, the Contractor shall inform all competent bodies without delay that the decision-making authority over the data lies exclusively with the Customer as the "responsible party" within the meaning of the GDPR.

(5) The Contractor shall inform the Customer without delay of any significant changes to the safety measures pursuant to § 6 Para. 2.

(6) A change in the person of the contact person for data protection shall be notified to the Customer without delay.

(7) The Contractor and, if applicable, its representative shall keep a register of all categories of processing activities carried out on behalf of the Customer, which shall contain all information pursuant to Article 30 (2) of the GDPR. The directory shall be made available to the Customer upon request.

(8) The Contractor shall cooperate in the creation of the procedure directory by the Customer by providing the Customer with the required information in an appropriate manner.

§ 8 Control rights of the Client

(1) The Customer shall satisfy itself of the technical and organizational measures of the Contractor prior to the commencement of data processing and thereafter regularly once a year. For this purpose, it may, for example, obtain information from the Contractor, have existing test certificates from experts, certifications or internal audits presented to it or personally inspect the Contractor's technical and organizational measures after timely coordination during normal business hours or have them inspected by a competent third party, provided that this third party is not in a competitive relationship with the Contractor. The Customer shall carry out inspections only to the extent necessary and shall not disproportionately disturb the Contractor's operating processes in the process.

(2) The Contractor undertakes to provide the Customer, upon the latter's written request and within a reasonable period of time, with all information and evidence required to carry out a check of the Contractor's technical and organizational measures.

(3) The Customer shall document the inspection result and notify the Contractor thereof within three weeks. In the event of errors or irregularities discovered by the Customer, the Customer shall inform the Contractor without delay. If facts are identified during the inspection, the future avoidance of which requires changes to the ordered procedure, the Customer shall inform the Contractor of the necessary procedural changes without undue delay. The Contractor shall then provide the Customer with a comprehensive and up-to-date data protection and security concept for the commissioned processing as well as on persons authorized to access the data at the Customer's written request. This shall also apply in the event that this becomes necessary for the Customer within the scope of an official

supervisory procedure, since the subject of the supervisory procedure is the processing of data of the Customer by the Contractor.

(4) The Contractor shall prove the obligation of the employees according to § 6 par. 4 to the Customer upon written request.

§ 9 Use of Subcontractors

(1) The contractually agreed services or the partial services described below shall be performed with the involvement of the subcontractors named in Appendix 4. Within the scope of its contractual obligations, the Contractor shall be authorized to establish further subcontracting relationships with subcontractors ("Subcontractor Relationship"), provided that it notifies the Customer thereof in advance and the Customer has given its prior written consent to the engagement of the subcontractor. The Contractor shall be obliged to carefully select subcontractors according to their suitability and reliability. When engaging subcontractors, the Contractor shall oblige them in accordance with the provisions of this Agreement and shall ensure that the Customer can exercise its rights under this Agreement (in particular its inspection and monitoring rights) directly against the subcontractors. If subcontractors in a third country are to be involved, the Contractor shall ensure that an appropriate level of data protection is guaranteed at the respective subcontractor (e.g., by concluding an agreement based on the EU standard data protection clauses). Upon request, the Contractor shall provide the Customer with evidence of 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 commissions third parties to provide services which are to be regarded as purely ancillary services. These include, for example, postal, transport and shipping services, cleaning services, telecommunications services without any specific reference to services provided by the Contractor for the Customer and security services. Maintenance and testing services constitute subcontractor relationships subject to approval insofar as these are provided for IT systems that are also used in connection with the provision of services for the Customer.

§ 10 Requests and Rights of Data Subjects

(1) The Contractor shall support the Customer with suitable technical and organizational measures in fulfilling the Customer’s obligations pursuant to Articles 12-22, 32 and 36 of the GDPR. The measures shall be discussed between the contracting parties on a case-by-case basis. They must be based on the scope of the performance obligations under the main contract and take place in consideration of the fact that the Customer is responsible for assessing the permissibility of the data processing.

(2) If a data subject asserts rights, such as the right to information, correction or deletion of his/her data, directly against the Contractor, the Contractor shall not react independently, but

shall immediately refer the data subject to the Customer and await the Customer's instructions. If such instructions are not issued within a reasonable period of time after notification with regard to the asserted right of the data subject, the resulting legal consequences do not fall within the Contractor's sphere of risk, but lie within the Customer’s sphere of risk.

§ 11 Liability

(1) For the compensation of damages suffered by a data subject due to inadmissible or incorrect data processing or use in the context of commissioned processing in accordance with the data protection laws, the Customer alone shall be responsible vis-à-vis the data subject in the internal relationship with the Contractor.

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

§ 12 Extraordinary Right of Termination

(1) The contracting parties may terminate this contract extraordinarily at any time for good cause.

(2) Good cause shall be deemed to exist for the Customer in particular if

- the Contractor violates provisions according to the GDPR intentionally or through gross negligence,
- the Contractor fails to comply with the Customer’s instructions, as described in § 4 of this Agreement, contrary to

does not comply with its contractual obligations. In the case of simple - i.e., neither intentional nor grossly negligent - violations of the provisions of the GDPR or obligations under this Agreement, the Principal shall set the Contractor a reasonable deadline within which the Contractor may remedy the violation.

(3) Good cause shall be deemed to exist for the Contractor in particular if the instructions of the Customer pursuant to § 4 of this Agreement are obviously unlawful and the Customer insists on the implementation of its instruction after having been notified of its unlawfulness. In the case of simple - i.e. not obviously unlawful - violations, the Contractor shall set the Customer a reasonable deadline within which the Customer may discontinue the instruction in writing or in text form.

(4) Termination of this contract in isolation from the main contract is excluded.

§ 13 Termination of the Main Contract

(1) The Contractor shall return to the Customer after termination of the main contract or at any time upon the Customer's request all documents, data and data carriers provided to the Contractor or - at the Customer's request, unless there is an obligation to store the personal data under Union law or the law of the Federal Republic of Germany - delete them. This shall also apply to any data backups at the Contractor. The Contractor shall provide documented proof of the proper deletion of any data still in existence. Documents to be disposed of shall be destroyed using a document shredder in accordance with DIN 32757-1. Data carriers to be disposed of shall be destroyed in accordance with DIN 66399.

(2) The Customer has the right to control the complete and contractually compliant return or deletion of the data at the Contractor in a suitable manner.

(3) The Contractor shall be obligated to treat as confidential any data of which it becomes aware in connection with the main contract, even beyond the end of the main contract. The present agreement shall remain valid beyond the end of the main contract as long as the Contractor has personal data at its disposal which have been forwarded to it by the Customer or which it has collected for the Customer.

§ 14 Final Provisions

(1) Amendments and supplements to this agreement must be made in writing. This shall also apply to any waiver of this formal requirement. The precedence of individual contractual agreements remains unaffected by this.

(2) If any provision of this Agreement is or becomes invalid or unenforceable in whole or in part, the validity of the remaining provisions shall not be affected thereby.

(3) This agreement is subject to German law. The exclusive place of jurisdiction is Münster.

Appendix:

Appendix 1 - Description of the data / categories of data requiring special protection
Appendix 2 - Description of the data subjects / groups of data subjects
Appendix 3 - Technical and organizational measures of the contractor
Appendix 4 - Approved subcontractors
Appendix 5 - Persons authorized to give instructions

_____	_____
Date, Customer Signature	Date, Contractor Signature

Appendix 1 – Description of the Data / Categories of Data requiring special Protection

- User data (e-mail and password (hashed))
- Personal master data (first name, last name, address)
- Employee data (name, e-mail, location, contracts)
- Customer data (name, e-mail, address, contact person)

Appendix 2 – Description of the affected Persons / Groups of affected Persons

- Employees of the Customer
- Customers of the Customer

Appendix 3 – Technical and organizational Measures of the Contractor

Description of the contractor's technical and organizational measures for:

Pseudonymization

The data entered into the software by the Customer cannot be pseudonymized by the Customer.

However, if data is required by the Contractor's development department to reproduce a specific error of the Customer in the software, it will be pseudonymized so that no conclusions can be drawn about information on real persons (employee and customer contacts) as well as customer names and project names. This concerns the following data:

- User data (e-mail and password)
- Personal master data (first name, last name, address)
- Employee data (name, e-mail, contracts)
- Customer data (name, e-mail, address, contact person)

Encryption

- The software is accessed via the web browser. The data is transmitted in encrypted form (SSL).
- Passwords are stored hashed in the database.
- Files uploaded via the web interface are stored encrypted in the server's file system.
- Backups of the database and data are stored encrypted.

Confidentiality

Admission Control

The servers required to operate the software are operated by Hetzner Online GmbH. Access control is guaranteed by Hetzner Online GmbH as follows:

- 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 (each customer exclusively for their colocation rack)
- Guidelines for escorting and tagging guests in the building.
- 24/7 staffing of data centers
- Video surveillance at entrances, exits, security gates and server rooms
- Access to the premises for persons outside the company (e.g., visitors) is restricted as follows: only in the company of a Hetzner Online GmbH employee.

Access Control

- Access to the web interface of the software is password protected. The password is assigned by the Customer's access-authorized persons themselves. The contractor has no access to the plain text passwords. Only for the first login to the system a password is generated and sent to the Customer. The Client is obliged to change this password after the first login.
- Access to the servers by the Contractor is only possible by means of a secured procedure (SSH). The passwords/access keys required for this are stored in encrypted form in a special security application. Only persons authorized by the contractor may access this application and thus the servers.
- By means of regular security updates (in accordance with the respective state of the art), the Contractor ensures that unauthorized access is prevented.

Segregation Control and Earmarking Control

- The software is multi-client capable, i.e., the data of one client cannot be accessed by another client. The separation control between the clients is implemented in the software (logical separation).
- During the test phase of the software, a new client is set up for the client on the "demo system" (logical separation).
- After the test phase, a separate server is provided for the client. All data is stored physically separate from each other (Physical separation).

Availability, Resilience

Availability Control

- Backup and recovery concept with daily backup of all relevant data.
- Expert use of protection programs (virus scanners, firewalls, encryption programs).
- Use of hard disk mirroring for all relevant servers (by Hetzner).

- Monitoring of all relevant servers.
- Use of uninterruptible power supply, backup power system (by Hetzner).
- Permanent active DDoS protection (by Hetzner)

Recoverability

- An escalation chain is defined for all internal systems that specifies who is to be informed in the event of an error in order to restore the system as quickly as possible.

Integrity

Transfer Control

- All employees have been instructed in accordance with Article 32 (4) of the GDPR and are obliged to ensure that personal data is handled in accordance with data protection requirements.
- Data protection-compliant deletion of data after completion of the order.

Input Control

- The responsibility of input control is incumbent on the customer.

Procedures for regular Review, Assessment and Evaluation

- Our employees are instructed in data protection law at regular intervals, and they are familiar with the procedural instructions and user guidelines for data processing on behalf of the customer, also with regard to the customer's right to issue instructions.
- The effectiveness of the technical and organizational measures to ensure the security of processing is regularly reviewed, assessed, and evaluated by the data protection officers and adjusted to the state of the art.

Appendix 4 – Approved Subcontractors

The following companies are approved subcontractors within the meaning of § 9:

- Hetzner Online GmbH
  Industriestr. 25
  91710 Gunzenhausen
  Deutschland

Appendix 5 – Persons authorized to give Instructions

Persons authorized to give instructions to the customer are:

- _____
- _____

The recipients of instructions at the contractor are:

- Andreas grosse Austing
- Bernfried Howe