
Data Processing Agreement according to article 28 GDPR

1. Parties

This Data Processing Agreement (“**DPA**”), dated [date] (“**Effective Date**”) is made between:

- (1) [DATA CONTROLLER] registered under the laws of [country] and having its registered office at [address], acting on its own behalf and on behalf of its affiliates (“**DATA CONTROLLER**”); and
- (2) GBTEC Software AG registered under the laws of Germany and having its registered office at Gesundheitscampus-Süd 23, 44801 Bochum acting on its own behalf and on behalf of its affiliates (“**GBTEC**”).

2. Summary of the Processing

2.1 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 DATA CONTROLLER] by GBTEC to DATA CONTROLLER (“Services Agreement”, and together with this DPA, “Agreement”).

2.2 Purpose: DATA CONTROLLER (Data Controller) requires GBTEC (Data 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.

3. Compliance with DATA CONTROLLER Instructions and the Law

GBTEC will:

Process Personal Data in accordance with the instructions of DATA CONTROLLER and as set out in this DPA. Comply with all privacy and data protection laws applicable to GBTEC when Processing the Personal Data. If applicable laws require GBTEC to process Personal Data other than as instructed by DATA CONTROLLER,

GBTEC will immediately inform DATA CONTROLLER of such legal requirement before such processing.

4. Compliance with DATA CONTROLLER Instructions and the Law

4.1 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.

4.2 In taking these security measures, GBTEC has taken into account 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.

5. Personal Data Breaches

5.1 GBTEC shall:

- a.** Notify DATA CONTROLLER without undue delay after becoming aware that a Personal Data Breach has occurred;
- b.** Provide sufficient information to allow DATA 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.

5.2 The information to be provided shall as a minimum:

- a.** Contain a detailed description of the nature of the Personal Data Breach, categories and approximate number of Personal Data records and Data Subjects concerned;
- b.** Contain the name and contact details of the GBTEC's data protection officer or another relevant contact from whom more information may be obtained;
- c.** Describe the likely consequences of the Personal Data Breach, and measures to address the Personal Data Breach.

5.3 GBTEC shall document such Personal Data Breach, including facts relating to such breach and remedial action taken.

6. Confidentiality and Disclosure Requests

GBTEC shall:

- a.** Ensure that persons authorised to process the Personal Data are required to maintain the confidentiality and security of the Personal Data;
- b.** Process Personal Data only on a “need-to-know” basis to the extent required to perform the Services.
- c.** To the extent permitted by applicable law, immediately notify DATA CONTROLLER, if it is compelled by applicable law to supply Personal Data or information about the Processing to a competent public authority.

7. Audits

7.1 GBTEC shall:

- a.** Allow DATA CONTROLLER to audit its compliance with the Agreement in line with the procedure set out in the Services Agreement;
- b.** Allow for audits by DATA CONTROLLER, its representatives and independent auditors appointed by DATA CONTROLLER that will be bound to confidentiality, and provide them with reasonable access to GBTEC’s and it’s Subcontractor’s premises (if applicable).
- c.** 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 DATA CONTROLLER.

7.2 Remediation

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

7.3 Costs

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

7.4 Public authorities' requests Subject, GBTEC shall:

- a. 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.
- b. Take immediate action to ensure future compliance with the law, if the competent public authority deems the Processing unlawful.

8. Cooperation

8.1 General cooperation:

GBTEC will deal promptly and appropriately with requests from DATA 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 DATA 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.

8.2 Requests from individuals:

GBTEC will immediately notify DATA CONTROLLER if it receives a request from an individual with respect to their Personal Data in connection with this Agreement, including DATA CONTROLLER's staff, and will not respond to such request unless expressly authorized to do so in writing by DATA CONTROLLER. This requirement does not apply to standard requests made by users in the normal course of using the Services, via default/basic functionalities of the Services, to access, re-initialize or edit basic Personal Data, such as their user name, profile information or password.]

9. Subcontractors

GBTEC shall not permit any Subcontractor to process Personal Data without: (a) DATA CONTROLLER's prior written approval, such approval having already been provided in respect of those Subcontractors listed in Annex 3; and (b) entering into a contract which binds the Subcontractor to substantially similar obligations with respect to the processing of DATA CONTROLLER's Personal Data as to which GBTEC is bound by this DPA. GBTEC remains fully liable to DATA CONTROLLER for the performance of its Subcontractors.

10. Cross-border Transfers

10.1 Where legal transfer restrictions apply, GBTEC shall:

- a.** 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 DATA CONTROLLER.
- b.** Ensure that a recognized transfer mechanism is in place to enable such transfer between the appropriate parties involved.
- c.** Provide DATA CONTROLLER with a copy of such transfer mechanism upon DATA CONTROLLER's request.

10.2 If the Services involve the transfer of Personal Data from a DATA CONTROLLER legal entity in the EU to a GBTEC entity or Subcontractor in a non-Adequate Country, which includes making such DATA CONTROLLER Personal Data accessible from any such non-Adequate Country, GBTEC shall:

- a.** To the extent necessary, GBTEC shall ensure that it, and any Subcontractor shall enter, into an EU Controller-to-Processors Standard Contractual Clauses in a valid version and with correct applicable modules.
- b.** Warrant that it, and any Subcontractors have implemented recognized and approved Binding Corporate Rules for Processors covering the Personal Data, and will notify DATA CONTROLLER should the authorization be modified, suspended or lost at any point in time during the Agreement.

11. Return and Deletion of Personal Data

11.1 Services Provider will delete or return all DATA CONTROLLER Personal Data to DATA 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 DATA CONTROLLER Personal Data. GBTEC shall not retain Personal Data any longer than necessary for the purposes of performing its obligations under the Agreement.

11.2 Services Provider will confirm in writing that it has returned or deleted all copies of DATA CONTROLLER Personal Data. In principle, the deletion or return set out in this Section 11 will be at no additional cost for DATA CONTROLLER.

12. Liability and Indemnity

GBTEC shall be liable and agrees to indemnify, keep indemnified, hold harmless and, upon DATA CONTROLLER's request, defend DATA 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.

13. 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.

14. Contract amendment

Data Processing Agreement (DPA-Agreement)

Version August 2nd, 2022



THE SUPPLIER IS ENTITLED TO CHANGE THE CONTENT OF THE CONTRACT RELATING TO THE TECHNICAL 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.

Data Processing Agreement (DPA-Agreement)

Version August 2nd, 2022



SIGNATURES

Signed by duly authorized representatives of **DATA CONTROLLER**

Signed by a duly authorized representative of **GBTEC**

Signature: _____
Name: _____
Position: _____
Date: _____

Signature: _____
Name: _____
Position: _____
Date: _____

Signature: _____
Name: _____
Position: _____
Date: _____

Signature: _____
Name: _____
Position: _____
Date: _____

Description of the Processing

1.1 Types of data

- Person master data
- Communications data (e.g., phone, e-mail)
- Contract master data (contractual relation, interest in products and contract)
- Customer / supplier history
- Data of contract billing and payment
- Report data
- Pictures
- Special categories of personal data (Art. 9 GDPR)
- Personal data on criminal convictions and offences (Art. 10 GDPR)
- ...

1.2 Categories of data subjects

- Customers
- Interested parties
- Subscribers
- Employees
- Employees of companies associated with the client
- Employees of companies in which the client holds shareholdings
- Suppliers
- Sales representatives
- Contact persons
- ...

1.3 Data protection officer / Contact person

Name: Andreas Reinke
Position: 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
Address: GBTEC Software AG, Gesundheitscampus-Süd 23, 44801 Bochum,
Germany
Phone number: 0234-97645-209
E-Mail-address: datenschutz@gbtec.com

Technical and Organisational 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.
- Pseudonymisation (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 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.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

1.1 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

1.2 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.

1.3 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 Luxembourg: 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.

2. Service by affiliated companies

2.1 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

2.3 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

2.4 Data protection and information security

- individual agreement within the GBTEC Group

3. Service for the product BIC Process Mining

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

3.1 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

3.2 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

3.3 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.