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

Agreement

between

xxxxx

– the Controller – hereinafter referred to as the Client –

and

xxxxx

– the Processor - hereinafter referred to as the Supplier;

(hereinafter this agreement referred to as the Order or Contract)

1. Subject matter and duration of the Order or Contract

(1) Subject matter

The Subject matter of the Order or Contract results from the Service Agreement..... dated ....., which is referred to here (hereinafter referred to as Service Agreement).

Kommentiert [JA1]: Pls. add the corresponding service agreement reference and the date

(2) Duration

The duration of this Order or Contract corresponds to the duration of the Service Agreement.

2. Specification of the Order or Contract Details

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

☐ Nature and Purpose of Processing of personal data by the Supplier for the Client are precisely defined in the Service Agreement dated ..... .

Kommentiert [JA2]: Is "Nature and Purpose of Processing of personal data really defined in the Service Agreement? If not, it must be added (in the service agreement or in the data processing agreement.

☐ 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.

(2) Type of Data

Kommentiert [JW3]: Pls. fill in all involved data categories

☐ The Subject Matter of the processing of personal data comprises the following data types/categories (List/Description of the Data Categories)

- ☐ Personal Master Data (Name, Surname)
- ☐ Contact Data
- ☐ Contract Billing and Payments Data
- ☐ Other: Any other categories of personal data which the Client inputs into databases or provides during the provision of services under the Service Agreement.

(3) Categories of Data Subjects

☐ The Categories of Data Subjects comprise:

- ☐ Customers
- ☐ Partners
- ☐ Employees
- ☐ Contact Persons
- ☐ Other: Any other groups of data subjects the personal data of whom partners of the Territory Representative choose to input into databases or provide during the provision of services.

Kommentiert [JW4]: Please fill in all involved data subjects

3. Technical and Organizational Measures

(1) The Supplier maintains appropriate technical and organizational measures, internal controls and data security routines (including pursuant to Article 32 of the GDPR) intended to protect the Personal Data against accidental loss or change, unauthorized disclosure or access, or unlawful destruction. The technical and organizational measures are listed in Appendix 1 to this Contract.

(2) The Technical and Organizational 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.

4. 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) Nevertheless, the Supplier shall, taking into account the nature of the processing, assist the Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Data Protection Legislation (including Chapter III of the GDPR).

5. Quality assurance and other duties of the Supplier

In addition to complying with the rules set out in this Order or 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:

a) ☐ Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR.
The Supplier has appointed Name, Address, phone-number, e-Mail, as Data Protection Officer.

Kommentiert [JW5]: Please enter data oft he DPO, if applicable

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 familiarized 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 Organizational 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].
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 Organizational 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. In addition:

a) ☐ The Client agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

Company subcontractor	Address/country	Service

b) ☐ 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) If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.
(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.

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

8. Communication in the case of infringements by the Supplier

(1) Taking into account the nature of processing and the information available to the Supplier, it 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.

(2) The Supplier may claim compensation for support services which are not included in the description of the services according to the Service Agreement 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 in writing (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.

Appendix - Technical and Organizational Measures

Kommentiert [JA6]: The Measures are Examples. Supplier needs to enter the actual measures taken to protect the data.

These measures will be checked by the Controller if they are sufficient to maintain compliance with GDPR.

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

- Physical Access Control
  No unauthorized access to Data Processing Facilities, use of 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 unauthorized use of the Data Processing and Data Storage Systems, use of (secure) passwords, automatic blocking/locking mechanisms, encryption of data carriers/storage media.
- Internal Access Control (permissions for user rights of access to and amendment of data)
  No unauthorized Reading, Copying, Changes or Deletions of Data within the system, use of rights authorization concept, need-based rights of access, logging of system access events
- Isolation Control
  The isolated Processing of Data, which is collected for differing purposes, multiple Client support, sandboxing;

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

- Data Transfer Control
  No unauthorized Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, use of Encryption, Virtual Private Networks (VPN), electronic signature;

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

- Availability Control
  Prevention of accidental or willful destruction or loss, having a 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);

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

Information security management policies are in progress.