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

Agreement between

User

GBTEC Academy

- hereinafter referred to as the Client –

and

Supplier

GBTEC Group

- hereinafter referred to as the Supplier -

1. Subject matter and duration of the Order or Contract

1.1 Subject matter

The Subject matter of the Contract regarding the processing of data is the execution of the following services or tasks by the Supplier: GBTEC Academy is a learning hub for BPM and digitalization by GBTEC Group, which offers free and fee-based e-learning courses. The users are provided with in-person training in our state-of-the-art training center, virtual live training with participants from around the world, webinars & events, digitization or product consulting, wide offering of whitepapers and a podcast.

1.2 Duration

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

2. Specification of the Order or Contract Details

2.1. 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 terms of service and the data privacy on the GBTEC Academy website.

The undertaking of the contractually agreed Processing of Data shall be carried out exclusively with-in 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. The adequate level of protection has been decided by the European Commission (Article 45 Paragraph 3 GDPR);

is the result of binding corporate rules (Article 46 Paragraph 2 Point b in conjunction with Article 47 GDPR);

is the result of Standard Data Protection Clauses (Article 46 Paragraph 2 Points c and d GDPR);

is the result of approved Codes of Conduct (Article 46 Paragraph 2 Point e in conjunction with Article 40 GDPR);

is the result of an approved Certification Mechanism. (Article 46 Paragraph 2 Point f in conjunction with Article 42 GDPR).

is established by Article 46 Paragraph 2 Point a, Paragraph 3 Points a and b GDPR.

2.2. Type of Data

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

- ☒ Personal Data (Name, E-Mail-address)
- ☐ Key Contract Data (Contractual/Legal Relationships, Contractual or Product Interest)
- ☒ Learning process
- ☐ Contract Billing and Payments Data
- ☐ Disclosed Information (from third parties, e.g. Credit Reference Agencies or from Public Di-rectories

Categories of Data Subjects

☒ The Categories of Data Subjects comprise:

☒ Customers

☒ Potential Customers

☒ Subscribers

☒ Partner

☐ Suppliers

☐ Authorised Agents

☐ Contact Persons

3. Technical and Organizational Measures

3.1 Before the commencement of processing, the Supplier shall document the execution of the necessary Technical and Organizational Measures, set out in advance of the awarding of the Order or Contract, 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 become the foundation of the contract. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

3.2 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]

3.3 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

4.1 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.

4.2 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.

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:

The Supplier has appointed Mr. Andreas Reinke, arbeitgeber ruhr GmbH, Königsallee 67, 44789 Bo-chum, 0234-58877-27, reinke@datenschutzbeauftragter.ruhr as Data Protection Officer. The Client shall be informed immediately of any change of Data Protection Officer.

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.

a) 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].

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

c) 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.

d) 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.

e) 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.

f) 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

6.1 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 da-ta

protection and the data security of the Client's data, even in the case of outsourced ancillary services.

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

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: See attached Subcontractors.

b) NOTWITHSTANDING THE PRINCIPLE ACCORDING TO 6 PARA. 2, P. 1, OUTSOURCING TO SUBCONTRACTORS OR CHANGING TO ANOTHER SUBCONTRACTOR IS ALSO PERMITTED WITH-OUT THE AFOREMENTIONED CONSENT IN THE FOLLOWING CASES:

• Case 1: the subcontractor is a company affiliated with the contractor (within the meaning of Section 15 German Stock Corporation Act) in a member state of the European Union or in another state party to the Agreement on the European Economic Area and the outsourcing is based on a contractual agreement in accordance with Art. 28 paras. 2 – 4 GDPR.

• Case 2: The following conditions are fulfilled:

o the contractor notifies the customer of such outsourcing / transfer to subcontractors a rea-sonable time in advance in writing or in text form, and

o the client does not object to the planned outsourcing in writing or in text form to the contractor by the time the data is handed over, and

o the outsourcing is based on a contractual agreement in accordance with Art. 28 paras. 2 - 4 GDPR.

6.3 The transfer of personal data from the Client to the subcontractor and the subcontractors who will commence data processing shall only be undertaken after compliance with all requirements has been achieved.

6.4 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.

6.5 Further outsourcing by the subcontractor requires the express consent of the main Client (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

7.1 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.

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 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).

7.4 The Supplier may claim compensation for enabling Client inspections. Compensation may be claimed for a maximum of one supplier employee at a daily rate of 600,00 EUR (for 8 hours). When the Client inspects on-premises, the mere presence of the supplier's employee during such inspection shall be considered such compensable expense. Non-compensable, on the other hand, are expenses that have been caused by a proven non-compliant behavior of the supplier (with respect to this agreement).

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 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

8.2 The Supplier may claim compensation for support services which are not included in the de-scription of the services, and which are not attributable to failures on the part of the Supplier. Sec. 7.4 applies accordingly.

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. Contract amendment

THE SUPPLIER IS ENTITLED TO CHANGE THE CONTENT OF THE CONTRACT RELATING TO THE TECH-NICAL AND ORGANISATIONAL MEASURES WITH THE CONSENT OF THE CLIENT, PROVIDED THAT THE CHANGE IS REASONABLE TAKING INTO ACCOUNT THE INTERESTS OF THE CLIENT. THE CONSENT TO THE AMENDMENT OF THE CONTRACT SHALL BE DEEMED TO HAVE BEEN GIVEN, UNLESS THE CLIENT OBJECTS TO THE AMENDMENT WITHIN FOUR WEEKS OF RECEIPT OF THE NOTIFICATION OF AMENDMENT.

Appendix - Technical and Organizational Measures

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

- Admission Control
- Servers are in locked server rooms.
- Keys are accessible only to IT support.
- Access to the building only possible by electronic key or reception. Outside office hours, the building is secured by a security service with regular patrols.
- For mobile work equipment, there are instructions to keep it in areas protected from access unless it is personally supervised electronic Access Control
- Entry Control
- Access to all IT systems is only possible with password and encrypted access.
- Password guidelines on complexity and frequency of change apply to password
- Handling of access data is regulated by work instructions.
- Access Control
- Access control takes place via the authorization system on server applications and network drives.

- Authorization is granted by the respective supervisor, while IT support is responsible for granting authorization.
- Pseudonymization (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)
- Mathematical methods (e.g. hashing)
- Further description / Further measures: For pseudonymization, GBTEC provides tools on request for customers to pseudonymize their data before handing it over to GBTEC).

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

- Data Transfer Control
- Data is always transferred via encrypted connections. A special system (https://support.bicplatform.com) is provided for this purpose.
- Data Entry Control
- Restriction of the work with all data of a client to the assigned employees is carried out by authorization system and obligation of the employees in work instruction.

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

- Availability Control
- Backup and recovery concept with disaster-proof storage.

- Failover protection through redundant hard disk systems and uninterruptible power supply.
- Use of appropriate protection software: virus scanners, firewalls, spam filters, data encryption).

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

- Data Protection Management
- Quality Management implemented
- Regular audits established
- The company data protection officer for GBTEC is Andreas Reinke (reinke@datenschutzbeauftragter.ruhr, 0234-5887727, arbeitgeber ruhr GmbH, Königsallee 67, 44789 Bochum, Germany).
- There is an Incident Response Management
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR)
- Only the minimum data necessary for the operation of the software is collected: Name, email, role and usual logging information.
- Order or Contract Control
- Data is only be processed by BIC Support: Email: bicsupport@gbtec.com, Phone: +4923497645-200