Commissioned Data Processing in Pursuance of Art. 28 GDPR

PureLink
digital solutions

AGREEMENT BETWEEN:

1. Controller

Company:
Street:
Post Code | Town:

[If applicable: Authorised Representative in accordance with Article 27 GDPR:]

The Client | Customer

And

2. Processor

PureLink GmbH
Managing Director Christian Ahrens
Von-Liebig-Str. 10
48432 Rheine, Germany

The Contractor | Supplier

In addition to the Distribution Agreement (Main Contract)
the Parties close this subsequent contract for the processing of the Client's data by the Contractor.

PREAMBLE:

This Commissioned Processing Agreement (AV) supplements any contractual agreement (including any related or equivalent documents such as service descriptions, SaaS, appendices, attachments, etc.) between **PureLink GmbH** and the customer or PureLink GmbH and any affiliated companies on the purchase of products, services and deliveries from PureLink, insofar as personal data will be processed by **PureLink** on behalf of the customer, or with customer affiliated companies (Main Contract).

This Agreement shall apply to all activities associated with the Main Contract while employees of **PureLink GmbH** or third parties commissioned by **PureLink** will process personal data on behalf of the Customer. This Agreement, in conjunction with the Main Contract, contains the documented instructions for the processing of personal data, subject matter, duration, specification of the content of the order, the nature and purpose of the processing, as well as the rights and obligations of the parties in relation to the processing of personal data.

1. SUBJECT MATTER AND DURATION OF THE COMMISSONED DATA PROCESSING

1.1 Subject Matter

The order of the client to the contractor shall include the administration of customer data for the purpose of sales and delivery related to the products offered by the Contractor on its websites and specified in the respective service descriptions.

1.2 Duration

The term of this Agreement shall correspond to the term of the Main Contract. If services are also provided after its termination, the provisions of this Agreement shall also apply to this further provision of services for the entire duration of the actual cooperation.

2. SPECIFICATION OF THE ORDER OR CONTRACT DETAILS

2.1 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 are specified in the Main Contract closed .

The provision of the contractually agreed data processing will solely take place in a member state of the European Union, or in another state party to the Agreement on the European Economic Area. Any transfer to a third country will be coordinated with the client beforehand and will only take place if the special requirements of Art. 44 et seq are fulfilled. The special conditions shall be checked by the contractor.

2.2 Type of Data

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

○ **Personal Master Data** *(Key Personal Data)*

○ **Communication Data** *(e.g. Phone, E-Mail)*

○ **Key Contract Data**
(Contractual/Legal Relationships, Contractual or Product Interest)

○ **Contract Billing and Payment Data**

○ **Planning and Control Data**

○ **Disclosed Information**
(from third parties, e.g. Credit Reference Agencies or from Public Directories)

○ **Bank Details**

○ **Order Data**

○ **Address Data**

○ **OTHER:**

2.3 Categories of Data Subjects

The Categories of Data Subjects are:

○ Customers

○ Potential Customers

○ Subscribers

○ Employees

○ Suppliers

○ Sales Agents

○ Contact Persons

○ OTHER:

3. TECHNICAL AND ORGANIZATIONAL MEASURES

3.1 Before the commencement of processing, the Contractor shall document the execution of the necessary Technical and Organisational Measures, set out prior to the closing of the Agreement,, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Client for inspection. Upon acceptance by the Client, the documented measures shall become the contract basis. Insofar as the inspection/audit by the Client results in necessary amendments, such amendments shall be implemented by mutual agreement.

3.2 The Contractor 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 Annex 1]*.

3.3 The technical and organizational measures are subject to technical progress and further development. In that regard, the contractor is permitted to implement alternative adequate measures. In doing so, the safety level of the specified measures must not be deceeded. Significant changes have to be documented.

4. RECTIFICATION, RESTRICTION AND ERASURE OF DATA

4.1 The Contractor may not rectify, erase or restrict the processing of data processed on behalf of the Client on its own authority but only according to the client‘s documented instructions. 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.

4.2 Insofar as included in the scope of services, the erasure policy, ‘right to be forgotten’, rectification, data portability and access shall be ensured by the Contractor according to the Client’s documented instructions.

5. QUALITY ASSURANCE AND OTHER OBLIGATIONS OF THE CONTRACTOR

The Contractor shall process personal data exclusively in line with the Agreements made. Purpose, type and scope of data processing shall be made in strict accordance with the instructions of the Client. In compliance with Articles 28 to 33 GDPR, the Contractor ensures adherence to the following provisions:

5.1 The Contractor confirms to having appointed a Data Protection Officer within the meaning of Art. 37 para. 1 GDPR and will inform the Client in writing, or text form, e.g. per email.

5.2 The Contractor confirms that he will only employ personnel he previously has committed to confidentiality and instructed in the relevant data protection regulations according to Art. Art. 28 para. 3 sentence 2 lit. b. 29, 32 para. 4 GDPR. The Contractor and any subordinated person with access to personal data may process such data only in accordance with and limited to the extent of the Client's instructions, unless they are legally obliged to process otherwise.

5.3 Upon request, the Client and the Contractor shall cooperate with the supervisory authority in the performance of their duties. This shall refer particularly to:

- Immediate information of the client about control actions and measures of the supervisory authority, insofar as they are related to the current order. Same shall apply insofar as a competent authority is investigating in an administrative or criminal procedure and refers to the processing of personal data.

- The Contractor shall use his best endeavours to assist the Client insofar as the Principal is liable to control of the supervisory authority for reasons of an administrative offense or criminal proceeding, claim of a data subject or a third party, or any other claim related to order processing by the Contractor.

5.4 The Contractor warrants to the Client the verifiability of the technical and organizational measures taken within the scope of his control powers pursuant to Section 7 of this contract.

5.5 The implementation and compliance with all technical and organizational measures required for this contract pursuant to Art. 28 para. 3 sentence 2 lit. c, 32 DSGVO *[Details in Appendix 1]*.

6. SUBCONTRACTING

6.1 Subcontractual relationships within the meaning of this regulation are to be understood as such services which relate directly to the performance of the main service. This does not include ancillary services provided by the Contractor, e.g. telecommunications, postal / transport services, maintenance and user service, or the disposal of data carriers and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment claims. However, the Contractor shall be obliged to provide appropriate and legally compliant contractual agreements and control measures in order to ensure data protection and data security of the Client's data, even with outsourced ancillary services.

6.2 The contractor may commission subcontractors (other processors) to process personal data on behalf of the Customer. PureLink must ensure by way of contract or other legal instrument under EU law that all subcontractors processing personal data on behalf of customers resident in the European Economic Area, have at least equivalent data protection obligations, such as stipulated in this Agreement; in particular providing sufficient guarantees for the implementation of appropriate technical and organizational measures.

The following subcontractors may be engaged by the Contractor in processing of personal data:

Subcontractor	Address / Country	Service
basecom GmbH & Co. KG	Hannoversche Str. 6-8 DE-49084 Osnabrück	Operation, maintenance website, contact forms, online shop
microtech GmbH	Arthur-Rauner-Str. 5 DE-55595 Hargesheim	Provider of „ERP complete" internal IT system
Clever Reach GmbH & Co. KG	Mühlenstraße 43 DE-26180 Rastede	Provider software for E-Mail delivery, evaluation

Before commissioning a new or changing a subcontractor, PureLink GmbH shall be obliged to inform Customers at least twenty (20) calendar days in advance. The customer shall be entitled to object to the assignment or employment of a new subcontractor in the processing of personal data on his behalf within a period of ten (10) working days.

His objection shall be sent to tsihlis@purelink.de, giving the full name (and other identifying details) of the client, as well as referring to the relevant main contract and reasons for entering the objection. All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

If the customer exercises his right of objection, PureLink GmbH has the right in its sole discretion:

a) to refrain from using the complained subcontractor for processing of personal data on behalf of the customer and to confirm the Customer in writing;

b) to contact the Customer for seeking a mutual agreement, e.g. by removing the reason for the contradiction. If an agreement is reached between the parties, the customer shall withdraw the objection;

c) to cancel the Main Contract as a whole, or partially for processing on behalf of the customer for which the objected new subcontractor was intended to be commissioned.

d) For every transfer of personal data to a country outside the EU, the requirements of Art. 44 GDPR must be met.

6.3 If the subcontractor provides the agreed service outside the EU / EEA, the contractor shall ensure that the data protection law is admissible by taking appropriate measures. The same shall apply if service providers within the meaning of para. 1 sentence 2 are to be used.

7. SUPERVISORY POWERS OF THE CLIENT

7.1 After consultation with the Contractor, the Client has the righ, 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 means of random checks, which are to be announced in good time.

7.2 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.

7.3 The Supplier may claim remuneration for enabling Client inspections.

8. COMMUNICATION IN THE CASE OF INFRINGEMENTS BY THE SUPPLIER

8.1 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 detecti on 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

8.2 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

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

9.2 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

10.1 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.

10.2 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.

10.3 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. CONFIDENTIALITY OBLIGATIONS

11.1 Both parties undertake to treat as confidential all information obtained in connection with the execution of this contract and to use it only for the execution of the contract. No party is entitled to use this information in whole or in part for purposes other than those just mentioned or to make this information available to third parties.

11.2 The above obligation shall not apply to information which one of the parties has verifiably received from third parties, without being obliged to maintain secrecy, or which are publicly known.

12. FINAL PROVISIONS

12.1 Should the Client's property be endangered by third party measures (such as seizure or seizure), insolvency proceedings or other events, the Contractor shall inform the Client immediately. The contractor will inform the creditors immediately about the fact that they are data processed on behalf of the contractor.

12.2 Ancillary agreements must be in writing.

12.3 The objection of the right of retention is excluded with regard to the processing data and the associated data carriers.

Should individual parts of this contract be ineffective, this does not affect the validity of the remaining provisions of the contract.

Given at

Rheine,

Client

Contractor **PureLink GmbH**

APPENDIX - TECHNICAL AND ORGANISATIONAL MEASURES

1. 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.

2. 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

3. 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);

4. 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.