Vereinbarung über die Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen der

.....

- Verantwortlicher – nachstehend Auftraggeber genannt –

und dem/der

GBTEC Software AG

- Auftragsverarbeiter – nachstehend Auftragnehmer genannt

[Vertreter gemäß Art. 27 DSGVO *wenn erforderlich*:

.....]

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/ dem SLA auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung)

1.2 Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: .....

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau in dem betreffenden Drittland (.....) wird durch ..... garantiert, auf die hier verwiesen wird: .....

2.2 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind die in Anlage 1 aufgeführten Datenarten/-kategorien.

2.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen sind in Anlage 1 aufgeführt:

3. Technisch-organisatorische Maßnahmen

3.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.2 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den

zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen (Anlage 3).

3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

4.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. *Ist der Auftragnehmer nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet, so benennt er einen Ansprechpartner für datenschutzrechtliche Fragen*.
Die Kontaktdaten des Datenschutzbeauftragten oder des Ansprechpartners sind dem Auftraggeber mitzuteilen [Anlage 1], jedweder Wechsel ist dem Auftraggeber unverzüglich anzuzeigen.

b) Wenn der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DSGVO in der Union [Anlage 1]

c) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO; (Anlage 3).

e) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

f) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

g) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

h) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

6.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2 Der Auftragnehmer darf grundsätzlich Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) Der Auftraggeber erteilt diese Zustimmung hiermit bereits für die Beauftragung der in der Anlage aufgeführten Unterauftragnehmer (Liste Subunternehmer), unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO.

b) ABWEICHEND VON DEM GRUNDSATZ GEM. ABS. 2, S. 1 SIND DIE AUSLAGERUNG AUF UNTERAUFTRAGNEHMER ODER DER WECHSEL DES BESTEHENDEN UNTERAUFTRAGNEHMERS IN FOLGENDEN FÄLLEN AUCH OHNE DIE VORBENNANTE ZUSTIMMUNG ZULÄSSIG:

- Fall 1: bei dem Unterauftragnehmer handelt es sich um ein mit dem Auftragnehmer verbundenes Unternehmen (i.S.d. § 15 AktG) in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen

Wirtschaftsraum und der Auslagerung wird eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 – 4 DSGVO zugrunde gelegt.

- Fall 2: Folgende Voraussetzungen sind erfüllt:
  - der Auftragnehmer zeigt dem Auftraggeber eine solche Aus-/Umlagerung auf Unterauftragnehmer eine angemessene Zeit vorab schriftlich oder in Textform an, und
  - der Auftraggeber erhebt nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung, und
  - der Auslagerung wird eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 – 4 DSGVO zugrunde gelegt.

6.3 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.4 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

6.5 Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers in Textform; sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

7.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber die erforderlichen Auskünfte zu erteilen und

insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. ISO 27001 oder BSI-Grundschutz).

7.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer eine Aufwandsentschädigung für maximal einen Mitarbeiter des Auftragnehmers zu einem Tagessatz von 600,00 EUR (bezogen auf 8 Stunden) geltend machen. Im Falle einer vom Auftraggeber vor Ort durchgeführten Kontrolle gilt auch eine reine Begleitung durch einen Mitarbeiter des Auftragnehmers als ein solcher zu entschädigender Aufwand. Nichtentschädigungspflichtig sind hingegen solche Aufwände, die durch nachgewiesenes pflichtwidriges Verhalten des Auftragnehmers verursacht wurden (bezogen auf diesen Vertrag).

8. Mitteilung bei Verstößen des Auftragnehmers

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken

berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers bei der Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen. Ziff. 7 (4) gilt entsprechend.

9. Weisungsbefugnis des Auftraggebers

9.1 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (in Textform).

9.2 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger

Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

10.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Haftung

Der Auftragnehmer haftet bei Pflichtverletzungen aus dieser Vereinbarung oder gesetzlicher Datenschutzbestimmungen für vorsätzliches und grob fahrlässiges Verhalten nach den gesetzlichen Bestimmungen unbeschränkt.

12. Schriftformerfordernis

Änderungen, Ergänzungen und Nebenabreden zu dieser Rahmenvereinbarung sowie deren Kündigung bedürfen der Schriftform. Dies gilt ebenfalls für die Abschaffung des Schriftformerfordernisses.

13. Vertragsänderung

Der Auftragnehmer ist berechtigt, den Inhalt dieses Vertrages, sofern sich dieser auf Technisch Organisatorische Maßnahmen bezieht, mit Zustimmung des Auftraggebers zu ändern, soweit die Änderung unter Berücksichtigung der Interessen des Auftraggebers für den Auftraggeber zumutbar ist. Die Zustimmung zur Vertragsänderung gilt als erteilt, sofern der Auftraggeber der Änderung nicht innerhalb von vier Wochen nach Zugang der Änderungsmitteilung widerspricht.

Ort, Datum

Auftraggeber
Unterschrift, Name, Position

Auftraggeber
Unterschrift, Name, Position

Bochum, Datum

Nicole Lüdecke-Gleitze
Rechtsanwältin
(Syndikusrechtsanwältin)
Unterschrift, Name, Position

Auftragnehmer

Unterschrift, Name, Position

1.1 Datenarten

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kunden- und Lieferantenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ Bilder
- ☐ Besondere Kategorien personenbezogene Daten (Art. 9 DSGVO)
- ☐ personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO)
- ☐ …

1.2 Kategorien betroffener Personen

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Beschäftigte von Unternehmen, die mit dem Auftraggeber verbunden sind
- ☐ Beschäftige von Unternehmen, an denen der Auftraggeber Beteiligungen hält
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ …

1.3 Datenschutzbeauftragter / Ansprechpartner beim Auftragnehmer

Vor-/Name:	Andreas Reinke
Position / Funktion:	externer Datenschutzbeauftragter
Standort / Adresse:	arbeitgeber ruhr GmbH (Büro Bochum) Königsallee 67, 44789 Bochum
Telefonnummer:	0234-58877-27
E-Mail-Adresse:	reinke@datenschutzbeauftragter.ruhr

Vor-/Name:	Volker Breitkopf
Position / Funktion:	interner Koordinator
Standort / Adresse:	GBTEC Software AG, Gesundheitscampus-Süd 23, 44801 Bochum
Telefonnummer:	0234-97645-209
E-Mail-Adresse:	datenschutz@gbtec.com

Liste der Subunternehmer der GBTEC AG

Die GBTEC Software AG mit Sitz in 44801 Bochum, Gesundheitscampus-Süd 23 bietet Kunden Services an und setzt dafür Subunternehmer ein.

Von den Subunternehmern werden im Rahmen der angebotenen Services folgende Leistungen erbracht:

1. Rechenzentren

1.1 Leistungen

- Bereitstellung von Rechenleistung (Compute Resources) als virtuelle Maschinen für die erforderliche Software zur Erbringung der Services
- Bereitstellung von Speicherkapazitäten (Storage Resources) als Block-, Objekt- und Datenbank-Speicher für die Speicherung und Sicherung von Daten, die von den Services verarbeitet werden
- Bereitstellung von Internet-Konnektivität und Datentransfer inkl. Netzwerkzugangsschutz und Verschlüsselung (Network Resources) für die Nutzung der Services durch Anwender, technische Betreuung der Services durch GBTEC und für Datentransfer zwischen Compute und Storage Resources.
- Erfüllung der DIN EN ISO 27001 für alle in Anspruch genommen Leistungen

1.2 Anbieter

Für Services, die unter der Internet-Domain „gbtec.de“ und Sub-Domains angeboten werden:

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

Für Services, die unter der Internet-Domain „gbtec.com“ und Sub-Domains angeboten werden:

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

Für Services, die unter der Internet-Domain „bicplatform.com“ und Sub-Domains angeboten werden:

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

Für Services, die unter der Internet-Domain „bicplatform.de“ und Sub-Domains angeboten werden:

- Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn

Für Services, die unter der Internet-Domain „bicplatform.net“ und Sub-Domains angeboten werden:

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

Für Services, die unter der Internet-Domain „bicplatform.com.au“ und Sub-Domains angeboten werden:

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

Für Services, die unter der Internet-Domain „biccloud.com“ und Sub-Domains angeboten werden:

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

Für Services, die unter der Internet-Domain „biccloud.de“ und Sub-Domains angeboten werden:

- Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn

Für Services, die unter der Internet-Domain „biccloud.com.au“ und Sub-Domains angeboten werden:

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

Für Services, die unter anderen Internet-Domains angeboten werden, setzt GBTEC einen oder mehrere der genannten Subunternehmer ein, sofern GBTEC mit Ihnen im Einzelfall nichts anderes vereinbart hat.

1.3 Datenschutz und Informationssicherheit

Um die Einhaltung der Vorgaben zu Informationssicherheit und Datenschutz zu gewährleisten, setzt GBTEC ausschließlich zertifizierte Subunternehmer ein und schließt im Einzelfall ergänzende vertragliche Regelungen zur Einhaltung des gesetzlichen Datenschutzes ab, die im Folgenden gelistet sind:

- Amazon Web Services EMEA SARL, 5 Rue Plaetis, L-2338 Luxemburg: Zertifiziert nach DIN EN ISO 27001 durch Ernst & Young CertifyPoint B.V., Antonio Vivaldistraat 150, 1083 HP Amsterdam, The Netherlands siehe auch: https://aws.amazon.com/de/compliance/iso-27001-faqs, https://aws.amazon.com/de/compliance. Mit Amazon Web Services EMEA SARL hat GBTEC zudem eine Vereinbarung zur Auftragsdatenverarbeitung geschlossen.

- Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn: siehe auch: https://cloud.telekom.de
  Zertifiziert nach DIN EN ISO 27001 durch DEKRA Certification GmbH, Handwerkstrasse 15, 70565 Stuttgart, siehe auch: https://cloud.telekom.de/de/infrastruktur/open-telekom-cloud/mehr/compliance. Mit Telekom Deutschland hat GBTEC zudem eine Vereinbarung zur Auftragsdatenverarbeitung geschlossen.

- Microsoft Ireland Operations Limited, 70 Sir Rogersons's Quay, Dublin, Ireland: Zertifiziert nach DIN EN ISO 27001 durch TÜV Nord Cert GmbH & Co.KG, Genovevastraße 5, 51065 Köln siehe auch: https://news.microsoft.com/de-de/microsoft-azure-deutschland-iso-zertifizierungen, https://www.microsoft.com/de-

de/cloud/compliance). Mit Microsoft Ireland Operations Limited hat GBTEC zudem eine Vereinbarung zur Auftragsdatenverarbeitung geschlossen.

2. Service durch verbundene Unternehmen

2.1 Leistungen

- Unterstützung des Produktsupports durch Bereitstellung von Entwicklungsleistungen bei der technischen Fehleranalyse im Produktcode und der Identifikation von Workarounds
- Bereitstellung von Fehlerbehebungen in Form von Service-Releases von Produktkomponenten zur Fehlerbehebung

2.2 Anbieter

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

2.3 Datenschutz und Informationssicherheit

- Individualvereinbarung innerhalb der GBTEC-Gruppe

3. Service für das Produkt BIC Process Mining

Die folgenden Subunternehmer werden ausschließlich für die hier beschriebenen

Leistungen für das Produkt BIC Process Mining eingesetzt.

3.1 Leistungen

- Unterstützung des Produktsupports durch Bereitstellung von Entwicklungsleistungen bei der technischen Fehleranalyse im Produktcode und der Identifikation von Workarounds
- Bereitstellung von Fehlerbehebungen in Form von Service-Releases von Produktkomponenten zur Fehlerbehebung

3.2 Anbieter

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

3.3 Datenschutz und Informationssicherheit

GBTEC wird stets zuerst versuchen, die Leistung ohne die Weitergabe von personenbezogenen Daten zu erbringen. Sofern die Weitergabe von Daten zur Leistungserbringung unvermeidlich ist, wird GBTEC personenbezogene Daten anonymisieren und nur mit Zustimmung des Auftraggebers an diese Subunternehmen weitergeben.

Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Der Auftragnehmer hat folgende Maßnahmen ergriffen:

☒ Server sind in abgeschlossenen Serverräumen

☒ Schlüssel sind nur für IT-Support zugänglich

☒ Zutritt zum Gebäude nur per elektronischem Schlüssel bzw. Empfang möglich. Außerhalb der Bürozeiten wird das Gebäude von einem Wachdienst mit regelmäßigen Kontrollgängen gesichert.

☒ Für mobile Arbeitsgeräte besteht die Arbeitsanweisung, diese in zutrittsgeschützten Bereichen zu verwahren, sofern sie nicht persönlich beaufsichtigt werden.

Zugangskontrolle

Der Auftragnehmer hat folgende Maßnahmen ergriffen:

☒ Zugang zu allen IT-Systemen ist nur mit Passwort und verschlüsseltem Zugang möglich

☒ Für Passworte gelten Passwortrichtlinien zur Komplexität und Änderungshäufigkeit

☒ Umgang mit Zugangsdaten ist durch Arbeitsanweisung geregelt

Zugriffskontrolle

Der Auftragnehmer hat folgende Maßnahmen zur bedarfsorientierten Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung ergriffen:

☒ Zugriffskontrolle findet über Berechtigungssystem auf Server-Anwendungen und Netzwerklaufwerke statt

☒ Die Bewilligung von Berechtigungen findet durch den jeweiligen Vorgesetzten statt, die Erteilung der Berechtigung erfolgt durch den IT-Support.

Trennungskontrolle

Der Auftragnehmer hat folgende Maßnahmen ergriffen:

☒ Daten verschiedener Mandanten werden getrennt aufbewahrt und verarbeitet

☒ Die Aufbewahrung erfolgt entsprechend des Berechtigungssystems

☒ Die Verarbeitung von Daten eines Mandanten findet immer in einem definierten Mitarbeiterkreis (Abteilung und Team) statt

Pseudonymisierung

Der Auftragnehmer hat folgende Maßnahmen ergriffen:

☒ Mathematische Verfahren (u.a. Hashing)

Nähere Beschreibung / Weitere Maßnahmen: Für die Pseudonymisierung stell GBTEC auf Wunsch Werkzeuge bereit, mit denen Kunden ihre Daten vor der Übergabe an GBTEC pseudonymisieren können)

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Der Auftragnehmer hat folgende Maßnahmen ergriffen:

☒ Die Weitergabe von Daten erfolgt grundsätzlich über verschlüsselte Verbindungen. Dafür wird ein spezielles System (https://support.bicplatform.de) bereitgestellt.

Eingabekontrolle

Der Auftragnehmer hat folgende Maßnahmen ergriffen:

☒ Beschränkung der Arbeit mit allen Daten eines Auftraggebers auf die beauftragten Mitarbeiter erfolgt durch Berechtigungssystem und Verpflichtung der Mitarbeiter in Arbeitsanweisung

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Der Auftragnehmer hat folgende Maßnahmen ergriffen:

☒ Backup- und Recovery-Konzept mit katastrophensicherer Aufbewahrung. Ausfallsicherung durch redundante Festplattensysteme und unterbrechungsfreie Stromversorgung. Einsatz angemessener Schutzsoftware: Virenscanner, Firewalls, Spam-Filter, Datenverschlüsselung)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Wiederherstellbarkeit

Der Auftragnehmer hat folgende Maßnahmen ergriffen:

☒ Es gibt einen Incident-Response-Management

Datenschutzmanagement

Der Auftragnehmer hat folgende Maßnahmen ergriffen:

☒ Qualitätsmanagement implementiert

☒ Regelmäßige Audits etabliert

Auftragskontrolle

Der Auftragnehmer hat folgende Maßnahmen ergriffen:

☒ Betrieblicher Datenschutzbeauftragter für GBTEC ist Andreas Reinke (reinke@datenschutzbeauftragter.ruhr, 0234-5887727, arbeitgeber ruhr GmbH, Königsallee 67, 44789 Bochum)