Agreement for processing of data

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

I. Preamble

This agreement is concluded between the provider (Contabo GmbH; below also named „supplier“) and the customer (below also named „client“; together named „contracting parties“) in addition to the existing main contract which is based upon the customer’s order and the provider’s general terms and conditions. In case the provider has to process personal data for which the customer is responsible according to regulation 2016/679 (General Data Protection Regulation; GDPR), while fulfilling his duties arising from the main contract, the contracting parties precautionary conclude the following agreement for processing of data corresponding to Article 28 Paragraph 9 GDPR in order to substantiate the mutual rights and duties in case of a possible data processing by the provider.

II. Subject matter and duration of the contract

The subject matter and the duration of the contract result from the current service description and the general terms and conditions in force at the time of placing the order.

III. Specification of the contract details

1. Nature and purpose of processing of personal data by the supplier for the client are precisely defined in the current service description and the general terms and conditions in force at the time of placing the order.
2. The undertaking of the contractually agreed processing of data shall be carried out exclusively within a member state of the European Union (EU) or within a member state of the European Economic Area (EEA). Each and every transfer of data to a state which is not a member state of either the EU or the EEA requires the prior agreement of the client and shall only occur if the specific conditions of Article 44 et seq. GDPR have been fulfilled.
3. The subject matter of the processing of personal data comprises the following data categories:
    - Personal master data (key personal data), e.g. name, address
    - Company data, e.g. employees, addresses, bank details, tax data
    - Contact data, e.g. telephone, e-mail
    - Key contract data, e.g. server data, login data
    - Customer logs, e.g. login history, used IP-addresses
    - Process data, e.g. e-mail tickets, network disturbances
    - Customer history
    - Contract billing and payments data
    - Disclosed information, e.g. credit reference agencies or from public directories
4. The categories of data subjects comprise employees and freelancers of the client as well as his customers, potential customers, website visitors, suppliers and other persons whose personal data have been stored on his servers.

IV. Technical and organisational measures

1. The contracting parties agree upon the technical and organisational measures constituted in appendix 1 of this agreement. This appendix 1 is part of the contract on hand.
2. The supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account. [Details in Appendix 1]
3. The technical and organisational measures are subject to technical progress and further development. In this respect, it is permissible for the supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

V. Rectification, restriction and erasure of data

1. The supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the client, but only on documented instructions from the client. Insofar as a data subject contacts the supplier directly concerning a rectification, erasure, or restriction of processing, the supplier will immediately forward the data subject's request to the client.
2. Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the supplier in accordance with documented instructions from the client without undue delay.

VI. Quality assurance and other duties of the supplier

In addition to complying with the rules set out in this contract, the supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the supplier ensures, in particular, compliance with the following requirements:

1. Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR. His / her current contact details are always available and easily accessible on the website of the supplier.
2. Confidentialy 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.

3. 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 Appendix 1].
4. The client and the supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.
5. The client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this 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 contract.
6. 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 contract data processing by the supplier, the supplier shall make every effort to support the client.
7. 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.
8. Verifiability of the technical and organisational measures conducted by the client as part of the client's supervisory powers referred to in item VIII of this contract.

VII. 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 based on the following agreement:
   Outsourcing to subcontractors is 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. If the subcontractor provides the agreed service outside the EU/EEA, the supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures.
5. Further outsourcing by the subcontractor 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.

VIII. Supervisory powers of the client

1. The client has the right, after consultation with the supplier and only during normal working hours without disturbing operations, 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 by means of random checks. The audits have to be announced to the supplier with a lead time of no less than 10 working days (Mon-Fri - not 24 and 31 December), in the case of a data security event of not less than 5 business days. The customer must take proper due care in the course of the business process, as well as to keep the supplier's business and business secrets. Any audits by a third party on behalf of customer are subject to supplier's prior written consent.
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. The supplier will claim remuneration for enabling client inspections.

IX. 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:
    - 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.
    - The obligation to report a personal data breach immediately to the client.
    - 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.
    - Supporting the client with its data protection impact assessment.
    - Supporting the client with regard to prior consultation of the supervisory authority.
2. The supplier will 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.

X. 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.

XI. 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 main contract, the supplier shall 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 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.

XII. Term of this agreement / termination

1. The term and termination of this agreement shall be governed by the terms of the term and termination of the main contract. A termination of the main contract automatically results in a termination of this agreement. An isolated termination of this agreement is excluded. A termination for important reasons remains unaffected.
2. Termination requires the written form to be effective.

XIII. Final clauses

1. The court of jurisdiction for all disputes arising from this agreement shall be Munich.
2. German law shall apply to this agreement, with exclusion of international private law.
3. Changes and additions to this agreement and all of its components - including any warranties of supplier - require a written agreement and the explicit reference to the fact that they constitute amendments or supplements to these terms. This also applies to waiving the requirement for making such changes in writing.
4. Should individual provisions of this agreement be or become invalid in whole or in part, the validity of the remaining provisions shall remain unaffected thereby. The contracting parties undertake, in this case, to replace the invalid provision with an effective provision which comes as close as possible to the economic purpose of the invalid provision. The same applies to any gaps in this agreement.

Appendix 1: Technical and organisational measures

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

- **Physical Access Control**
  No unauthorised access to data processing facilities, e.g.: chip cards, keys, electronic door openers, facility security services, 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
- **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

II. 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

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

- **Availability Control**
  Prevention of accidental or willful destruction or loss, e.g.: backup strategy (if explicitly ordered by customer), Uninterruptible Power Supply (UPS) at the data center Nuremberg, virus protection, firewall, reporting procedures and contingency planning
- **Rapid Recovery** (Article 32 Paragraph 1 Point c GDPR)

IV. 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)**
- **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, formalized order management, strict controls on the selection of the service provider, duty of pre-evaluation, supervisory follow-up checks.