Processing in accordance with Article 28 General Data Protection Regulation (GDPR)

Agreement

between

....

- the Controller – hereinafter referred to as the Client -

and

Hako GmbH

Hamburger Straße 209-239

23843 Bad Oldesloe

- the Processor – hereinafter referred to as the Supplier -

1. Subject matter and duration of the Order of Contract

(1) Subject matter

The subject matter of the order results from the contract for the fee-based use of the Hako Fleet-Management.

(2) Duration

The duration of this order corresponds to the term of the above contract of the framework contract.

2. Specification of the Order or Contract Details

(1) Nature and Purpose of the intended Processing of Data:

The nature and purpose of the processing of personal data by the contractor for the client is to grant the use of the Hako Fleet Management Portal as software as a service. Details of the processing can be found in the relevant terms of use to this contract.

(2) Type of Data

The Subject Matter of the processing of personal data comprises the following data types/categories:

- Personal Master Data (Key Personal Data)
- Contact Data
- Key Contract Data (Contractual/ Legal Relationships, Contractual or Product Interest)
- Customer History
- Contract Billing and Payments Data
- Planning and control data

(3) Categories of Data Subjects

The Categories of Data Subjects are precisely defined in the Service Agreement under:

- Customers
- Employees

3. Technical and Organisational Measures

(1) The contractor shall document the implementation of the technical and organisational measures set out and required in the run-up to the awarding of the contract before the start of the processing, in particular with regard to the specific execution of the contract, and shall hand them over to the client for inspection. If accepted by the Client, the documented measures shall become the basis of the contract. If the examination/audit of the Client reveals a need for adaptation, this shall be implemented by mutual agreement.

(2) The contractor shall establish security pursuant to Art. 28 (3) lit. c, 32 DS-GVO, in particular in connection with Art. 5 (1), (2) DS-GVO. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and the resilience of the systems. In this context, the state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR must be taken into account [details in Annex 1].

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures must not be undercut. Significant changes shall be documented.

4. Rectification, restriction and erasure of data

(1) The contractor may not correct, delete or restrict the processing of data processed under the contract on its own authority but only in accordance with documented instructions from the client. Insofar as a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Client without delay.

(2) Insofar as included in the scope of services, deletion, the right to be forgotten, correction, data portability and information shall be ensured directly by the contractor in accordance with documented instructions from the client.

5. Quality assurance and other duties of the Supplier

In addition to compliance with the provisions of this Order, the Contractor shall observe the statutory obligations pursuant to Articles 28 to 33 of the GDPR; in this respect, the Contractor shall in particular ensure compliance with the following requirements:

a) a) Ms. Astrid Bartel [Hako GmbH, Hamburger Straße 209-239, 23843 Bad Oldesloe, Phone: +49-4531-806-0, Fax: +49-4531-806-338, privacy@hako.com] is appointed as data protection officer at the Contractor.

b) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so by law.

c) Implementation of and compliance with all Technical and Organisational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR [details in Annex 1].

d) The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.

e) The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Order or Contract.

f) Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by the Supplier, the Supplier shall make every effort to support the Client.

g) The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

h) Verifiability of the Technical and Organisational Measures conducted by the Client as part of the Client’s supervisory powers referred to in item 7 of this contract.

6. Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software

of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

(2) The Supplier may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from the Client.

The outsourcing to subcontractors of changing the existing subcontractor are permissible when:

- The Supplier submits such an outsourcing to a subcontractor to the Client in writing or in text form with appropriate advance notice; and
- The Client has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Supplier; and
- The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(3) The transfer of personal data from the Client to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

(4) The provision of the contractually agreed data processing by subcontractors shall take place exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 et seq. DS-GVO are fulfilled.

(5) Further outsourcing by the subcontractor requires the express consent of the main Client (at the minimum in text form); as well requires the express consent of the Supplier (at the minimum in text form); all contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

7. Supervisory powers of the Client

(1) The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

(2) The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR**.** The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

(3) Evidence of such measures, which concern not only the specific Order or Contract, may be provided by

- Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
- Certification according to an approved certification procedure in accordance with Article 42 GDPR;
- Current auditor’s certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor);

- A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or ISO/IEC 27001).

(4) The Supplier may claim remuneration for enabling Client inspections.

8. Communication in the case of infringements by the Supplier

(1) The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

b) The obligation to report a personal data breach immediately to the Client

c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.

d) Supporting the Client with its data protection impact assessment

e) Supporting the Client with regard to prior consultation of the supervisory authority

(2)The Supplier may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Supplier.

9. Authority of the Client to issue instructions

(1) The Client shall immediately confirm oral instructions (at the minimum in text form).

(2) The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its

possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on 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.

11. Place of jurisdiction

(1) Place of jurisdiction is the local court of the Client.

____

Place, Date, Signature
Controller

____

Place, Date, Signature
Processor

Annex 1 – Technical and Organisational Measures

1. Organisational Measures

- Employees are contractually bound to observe data protection, as well as where appropriate to the secrecy of telecommunications
- Procedure-independent plausibility and safety tests exist (for example technical supported or from external).

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

- 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
- 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, encryption of data carriers/storage media
- 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
- Isolation Control

  The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing;
- 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.

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

- 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;

- 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

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

- 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
- Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR)

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

- Data Protection Management;
- Incident Response Management;
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);
- 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.