Appendix 1 – Data Processing Agreement (Article 28 of the GDPR)

Between XXXXXXXXXXXXXX – the Controller - hereinafter referred to as the Client – and

Fairmas GmbH, EUREF-Campus 13, 10829 Berlin – Processor – hereinafter referred to as the Supplier.

1. Subject matter and term of the order

(1) Subject Matter

The subject matter and term of this Order are laid down in the aforementioned Contract (hereinafter referred to as the Service Agreement).

(2) Term

The CONTRACT period (Term) shall correspond to the term(s) of the Service Agreement(s) and shall in any case last for as long as the Supplier processes the personal data of the Client (including backups).

(3) In the event that different agreements have been made between the Client and the Supplier regarding data privacy, this CONTRACT shall take precedence over any other agreement related to order processing, unless the Parties to this Contract expressly agree otherwise.

2. Order Content in Detail

(1) Nature and Purpose of Envisaged Data Processing

The nature and purpose of the Supplier processing personal data for the Client are specified in the Service Agreement(s) referred to in clause 1 above.

(2) Type of Data

The following types/categories of personal data shall be processed (list/description of data categories):

- person's master data (title, first name, last name);
- contact details (phone, email);
- contract master data (contractual relationship, product or contractual interest);
- client history;
- contract billing and payment data;
- planning and control data;
- company's financial data;
- wage or salary information.

(3) Categories of Data Subjects

The categories of data subjects shall include

- customers;
- employees;
- contact persons.

3. Technological or Organisational Measures

(1) Pursuant to Article 32 of the GDPR, the Supplier shall take all technological or organisational measures required within the scope of its responsibility to protect personal data and shall submit all relevant documentation to the Client for review. Once the measures recorded are approved by the Client, they shall form the basis of this CONTRACT.

(2) Should the review/audit by the Client result in adjustments to be made, they shall be implemented by mutual consent.

(3) The technological or organisational measures agreed upon shall be subject to technological advancement and development. To this effect, the Supplier shall be permitted to implement adequate alternative measures in the future, whereby the security level of the measures agreed upon pursuant to Annex 1 may not be compromised. The Supplier shall record any significant changes and promptly inform the Client accordingly.

(4) Remote Work

Homeworking or teleworking: the processing of data pursuant to this CONTRACT may be permitted at premises other than those of the Supplier and may be carried out at private homes.

The Supplier undertakes measures to ensure the confidentiality of the data as well as the security and controllability of the processing to the same extent by means of suitable regulations and security measures as it would be the case if the service were performed from the Supplier's location. In case of any deviation, it is required to obtain a separate written consent of the Client.

4. Rights of Data Subjects

(1) The Supplier shall support the Client within the scope of its responsibility in responding to and complying with requests by data subjects concerning their data privacy rights and shall do so by means of appropriate technological or organisational measures if possible. The Supplier may neither provide information on or transfer, correct or erase data nor may it restrict the processing of data on behalf of the Client on its own accord, but may solely do so on the basis of the Client's recorded instructions. Should a data subject contact the Supplier directly in this regard, the Supplier shall promptly forward any such request to the Client.

(2) If included in the scope of services, the rights to information, correction, restrict processing, erasure as well as data portability shall be promptly ensured by the Supplier based on the recorded instructions of the Client.

5. Quality Assurance and Other Obligations of the Supplier

(1) Apart from complying with the provisions of this Order, the Supplier shall also comply with its legal obligations pursuant to the GDPR. To this effect, the Supplier shall ensure that the obligations listed hereunder are met.

a) Written appointment of a data protection officer who performs his or her duties in accordance with Articles 38 and 39 of the GDPR. The contact details of the data protection officer shall be communicated to the Client for the purpose of direct contact upon request. The respective current contact details are easily accessible on the contractor's homepage (Privacy Policy - Fairmas).

Questions and concerns regarding data protection can also be sent directly to the following email address: datenschutz@fairmas.com

b) Pursuant to Articles 28 paragraph 3 sentence 2 lit. b, 29, 32 paragraph 4 of the GDPR all matters pertaining to this Order have to be kept strictly confidential. The Supplier shall ensure that the Order is solely performed by employees that have been obligated to maintain confidentiality and have previously been familiarised with the relevant data protection provisions. The Supplier and any person reporting to the Supplier having legitimate access to the personal data may exclusively process such data in accordance with the Client's instructions, including the rights granted in this CONTRACT, unless they are by law obligated to process data beyond the scope of the Client's instructions.

c) Upon request, the Client and the Supplier shall cooperate with a supervisory authority when performing their duties.

d) The Client shall be immediately informed of any investigations or measures taken by a supervisory authority in regard to this CONTRACT. This shall also apply if the competent authority carries out investigations at the Supplier's premises in terms of misdemeanour or criminal proceedings pertaining to the processing of personal data.

e) In the event that the Client is subject to investigations by a supervisory body, or subject to a regulatory offence or criminal proceedings, a liability claim by a data subject or a third party, or any other claim or request for information with regard to the order processing by the Supplier, the Supplier shall support the Client to the best of its ability.

f) The Supplier shall regularly monitor its internal processes as well as the technological and organisational measures taken to ensure that the processing of data within the Supplier's field of responsibility is carried out pursuant to the provisions of the applicable data protection law, and that the rights of the respective data subjects are protected and guaranteed.

g) The technological and organisational measures taken shall be demonstrated if and when the Client exercises its Right of Control pursuant to Clause 8 of this CONTRACT.

h) The Supplier shall immediately report any data privacy violation to the Client, and it shall do so in a way to ensure that the Client may comply with its legal obligations, in particular those pursuant to Articles 33, 34 of the GDPR. The Supplier shall record the entire process and shall provide the Client with the respective documentation for any further measures to be taken.

i) Within the scope of its responsibility and to the extent possible in light of its existing information obligations, the Supplier shall assist the Client vis-à-vis supervisory bodies and data subjects, and shall to this effect immediately provide all relevant information.

j) In the event that the Client is obligated to conduct a data protection impact assessment, the Supplier shall provide assistance with regard to the type of processing carried out and the information obtained. The same shall apply if the Client is obligated to consult the competent data protection supervisory body.

(2) This CONTRACT shall not exempt the Supplier from compliance with other provisions of the GDPR.

6. Subcontracting relationships

(1) Subcontracting relationships within the meaning of this provision shall be deemed to be those services that are directly related to the provision of the primary service. Ancillary services used by the Supplier, e.g., telecommunication services, postal/transportation services, cleaning services or security services, shall not be included. Maintenance and testing services shall constitute a subcontracting relationship, provided they are rendered for IT systems that are related to a service provided by the Supplier pursuant to this CONTRACT. However, the Supplier shall be obligated to enter into appropriate and legally binding contractual agreements to ensure that the Client's data are protected and secure if and when ancillary services are outsourced, and the Supplier shall take measures to monitor such ancillary services.

(2) Pursuant to Article 28 paragraph 2 sentence 2 of the GDPR, the Client shall hereby generally authorise the Supplier to enlist the services of further order processors (Subcontractors) for processing the Client's data.

The applicable overview of further Suppliers shall be published by the Supplier on the website listed hereunder. The up-to-date list may be accessed by the Client at any time:

https://fairmas.com/data-protection-software/

Furthermore, the Client may request a copy of the list of further Suppliers (Subcontractors) at any time in writing or by email addressed to datenschutz@fairmas.com.

The Client may choose to be automatically informed by the Supplier of any changes to the list of further Suppliers (Subcontractors). To this effect, the Client is requested to provide a role account email address here: _____

The aforementioned duty to inform shall not apply if no email address is provided or if the above email address cannot be reached.

Upon request, the Client may be furnished with the respective contractual agreements reached with further Suppliers (Subcontractors), whereby business clauses that are unrelated to data privacy shall be excluded.

(3) The personal data of the Client may only be transferred to a Subcontractor, and the Subcontractor may in turn only start working on such data once all requirements for subcontracting have been met. In view of the risks involved, the Supplier shall check whether the Subcontractor implements and complies with the technological and organisational measures taken before the Subcontractor starts processing the personal data of the Client, and the Supplier shall continue to regularly monitor compliance with and implementation of said measures on the part of the Subcontractor. The Supplier shall provide the monitoring results to the Client upon request. Furthermore, the Supplier shall ensure that the Client may directly exercise its rights under this Agreement (in particular its Right of Control) vis-à-vis any Subcontractor.

(4) In the event that a Subcontractor provides the services agreed upon from outside the EU/EEA, the Supplier shall take appropriate measures to ensure that any such service provision is permissible under data protection law. The same shall apply if service providers within the meaning of paragraph 1 sentence 2 are to be used.

(5) Any outsourcing by a Subcontractor shall require the express consent of the Supplier (at least in text form).

All provisions of previous contracts concluded shall also apply to further Subcontractors.

7. International transfer of data

(1) Any transfer of personal data to a third country or to an international organisation shall be subject to written instructions by the Client and shall be in compliance with the requirements for the transfer of personal data to third countries pursuant to Chapter V of the GDPR.

The processing of data contractually agreed upon shall exclusively be done in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area.

(2) Should the Client request that data be transferred to third parties in a third country, the Client shall be responsible for compliance with Chapter V of the GDPR.

8. Client's right of control

(1) The Client shall reserve the right to examine the work carried out in consultation with the Supplier, or to have checks done by examiners to be named in some instances. It shall have the right to ascertain that the Supplier complies with the provisions of this Agreement by carrying out spot checks at the Supplier's premises. The Supplier is generally to be notified of any such spot check in good time.

(2) The Supplier shall ensure that the Client may convince itself that the Supplier has met its obligations pursuant to Article 28 of the GDPR. Upon request, the Supplier shall undertake to provide the Client with all the information required and shall in particular provide proof that all technological and organisational measures have been implemented.

(3) Evidence of technological-organisational measures having been taken in compliance with the specific requirements pertaining to data protection in general as well as with regard to this Order in particular may be provided by way of

- compliance with the approved codes of conduct pursuant to Article 40 of the GDPR;
- certification in accordance with the criteria of an accredited certification scheme pursuant to Article 42 of the GDPR;
- latest attestations, reports or extracts from reports by independent bodies (e.g., auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors);
- appropriate certification by IT security audit or data protection audit (e.g., in accordance with the BSI security baseline).

9. Client's Authority to give instructions

(1) The Supplier shall solely process personal data on the basis of recorded instructions by the Client, unless it is obligated to process such data pursuant to the law of the respective member state or pursuant to European Union law. The Client shall promptly confirm verbal instructions (at least in text form). The Client's initial instructions shall be laid down in this Agreement.

(2) If the Supplier is of the opinion that an instruction contravenes data protection regulations, it shall immediately inform the Client accordingly. The Supplier shall be entitled to suspend the task in question until such time that the Client either confirms or amends the instruction concerned.

10. Erasure and Return of Personal Data

(1) No copies or duplicates of data shall be made without the prior knowledge of the Client. This shall not apply to security copies, provided they are required to ensure proper data processing, as well as to data required to comply with statutory retention requirements.

(2) Upon completing the work contractually agreed upon, or earlier upon request by the Client – at the latest upon termination of the CONTRACT or Service Agreement(s) – the Supplier shall hand the Client all documents and processing utilisation results prepared as well as databases that have come into its possession in the course of the contractual relationship, or the Supplier shall destruct any such data pursuant to data protection law upon prior consent. The same shall apply to testing or rejection materials. The erasure protocol shall be submitted upon request.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

Appendix 1 to the Data processing agreement – Technical and Organizational Measures

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

(1) Physical Access Control
No unauthorised access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems

(2) Electronic Access Control
No unauthorised use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, and encryption of data carriers/storage media

(3) Internal Access Control (permissions for user rights of access to and amendment of data)
No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events

(4) Isolation Control
The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing;

(5) Pseudonymisation (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)
The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

(1) Data Transfer Control
No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;

(2) Data Entry Control
Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

(1) Availability Control
Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning

(2) Rapid Recovery (Article 32 Paragraph 1 Point c GDPR);

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

(1) Data Protection Management;

(2) Incident Response Management;

(3) Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);

(4) Order or Contract Control
No third party data processing as per Article 28 GDPR without corresponding instructions from the Client, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.

Appendix 2 – Subcontractors

Pursuant to clause 6 (1) of the Order Processing Agreement, the Supplier shall provide an updated list of Subcontractors either upon request or by submitting it to the email address stated in the Agreement. The list below shall therefore only apply at the time the Agreement is signed, and it shall be superseded by relevant up-to-date versions.

List of Subcontractors pursuant to clause 6 of the Order Processing Agreement between the Client and the Supplier – as of **1 February 2024**

Subcontractor	**Address/Country**	**Services Rendered**
Host Europe GmbH	Hansestr. 111 51149 Köln Germany	Provision, management and maintenance of IT hardware (server) and data lines.
Hetzner Online GmbH	Industriestraße 25 91710 Gunzenhausen Germany	Provision, management and maintenance of IT hardware (server) and data lines.
Microsoft Corporation	One Microsoft Way Redmond, Washington 98052 USA	Provision, management and maintenance of IT hardware (server) and data lines, including provision of software applications for editing and displaying data as well as support and consulting services.
Entity in charge in Europe: Microsoft Ireland Operations Ltd.	Attn: Data Protection One Microsoft Place South County Business Park, Leopardstown Dublin 18, D18 P521 Ireland	
Sendinblue GmbH ("Brevo")	Köpenicker Str. 126 10179 Berlin Germany	Transmission of system messages and reports to software users and registered recipients by email or SMS.
IONOS SE	Elgendorfer Straße 57 56410 Montabaur Germany	Receipt, storage and forwarding of business management data and transmission of system messages and reports to software users and registered recipients by email or SMS.