Data Processing Agreement based on article 28 GDPR

This Agreement shall regulate the processing of personal data on behalf of _____) (“CONTROLLER”)

by the processor acc. to art. 28 GDPR

GBTEC Software AG registered under the laws of Germany and having its registered office at Gesundheitscampus-Süd 23, 44801 Bochum and its entities that might be brought in as subcontractors (“GBTEC” or “PROCESSOR”).

1. Summary and duration of the processing

1.1 Subject matter: On [date], the parties concluded a [Name of the agreement (e.g., (Master) Services Agreement, Purchase Order, etc.)] for the provision of [high-level description of services to CONTROLLER] by GBTEC to CONTROLLER ("Services Agreement", and together with this DPA, “Agreement”).

1.2 Purpose: CONTROLLER requires GBTEC (PROCESSOR) to process personal data as described in Annex 1. This DPA shall apply to all processing activities made in relation to the Services Agreement.

1.3 Duration:

The duration of this DPA corresponds to the term of the Service Agreement.

2. Scope and specifications of the processing

2.1 Nature and purpose of the intended data processing

Detailed description of the subject matter of the contract regarding the nature and purpose of the PROCESSOR's tasks: Operation of software

The provision of the contractually agreed data processing shall take place exclusively in a member state of the European Union or in another state party to the Agreement in the European Economic Area. Any relocation to a third country requires the prior consent of the

CONTROLLER and may only take place if the special requirements of Art. 44 et seq. GDPR are fulfilled [see 9. Subcontractors].

2.2 Data categories

The subject of the processing of personal data are the data types/categories listed in Annex 1.

2.3 Categories of data subjects

The categories of data subjects affected by the processing are listed in Annex 1:

2.4 GBTEC shall document the implementation of the technical and organizational measures set out and required prior to the start of processing, in particular regarding the specific execution of the Agreement and submit them to the CONTROLLER for review. If accepted by the CONTROLLER, the documented technical and organizational measures become an integral part of the DPA. If the inspection/audit by the CONTROLLER reveals a need for adjustment, this must be implemented by mutual agreement.

2.5 GBTEC must establish security in accordance with Art. 28 para. 3 lit. c, 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are information security measures and measures that ensure a level of data protection appropriate to the risk in terms of confidentiality, integrity, availability and resilience. In this respect, the state of the art, the costs of implementation 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 Art. 32 (1) GDPR are considered (see Annex 3).

3. Quality assurance, privacy compliance and other obligations of the PROCESSOR

3.1 GBTEC shall take appropriate technical and organizational measures to ensure confidentiality and protection against accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure, access or any other unlawful form of processing, including a personal data breach. At the very least, GBTEC will maintain the security measures described in Annex 2 to protect personal data.

3.2 In taking these security measures, GBTEC has considered the state of the art, the implementation costs of the security measures, the nature, scope and context of the processing, the purposes and the intended use of its Services, the processing risks and the risks

for the rights and freedoms of data subjects that it may expect in view of the intended use of the Services.

3.3 In addition to the compliance with the provisions of this DPA, the CONTROLLER has statutory obligations pursuant to Art. 28 to 33 GDPR; in this respect, the CONTROLLER shall, in particular, ensure compliance with the following requirements:

3.3.1 Written designation of a data protection officer who performs his/her duties in accordance with Art. 38 and 39 GDPR. The contact details of the data protection officer and other contact person(s) for privacy issues must be communicated to the CONTROLLER [Annex 1]; any change must be reported to the CONTROLLER immediately.

3.3.2 If the CONTROLLER has its registered office outside the European Union, it shall designate the following representative in the European Union pursuant to Art. 27 (1) GDPR [Annex 1]

3.3.3 The maintenance of confidentiality pursuant to Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. When carrying out the processing, GBTEC shall only employ employees who have been obliged to maintain confidentiality and who have previously been familiarized with the data protection provisions relevant to them. GBTEC and any person subordinate who has access to personal data may only process this data in accordance with the instructions of the CONTROLLER, including the authorizations granted in this contract, unless they are legally obliged to process it.

3.3.4 The implementation of and compliance with all technical and organizational measures required for processing in accordance with Art. 28 para. 3 sentence 2 lit. c, 32 GDPR; (Annex 3).

3.3.5 If the CONTROLLER carries out a data protection impact assessment (DPIA) on the contractual processing of personal data, GBTEC shall provide the CONTROLLER with suitable information - in particular on the technical and organizational measures.

3.3.6 Upon request, CONTROLLER and GBTEC shall cooperate with the supervisory authority in the accomplishment of their duties.

3.3.7 Immediate information of the CONTROLLER about inquiries and measures of the supervisory authority, insofar as they relate to this DPA. This shall also apply if a competent

authority investigates the processing of personal data or conducts prosecution at the CONTROLLER's premises.

3.3.8 To the extent CONTROLLER is subject to an inspection by the supervisory authority, administrative or criminal proceedings, a liability claim by a data subject or a third party or any other claim in connection with the processing on behalf of the CONTROLLER, GBTEC shall support the CONTROLLER to the best of its ability.

3.3.9 GBTEC shall regularly monitor the internal processes and the technical and organizational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.

3.3.10 GBTEC ensures that the technical and organizational measures acc. Annex 3 are implemented.

4. Personal data breaches

GBTEC shall:

4.1 Notify CONTROLLER without undue delay after becoming aware that a personal data breach has occurred.

4.2 without undue delay, take necessary and, considering the risks associated with the breach of personal data protection, appropriate measures to prevent or at least mitigate possible damage to data subjects.

4.3 Provide sufficient information to allow CONTROLLER to meet any obligations to notify or inform supervisory authorities and/or data subjects of the personal data breach in accordance with applicable laws.

4.4 The information to be provided shall as a minimum:

4.4.1 Contain a detailed description of the nature of the personal data breach, categories and approximate number of personal data records and data subjects are or might be concerned.

4.4.2 Contain the name and contact details of the GBTEC´s data protection officer or another relevant contact from whom more information may be obtained.

4.4.3 Describe the likely consequences of the personal data breach, and measures to address the personal data breach.

5. Confidentiality and disclosure requests

GBTEC shall:

5.1 Ensure that persons authorized to process the personal data are required to maintain the confidentiality and security of the personal data.

5.2 Process personal data only on a “need–to-know” basis to the extent required to perform the Services.

5.3 To the extent permitted by applicable law, immediately notify CONTROLLER, if it is compelled by applicable law to supply personal data or information about the processing to a competent public authority.

6. Audits

6.1 GBTEC shall:

6.1.1 Allow CONTROLLER to audit its compliance with this DPA in line with the procedure set out in the Services Agreement.

6.1.2 Allow for audits by CONTROLLER, its representatives and independent auditors appointed by CONTROLLER that will be bound to confidentiality and provide them with reasonable access to GBTEC´s and its Subcontractor’s premises (if applicable).

6.1.3 Audit its own compliance with the DPA. Such audit shall:

i. cover all processing of personal data under the Agreement.

ii. be performed by an independent auditor which GBTEC shall provide to CONTROLLER.

6.2 Remediation

GBTEC shall take all immediate action to ensure that any weaknesses and issues identified by the audit report are adequately addressed.

6.3 Costs. The costs of the audit shall be at CONTROLLER´s expense if CONTROLLER conducts the audit unless the audit concludes that GBTEC is in breach of its obligations under the Agreement.

6.4 If public authorities request information regarding the Subject, GBTEC shall:

6.4.1 Submit its processing systems, facilities, records and supporting documentation to an inspection by a competent public authority if this is necessary to comply with a legal obligation.

6.4.2 Take immediate action to ensure future compliance with the law if the competent public authority deems the processing unlawful.

7. Cooperation

7.1 General cooperation. GBTEC will deal promptly and appropriately with requests from CONTROLLER relating to the processing of personal data under the Agreement and provide reasonable assistance and support. This includes, without limitation, providing information, assistance, and support to enable CONTROLLER to assess and ensure an adequate level of data security, complete and maintain data protection impact assessments and records, comply with personal data breach notification requirements, provide necessary notices, and consent to individuals, and comply with requests from individuals and supervisory authorities.

7.2 Requests from individuals. GBTEC will not adjust, delete or restrict the processing of the processed data without authorization, but only in accordance with documented instructions from the CONTROLLER. If a data subject contacts the PROCESSOR directly in this regard, the PROCESSOR shall a) forward this request to the CONTROLLER without delay, with the consent of the data subject, and b) will advise the data subject that they must address their request to the CONTROLLER.

8. Subcontractors

8.1 Subcontracting relationships within the meaning of this provision are to be understood as those services which relate directly to the provision of the main service. This does not include ancillary services that the processor uses, e.g. as telecommunications services, postal/transport services, maintenance and user service 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 systems. However, the processor is obliged to take appropriate and legally compliant contractual agreements and control measures to ensure the data protection and data security of the controller's data, even in the case of outsourced ancillary services.

8.2 As a matter of fact, the processor may only commission subcontractors (other processors) with the prior express written or documented consent of the controller.

a) The controller hereby grants this consent already for the commissioning of the subcontractors listed in the Annex (list of subcontractors), subject to a contractual agreement in accordance with Art. 28 para. 2-4 GDPR.

b) IN DEVIATION FROM THE PRINCIPLE PURSUANT TO PARA. 2, SENTENCE 1, OUTSOURCING TO SUBCONTRACTORS OR CHANGING THE EXISTING SUBCONTRACTOR IS ALSO PERMISSIBLE WITHOUT THE AFOREMENTIONED CONSENT IN THE FOLLOWING CASES:

- Case 1: the subcontractor is a company affiliated with the processor (within the meaning of Section 15 of the 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 (2) – (4) GDPR.
- Case 2: The following requirements are met: the processor shall notify the controller of such outsourcing/relocation to subcontractors a reasonable period of time in advance in writing or in text form, and the controller does not object to the planned outsourcing to the processor in writing or in text form until the time the data is handed over, and the outsourcing is based on a contractual agreement in accordance with Art. 28 (2) – (4) GDPR.

8.3 The disclosure of personal data of the controller to the subcontractor and the subcontractor's initial activity are only permitted if all the prerequisites for subcontracting have been met.

8.4 If the subcontractor provides the agreed service outside the EU/EEA, the processor ensures that it is permissible under data protection law by taking appropriate measures. The same applies if service providers within the meaning of subsection 1 sentence 2 are to be used.

8.5 Further outsourcing by the subcontractor requires the express consent of the main controller in text form; all contractual provisions in the contract chain shall also be imposed on the other subcontractor.

9. Cross-border transfers

9.1 Where legal transfer restrictions apply, GBTEC shall:

9.1.1 Not transfer (including by providing remote access) any personal data without having been explicitly informed beforehand and having been granted a right of objection to CONTROLLER.

9.1.2 Ensure that a recognized transfer mechanism is in place to enable such transfer between the appropriate parties involved.

9.1.3 Provide CONTROLLER with a copy of such transfer mechanism upon CONTROLLER's request.

9.2 If the Services involve the transfer of personal data from a CONTROLLER legal entity in the EU to a GBTEC entity or subcontractor in a non-Adequate Country, which includes making such CONTROLLER personal data accessible from any such non-Adequate Country, GBTEC shall:

9.2.1 To the extent necessary, ensure that it, and any subcontractor shall enter into an EU Controller-to-Processors Standard Contractual Clauses agreement in a valid version and based on the correct applicable modules.

9.2.2 Warrant that it, and any subcontractors have implemented recognized and approved binding corporate rules for processors covering the personal data and will notify CONTROLLER should the authorization be modified, suspended, or lost at any point in time during the Agreement.

10. Return and deletion of personal data

10.1 Services Provider will delete or return all CONTROLLER personal data to CONTROLLER after the end of the provision of the Services relating to the processing and will delete all existing copies

unless applicable data protection law requires storage of the CONTROLLER personal data. GBTEC shall not retain personal data any longer than necessary for the purposes of performing its obligations under the Agreement.

10.2 PROCESSOR will confirm in writing that it has returned or deleted all copies of CONTROLLER personal data. In principle, the deletion or return set out in this Section 11 will be at no additional cost for CONTROLLER.

11. Liability and indemnity

GBTEC shall be liable and agrees to indemnify, keep indemnified, hold harmless and, upon CONTROLLER's request, defend CONTROLLER and its directors, employees, shareholders and agents from and against any and all damages, liabilities, expenses, claims, fines and losses of any type, including without limiting reasonable attorneys' fees, in connection with, arising out of or relating to, in whole or in part GBTEC's failure to comply with privacy and data protection obligations under this Agreement, including in case of a personal data breach.

12. Requirement of written form

Changes, additions, and subsidiary agreements to this framework agreement as well as their termination must be made in written form. This also applies to the abolition of the written form requirement.

13. Contract amendment

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

---------- Signature page follows ----------

SIGNATURES

Signed by duly authorized representatives of CONTROLLER

Signature: _____

Name: _____

Position: _____

Date: _____

Signature: _____

Name: _____

Position: _____

Date: _____

Signed by a duly authorized representative of GBTEC

Signature: _____

Name: Nicole Lüdecke-Gleitze

Position: Rechtsanwältin (SyndikusRA'in)
General Counsel/ Head of
Corporate Legal & Compliance
GBTEC Group

Date: _____

Desciption of the Processing

1.1 Types of data

☒ Person master data (first and last names)

☒ Communications data (e.g., phone, e-mail)

1.2 Categories of data subjects

☒ Customers

☒ Interested parties

☒ Users

☒ Employees

☐ Suppliers

1.3 Data protection officer / contact person

Name:	Andreas Reinke
Title:	external data protection officer
Address:	Arbeitgeber Ruhr GmbH (Bochum), Königsallee 67, 44789 Bochum, Germany
Phone number:	0234-58877-27
E-Mail-address:	reinke@datenschutzbeauftragter.ruhr

Name:	Volker Breitkopf
Position:	internal coordinator
Addresse:	GBTEC Software AG, Gesundheitscampus-Süd 23, 44801 Bochum, Germany
Phone number:	0234-97645-209
E-Mail-address:	datenschutz@gbtec.com

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.de) is provided for this purpose.
- Data Entry Control
  - Restriction of the work with all data of a CONTROLLER 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.de, Phone: +4923497645-200

List of subcontractors of GBTEC AG

GBTEC AG with its registered office in 44801 Bochum, Gesundheitscampus-Süd 23 offers customers services and uses subcontractors for this purpose.

The subcontractors provide the following services within the scope of the offered performance:

1. Data Centres

1. **Services**

- Provision of computing power (computer resources) as virtual machines for the software required to provide the services
- Provision of storage resources as block-, object- and database storage for keeping and protection information which processed by the services
- Provision of internet connectivity and data transfer incl. Network access protection and encryption (network resources) for the use of services by users, technical support of the services by GBTEC and for data transfer between computer and storage resources
- Compliance with DIN EN ISO 27 001 for all services used

2. **Provider**

For all services offered under the internet domain „gbtec.de“ and sub-domains:

- Amazon Web Services EMEA SARL, 5 Rue Plaetis, L-2338 Luxemburg

For all services offered under the internet domain „gbtec.com“ and sub-domains:

- Amazon Web Services EMEA SARL, 5 Rue Plaetis, L-2338 Luxemburg

For all services offered under the internet domain „bicplatform.com“ and sub-domains:

- Amazon Web Services EMEA SARL, 5 Rue Plaetis, L-2338 Luxemburg

For all services offered under the internet domain „bicplatform.de“ and sub-domains:

- Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn

For all services offered under the internet domain „bicplatform.net“ and sub-domains:

- Microsoft Ireland Operations Limited, 70 Sir Rogersons’s Quay, Dublin, Ireland

For all services offered under the internet domain „bicplatform.com.au“ and sub-domains:

- Amazon Web Services EMEA SARL, 5 Rue Plaetis, L-2338 Luxemburg

For all services offered under the internet domain „biccloud.com“ and sub-domains:

- Amazon Web Services EMEA SARL, 5 Rue Plaetis, L-2338 Luxemburg

For all services offered under the internet domain „biccloud.de“ and sub-domains:

- Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn

For all services offered under the internet domain „biccloud.com.au“ and sub-domains:

- Amazon Web Services EMEA SARL, 5 Rue Plaetis, L-2338 Luxemburg

For services offered under other internet domains GBTEC uses one or more of the subcontractors unless GBTEC and the customer has agreed an individual case.

3. **Data protection and information security**

To ensure compliance with the requirements on information security and data protection, GBTEC employs only certified subcontractors and in individual cases concludes additional contractual provisions for compliance with legal data protection which are listed below:

- Amazon Web Services EMEA SARL, 5 Rue Plaetis, L-2338 Luxemburg: certified according to DIN EN ISO 27001 by Ernst & Young CertifyPoint B.V., Antonio Vivaldistraat 150, 1083 HP Amsterdam, The Netherlands see also: https://aws.amazon.com/de/compliance/iso-27001-faqs,

https://aws.amazon.com/de/compliance. GBTEC has also concluded an agreement with Amazon Web Services EMEA SARL for data processing.

- Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn: see also: https://cloud.telekom.de
  certified according to DIN EN ISO 27001 by DEKRA Certification GmbH, Handwerkstrasse 15, 70565 Stuttgart, see also: https://cloud.telekom.de/de/infrastruktur/open-telekom-cloud/mehr/compliance. GBTEC has also concluded an agreement with Telekom Deutschland for data processing

- Microsoft Ireland Operations Limited, 70 Sir Rogersons's Quay, Dublin, Ireland: certified according to DIN EN ISO 27001 by TÜV Nord Cert GmbH & Co.KG, Genovevastraße 5, 51065 Köln see also: https://news.microsoft.com/de-de/microsoft-azure-deutschland-iso-zertifizierungen, https://www.microsoft.com/de-de/cloud/compliance). GBTEC has also concluded an agreement with Microsoft Ireland Operations Limited for data processing.

4. **Service by affiliated companies**

4.1 Services

- Assistance of product support by providing development services for technical fault analysis in product code and identification of workarounds
- Provision of troubleshooting in the form of service release of product components for troubleshooting

4.2 Provider

- GBTEC Software S.L., Edificio CITEXVI, Fonte de Abelleiras s/n – local 27, 36310 Vigo (Pontevedra), Spain
- GBTEC Austria GmbH, Franz-Klein-Gasse 5, 1190 Wien, Austria

4.3 Data protection and information security

- individual agreement within the GBTEC Group

5. Service for the product BIC Process Mining

The following subcontractors are used exclusively for the services described here for the product BIC Process Mining.

5.1 Services

- Assistance of product support by providing development services for technical fault analysis in product code and identification of workarounds
- Provision of troubleshooting in the form of service release of product components for troubleshooting

5.2 Provider

- Arvato Systems S4M GmbH, Am Coloneum 3, 50829 Köln
- Apromore Pty Ltd, Level 10, Building 168, The University of Melbourne Victoria 3010, Australia

  Apromore Holding Pty Ltd, Level 10, Building 168, The University of Melbourne Victoria 3010, Australia

6. Data protection and information security

GBTEC will always first try to provide the service without passing on personal data. If the transfer of data for the provision of services is unavoidable GBTEC will anonymize personal data and will only pass it on to these subcontractors with the consent of the client.