Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO[1]

Zwischen der

.....

.....

.....

– im Folgenden **„Auftraggeber“**
bzw. „Verantwortlicher“ –

und der

Teamdb Business Solutions GmbH & Co. KG

Frankenring 18

30855 Langenhagen

– im Folgenden **„Auftragnehmer“**
bzw. „Auftragsverarbeiter“ –

wird folgende Vereinbarung geschlossen:

[1] DS-GVO = Europäische Datenschutz-Grundverordnung

Inhalt

1. Zusammenarbeit und Auswahl des Auftragsverarbeiters[2]

1.1. Zwischen dem Auftraggeber und der Teamdb Business Solutions GmbH & Co. KG als Auftragnehmer besteht eine Zusammenarbeit über Leistungen im IT-Umfeld. Da es im Rahmen der Durchführung dieser Leistungen möglich oder für die Auftragserfüllung notwendig ist, dass der Auftragnehmer Zugriff auf personenbezogene Daten erhält, bedarf es gemäß Art. 28 Abs. 3 S. DS-GVO zwischen dem Auftraggeber als Verantwortlichen und dem Auftragnehmer als Auftragsverarbeiter einer vertraglichen Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag.

1.2. Der Auftragsverarbeiter hat die DS-GVO in seinem Unternehmen umgesetzt. Hierüber existiert eine umfangreiche Dokumentation, die beim Auftragsverarbeiter eingesehen werden kann. Damit erfüllt der Auftragsverarbeiter die Anforderungen nach Art. 28 Abs. 1 DS-GVO.

1.3. Die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie die Wahrung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO obliegt allein der Verantwortung des Auftraggebers.

2. Gegenstand und Dauer des Auftrags

2.1. Der Auftragnehmer erbringt seine Leistungen für den Auftraggeber auf der Grundlage der seitens des Auftraggebers erteilten Aufträge oder der zwischen den Parteien geschlossenen Dienstleistungsverträge.

2.2. Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers gemäß dem vorliegenden Vertrag.

2.3. Die Vertragslaufzeit richtet sich nach der Laufzeit der erteilten Aufträge oder der geschlossenen Dienstleistungsverträge.

2.4. Darüber hinaus ist eine vorzeitige Beendigung dieses Auftrags, ohne Einhaltung einer Kündigungsfrist im Falle einer schwerwiegenden Verletzung von gesetzlichen oder vertraglichen Datenschutzbestimmungen zulässig, sofern ein Festhalten an dieser Vereinbarung für die jeweilige Vertragspartei nicht zumutbar ist.

2.5. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt eine schwerwiegende Verletzung dar.

[2] Mit Begriffen wie „Auftragsverarbeiter" können Personen männlichen und weiblichen Geschlechts gleichermaßen gemeint sein; aus Gründen der einfacheren Lesbarkeit wird im Folgenden nur die männliche Form verwendet. „Auftragsverarbeiter" und andere männliche Begriffe sind generisch maskuline Personenbezeichnungen, die so dem Gesetz entnommen wurden.

3. Form der Auftragserteilung

3.1. Der Auftraggeber erteilt seine Aufträge, Teilaufträge und Weisungen schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen werden unverzüglich schriftlich oder in einem dokumentierten elektronischen Format bestätigt.

3.2. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

4. Art und Zweck der Verarbeitung, Kategorien betroffener Personen

4.1. Der Umfang, die Art und der Zweck der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten richtet sich nach den zwischen den Parteien konkret vereinbarten Leistungen. Der Auftragnehmer erbringt für den Auftraggeber die Leistungen, die in den erteilten Aufträgen beschrieben sind.

4.2. Der Auftraggeber ist dafür verantwortlich die Datenkategorien und die Kategorien der Betroffenen, die im Rahmen der Vertragserfüllung durch den Auftragnehmer im Auftrag verarbeitet werden, in der Anlage zu diesem Vertrag auszuweisen. Darüber hinaus besteht die Pflicht zur fortlaufenden Prüfung und Ergänzung der Anlage, soweit durch weitere Beauftragungen neue Kategorien hinzukommen.

5. Ort der Datenverarbeitung

5.1. Die Verarbeitung und Nutzung der Daten durch den Auftragnehmer findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

5.2. Die Übermittlung personenbezogener Daten in ein Drittland oder an internationale Organisationen bedarf der vorherigen Zustimmung des Auftraggebers. Sie wird nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 50 DS-GVO erfüllt sind.

5.3. Soweit der Auftraggeber Microsoft Onlinedienste im Einsatz hat, beruht die Datenverarbeitung auf den geltenden Bestimmungen von Microsoft. Microsoft erfüllt gegenüber allen Kunden mit Wirkung vom 25. Mai 2018 die Verpflichtungen aus (a) der „Verarbeitung personenbezogener Daten; GDPR“ des Abschnitts „Datenschutzbestimmungen“ in den Bestimmungen für Onlinedienste und (b) aus den Bestimmungen der EU-Datenschutz-Grundverordnung in Anlage 4 der Bestimmungen für Onlinedienste. Die jeweils aktuell geltende Version der Bestimmungen für Onlinedienste ist unter https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx verfügbar. Microsoft stellt für alle Kunden die mit der EU-Kommission abgestimmten EU-Standardvertragsklauseln bereit und sichert damit zu,

dass ein angemessenes Datenschutzniveau international gewährleistet ist. Darüber hinaus ist Microsoft Privacy Shield Frameworks zertifiziert. Alle Übertragungen personenbezogener Daten an ein Drittland oder eine internationale Organisation unterliegen entsprechend angemessenen Absicherungen, wie sie Art. 46 DSGVO voraussetzt.

6. Pflichten des Auftragnehmers als Auftragsverarbeiter

6.1. Der Auftragnehmer und ihm unterstellte Personen, die Zugang zu den personenbezogenen Daten haben, werden die personenbezogenen Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind (Art. 29 DS-GVO).

6.2. Der Auftragnehmer beachtet, dass alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf die für die Auftragsverarbeitung einschlägigen rechtlichen Vorschriften der DS-GVO und das Datengeheimnis verpflichtet sind und über die sich aus diesem Auftrag ergebende Weisungs- bzw. Zweckbindung belehrt wurden.

6.3. Der Auftragnehmer wird die Datenverarbeitung mittels geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 32 DS-GVO durchführen.

6.4. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit dabei unterstützen, dass dieser seinen Pflichten hinsichtlich der in Art. 16 bis 20 und Art. 32 bis 36 DS-GVO genannten Rechte der betroffenen Personen nachkommen kann.

6.5. Der Auftragnehmer wird dem Auftraggeber alle erforderlichen Informationen im Hinblick auf die Kontrollverpflichtungen des Auftraggebers zur Verfügung stellen und Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und unterstützen. Der Auftraggeber hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung der gesetzlichen Pflichten und dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

6.6. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen als die vereinbarten, insbesondere nicht für eigene Zwecke.

6.7. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, sind als solche kenntlich zu machen.

6.8. Der Auftragnehmer wird den Auftraggeber darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 S. 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch

den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

6.9. Der Auftragnehmer teilt dem Auftraggeber Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit.

6.10. Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DS-GVO kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne des Art. 28 DS-GVO nachzuweisen.

7. Technische und organisatorische Maßnahmen

7.1. Der Auftragnehmer ist gemäß Art. 28 Abs. 3 S. 2 lit. c DS-GVO verpflichtet, diejenigen technischen und organisatorischen Maßnahmen (TOM) zu treffen und während der Vertragslaufzeit aufrechtzuerhalten, die erforderlich sind, um die in Art. 32 DS-GVO genannten Anforderungen zu gewährleisten. Der Auftragnehmer hat seine TOM in Anlage A 3 zu diesem Vertrag zusammengefasst.

7.2. 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.

7.3. Die technischen und organisatorischen Maßnahmen unterliegen dem Stand der Technik und dem technischen Fortschritt. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen und Produkte um- und einzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber mitzuteilen.

7.4. Für alle Clouddienste dritter Cloudanbieter gelten zusätzlich die Sicherheitsbestimmungen der Cloudanbieter. Die Cloudanbieter werden angemessene technische und organisatorische Maßnahmen zum Schutz von Kundendaten und personenbezogenen Daten treffen und aufrechterhalten. Für die Microsoft Onlinedienste gelten die in Anhang B der Bestimmungen für Onlinedienste beschriebenen Sicherheitsmaßnahmen zum Schutz der Kundendaten.

8. Unterauftragsverhältnisse

8.1. Der Auftragnehmer nimmt Auftragsverarbeiter als Subunternehmer nicht ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der

Auftragnehmer den Auftraggeber vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

8.2. Nimmt der Auftragnehmer die Dienste eines Subunternehmers in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag zwischen dem Auftraggeber als Verantwortlichen und dem Auftragnehmer als Auftragsverarbeiter festgelegt sind. Dabei müssen insbesondere hinreichende Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer als Auftragsverarbeiter gegenüber dem Auftraggeber als Verantwortlichen für die Einhaltung der Pflichten des Subunternehmers.

8.3. Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

8.4. Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

8.5. Für die bereits zum Zeitpunkt des Abschlusses dieses Vertrages feststehenden Subunternehmer erfolgt die schriftliche Genehmigung für die in der Anlage zu diesem Vertrag benannten juristischen oder natürlichen Personen.

8.6. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme, vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

9. Benennung eines Datenschutzbeauftragten

9.1. Der Auftragnehmer verpflichtet sich zur schriftlichen Benennung eines Datenschutzbeauftragten, soweit gesetzlich vorgeschrieben, gemäß Art. 37 DS-GVO.

9.2. Die Kontaktdaten des bestellten Datenschutzbeauftragten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Dies kann als Anlage zu diesem Vertrag erfolgen.

10. Rechte und Pflichten des Auftraggebers

10.1. Der Auftraggeber ist im Verhältnis zum Auftragnehmer wie ein Eigentümer der Daten anzusehen (§ 903 BGB analog) und Inhaber aller etwaigen Rechte.

10.2. Der Auftraggeber als Verantwortlicher ist gemäß Art. 5 Abs. 2 DS-GVO für die Einhaltung der in Art. 5 Abs. 1 DS-GVO festgeschriebenen Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich (Rechenschaftspflicht).

10.3. Der Auftraggeber ist für die rechtmäßige Erhebung, Verarbeitung und Nutzung der Daten sowie für die Implementierung eigener geeigneter technischer und organisatorischer Maßnahmen und die Wahrung der Betroffenenrechte verantwortlich.

10.4. Der Auftraggeber hat den Auftragnehmer unverzüglich darüber zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

10.5. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über Geschäftsgeheimnisse und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung des Vertrags bestehen.

11. Weisungsbefugnis des Auftraggebers

11.1. Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers gemäß Art. 29 DS-GVO. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

11.2. Der Weisungsberechtigte auf Seiten des Auftraggebers sowie der Weisungsempfänger auf Seiten des Auftragnehmers und die zuständigen Datenschutzbeauftragten, soweit eine gesetzliche Benennungspflicht besteht, sind schriftlich zu fixieren. Dies kann als Anlage zu diesem Vertrag erfolgen. Bei einem

Wechsel der zuständigen Ansprechpartner ist dem Vertragspartner unverzüglich und schriftlich der jeweilige Nachfolger mit Kontaktdaten mitzuteilen.

12. Zusammenarbeit mit den Aufsichtsbehörden / Verarbeitungsverzeichnisse

12.1. Dem Auftragnehmer ist bekannt, dass er gemäß Art. 31 DS-GVO verpflichtet ist, auf Anfrage mit dem Auftraggeber und der Aufsichtsbehörde bei der Erfüllung von Aufgaben zusammenzuarbeiten.

12.2. Dem Auftragnehmer ist bekannt, dass er gemäß Art. 30 Abs. 2 DS-GVO verpflichtet ist, ein eigenes Verzeichnis von Verarbeitungstätigkeiten für alle Kategorien von im Auftrag durchgeführten Tätigkeiten der Verarbeitung zu führen. Diese müssen der Aufsichtsbehörde auf Anfrage vorgelegt werden.

13. Maßnahmen bei Datenschutzverletzungen

13.1. Der Auftragnehmer ist gemäß Art. 33 Abs. 2 DS-GVO verpflichtet, jede ihm bekanntwerdende Verletzung des Schutzes personenbezogener Daten unverzüglich an den Verantwortlichen zu melden.

13.2. Der Auftragnehmer erstattet dem Auftraggeber in allen Fällen und unverzüglich eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

13.3. Der Auftragnehmer verpflichtet sich darüber hinaus unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen, den Auftraggeber bei den zu ergreifenden Maßnahmen und Meldepflichten gemäß Art. 33 und 34 DS-GVO zu unterstützen.

13.4. Der Auftragnehmer hält von ihm festgestellte Datenschutzverletzung schriftlich fest.

14. Haftung

14.1. Die nachfolgenden Haftungsklauseln betreffen ausschließlich das Vertragsverhältnis zwischen dem Auftraggeber und dem Auftragnehmer. Sie stellen keine Ausschlussklausel im Hinblick auf die Betroffenenrechte nach Art. 82 Abs. 1 DS-GVO dar.

14.2. Die Haftung des Auftragnehmers, gleich aus welchem Rechtsgrund, ist unbegrenzt für Schäden, die vorsätzlich oder grob fahrlässig verursacht werden oder die aus der schuldhaften Verletzung des Lebens, des Körpers oder der Gesundheit resultieren.

14.3. Der Auftragnehmer haftet nicht bei leichter Fahrlässigkeit. Dieser Ausschluss für die Haftung bei leichter Fahrlässigkeit gilt jedoch dann nicht, wenn es sich um die Verletzung einer wesentlichen Vertragspflicht (Kardinalpflicht) handelt.

Kardinalpflichten bzw. wesentliche Vertragspflichten sind solche Pflichten des Auftragnehmers, deren Erfüllung die ordnungsgemäße Durchführung dieses konkreten Vertrages überhaupt erst ermöglichen und auf deren Einhaltung der Kunde regelmäßig vertrauen darf; mithin also Pflichten, deren Verletzung ein Erreichen des Vertragszwecks gefährden würde.

14.4. Wenn und soweit der Auftragnehmer für leichte Fahrlässigkeit haftet, ist die Haftung bei Sach- und Vermögensschäden auf den vertragstypischen und vorhersehbaren Schaden beschränkt.

14.5. Alle Schadensersatzansprüche des Auftraggebers gegen den Auftragnehmer verjähren in 6 Monaten nach Lieferung. Dies gilt nicht für Ansprüche wegen unerlaubter Handlung oder vorsätzlicher Schädigung.

14.6. Soweit die Haftung des Auftragnehmers ausgeschlossen ist, gilt dies auch für die persönliche Haftung der Angestellten, Arbeitnehmer, Mitarbeiter, Vertreter und Erfüllungsgehilfen des Auftragnehmers.

14.7. Der Auftragnehmer haftet im Innenverhältnis zum Auftraggeber dann nicht, wenn er den Nachweis nach Art. 82 Abs. 3 DS-GVO erbringt.

14.8. Sollten Betroffene gegen den Auftragnehmer Ansprüche aufgrund datenschutzrechtlicher Pflichtverletzungen geltend machen, die nicht in die Verarbeitungssphäre des Auftragnehmers fallen, wird der Auftraggeber den Auftragnehmer von diesen Ansprüchen freistellen.

15. Umgang mit den Daten während und nach Beendigung des Auftrags (Exit-Klausel)

15.1. Gemäß Art. 28 Abs. 3 S. 2 lit. g DS-GVO wird der Auftragnehmer nach Wahl des Auftraggebers nach Abschluss der Erbringung der Verarbeitungsleistungen, spätestens aber mit Beendigung der Leistungsvereinbarung sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse, sowie Datenbestände dem Auftraggeber aushändigen oder nach vorheriger Zustimmung datenschutzgerecht vernichten, soweit nicht das Unionsrecht oder das Recht der Mitgliedstaaten eine Speicherung der personenbezogenen Daten vorschreibt.

15.2. Ein Löschen bzw. Vernichten von Daten ist dem Auftraggeber mit Zeitangabe schriftlich zu bestätigen. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind darüber hinaus durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

16. Schlussbestimmungen

16.1. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelungen eine solche rechtlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelungen am nächsten kommt.

16.2. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere einem Hauptvertrag, gehen die Regelungen dieses Vertrags vor. Nebenabreden, Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für die Änderung dieser Schriftformvereinbarung.

16.3. Dieser Vertrag und alle im Rahmen seiner Durchführung geschlossenen Rechtsgeschäfte unterliegen soweit anwendbar deutschem Recht unter Ausschluss des internationalen UN-Kaufrechts (UNCITRAL).

16.4. Gerichtsstand für alle Streitigkeiten aus dieser Vereinbarung ist der Gerichtsbezirk des Landgerichts Hannover.

16.5. Die nachfolgenden Anlagen sind Bestandteil dieses Vertrages.

_____	_____
Ort / Datum	Ort / Datum
_____	_____
Auftraggeber	Teamdb Business Solutions GmbH & Co. KG

Anlagen:

A 1 Kategorien / Personengruppen, die von der Verarbeitung betroffen sind

Art der Daten

Gegenstand der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien:

- ☒ Personenstammdaten (z.B. Name, Vorname, Anschrift und Geburtsdatum)
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☒ Vertragsstammdaten (z.B. Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☒ Vertragsabrechnungs- und Zahlungsdaten (z.B. Lohn, Gehalt und Reisekosten)
- ☒ IT-Nutzungsdaten (z.B. UserID, Passwörter und Rollen)
- ☒ Bankdaten (z.B. Kontoverbindung und Kreditkartennummer)
- ☒ Bonitätsdaten (z.B. Zahlungsverhalten und Bilanzen)
- ☐ Sonstige: _____

Kreis der Betroffenen

Der Kreis, der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen, umfasst:

- ☒ Kunden / Leistungsempfänger des Auftraggebers
- ☒ Beschäftigte des Auftraggebers
- ☒ Lieferanten / Dienstleister des Auftraggebers
- ☐ Sonstige: _____

A 2 Kontaktdaten

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner die Nachfolger bzw. die Vertreter mitzuteilen.

1. Weisungsberechtigte und Weisungsempfänger

Auftraggeber

Name	Telefon	E-Mail

Teamdb Business Solutions GmbH & co. KG (Auftragnehmer)

Name	Telefon	E-Mail
Karin Seiboth	0511 – 27 07 27 60	kseiboth@teamdb.de

2. Datenschutzbeauftragter des Auftraggebers

Name	Telefon	E-Mail

3. Datenschutzbeauftragter der Teamdb Business GmbH & Co. KG

Name	Telefon	E-Mail
Ulrich Seiboth	0511 – 27 07 27 60	datenschutz@teamdb.de

A 3 Technische und organisatorische Maßnahmen gem. Art. 32 DS-GVO

Es wird vom Auftragnehmer ein für die konkrete Auftragsverarbeitung angemessenes Schutzniveau gewährleistet. Dies wird wie folgt beschrieben:

1. Technische und organisatorische Sicherheitsmaßnahmen

Gemäß Artikel 28 Abs. 3 DSGVO sind die Vertragspartner verpflichtet, die technischen und organisatorischen Sicherheitsmaßnahmen festzulegen.

a) Innerbetriebliche Organisation des Auftragnehmers

Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

b) Konkretisierung der Einzelmaßnahmen

Der Auftragnehmer setzt die Anforderungen wie folgt in seinem Einflussbereich in Bezug auf diese Vereinbarung um. Darüber hinaus ist im Rahmen der besonderen Vertragskonstellation zwischen dem Cloud-Dienste Anbieter Microsoft, dem IT-Dienstleister als Auftragnehmer und dem Auftraggeber hinsichtlich der Konkretisierung der Einzelmaßnahmen auch auf die spezifischen Sicherheitsmaßnahmen von Microsoft zu verweisen.

2. Zutrittskontrolle

a) Mit dem Begriff „Zutritt" ist der physische Zugang von Personen zu Gebäuden und Räumlichkeiten gemeint, in denen IT-Systeme betrieben und genutzt werden. Dies können z.B. Rechenzentren sein, in denen Web-Server, Applikationsserver, Datenbanken, Mainframes, Speichersysteme betrieben werden und Arbeitsräume, in denen Mitarbeiter Arbeitsplatzrechner nutzen. Auch die Räumlichkeiten, in denen sich Netzkomponenten und die Netzverkabelungen befinden und verlegt sind, gehören hierzu. Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden (können), zu verwehren. Der Auftragnehmer muss deshalb dafür Sorge tragen, dass unbefugte Räume, in denen Daten vom Auftraggeber verarbeitet oder gespeichert werden, nicht betreten können und keinen Einblick oder Zugriff auf Datenverarbeitungsgeräte (Monitore, Drucker, etc.) erlangen können, auf denen diese Daten verarbeitet oder ausgegeben werden.

b) <u>Umsetzung der Zutrittskontrolle bei Teamdb</u>

Der Auftragnehmer hat die folgenden Maßnahmen zur Zutrittskontrolle umgesetzt:

Die Eingangstüren des Gebäudes sind mit folgender Schließanlage versehen:

☒ Manuelle Schließanlage ☐ Chipkarten Schließanlage

☐ Die Nutzung der Schließanlage wird dokumentiert

☒ Der Zutritt und Aufenthalt von Besuchern erfolgt nur in Begleitung von Firmenpersonal

☐ Der Zutritt von Reinigungs- und Wartungspersonal zum Gebäude wird dokumentiert

☒ Der Entzug von Gebäudezutrittsberechtigungen ist geregelt und dokumentiert

☒ Es besteht ein gesondertes Zutrittskonzept für Serverräume

c) Umsetzung der Zutrittskontrolle bei Microsoft

Desweitern ist auf die spezifischen Sicherheitsmaßnahmen von Microsoft zu verweisen. Die konkreten Maßnahmen hinsichtlich der Zutrittskontrolle zu Microsoft Systemen sind in den Online Services Terms beschrieben. Die Umsetzungen der Zutrittskontrolle bei Wortmann sind bei Wortmann beschrieben.

3. Zugangskontrolle

a) Ergänzend zur Zutrittskontrolle ist es Ziel der Zugangskontrolle zu verhindern, dass DV-Anlagen von Unbefugten benutzt werden, mit denen personenbezogene Daten gespeichert, verarbeitet oder genutzt werden. Unbefugte dürfen keinen Zugang zu den Datenverarbeitungssystemen des Auftragnehmers erlangen können. Daher muss der Auftragnehmer die mit der Erfüllung der Leistungen des Auftrags beauftragten Personen mit einer sicheren Benutzeridentifikation versehen. Desweitern ist auf die spezifischen Sicherheitsmaßnahmen hinsichtlich der Zugangskontrollen zu den Microsoft Rechenzentren auf die Bestimmungen in den Online Services Terms zu verweisen.

b) Umsetzung der Zugangskontrolle bei Teamdb

Der Auftragnehmer hat die folgenden Maßnahmen zur Zugangskontrolle umgesetzt:

☒ Das Firmennetzwerk ist durch eine Firewall geschützt

☒ Die Daten des Auftraggebers werden innerhalb des Firmennetzwerkes separiert

Die Mitarbeiter des Auftragnehmers müssen folgende Passwortvorgaben erfüllen:

☐ Individuelle Passwörter für verschiedene Systeme (keine Sammelpasswörter)

☒ Die Passwörter haben eine Mindestlänge/Komplexität, wenn zutreffend Anzahl der Zeichen:

8 Zeichen/Komplex

☐ Die Passwörter müssen regelmäßig gewechselt werden, wenn zutreffend Intervall angeben:

8 Zeichen/Komplex

☒ Der Zugang zum System wird gesperrt bei der fehlerhaften Eingabe des Passwortes, bitte Anzahl der Fehlversuche und Dauer der Sperrung angeben:

5 Versuche/30 min

An den folgenden Übergängen zum Firmennetzwerk werden Virenscanner eingesetzt:

☒ E-Mail Account ☒ FTP ☒ Web

☒ Mitarbeiter haben lokale Administrationsrechte

c) Umsetzung der Zugangskontrolle bei Microsoft

Desweitern ist auf die spezifischen Sicherheitsmaßnahmen von Microsoft zu verweisen. Die konkreten Maßnahmen hinsichtlich der Zugangskontrolle zu Microsoft Systemen sind in den Online Services Terms beschrieben.

4. Zugriffskontrolle

a) Die Anforderungen der Zugriffskontrolle sind darauf ausgerichtet, dass nur durch Berechtigte auf die Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht und dass die Daten nicht durch Unbefugte manipuliert oder gelesen werden können. Es dafür zu sorgen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

b) Umsetzung der Zugriffskontrolle bei Teamdb/Wortmann

Der Auftragnehmer hat die folgenden Maßnahmen zur Zugriffskontrolle umgesetzt:

☒ Ein Berechtigungskonzept ist vorhanden

☒ Die Anzahl der Administratoren mit Berechtigung ist auf ein Mindestmaß beschränkt

c) Umsetzung der Zugriffskontrolle bei Microsoft

Desweitern ist auf die spezifischen Sicherheitsmaßnahmen von Microsoft zu verweisen. Die konkreten Maßnahmen hinsichtlich der Zugriffskontrolle zu den Microsoft Systemen sind in den Online Services Terms beschrieben.

5. Weitergabekontrolle

a) Der Auftragnehmer muss verhindern, dass personenbezogene Daten vom Auftraggeber bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

b) Umsetzung der Weitergabekontrolle

Im Rahmen der Nutzung von Microsoft Online Diensten, liegt die Umsetzung der Weitergabekontrolle bei Microsoft. Microsoft setzt im Rahmen der Online Dienste bei der Datenübertragung über das Internet auf TLS Verschlüsselung. Der Auftraggeber hat zudem jederzeit die Möglichkeit weitere von Microsoft zur Verfügung gestellte Sicherheitstools als zusätzlichen Service auszuwählen und zu aktivieren.

6. Eingabekontrolle

a) Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Es müssen daher für derartige Maßnahmen entsprechende Protokollierungssysteme vorhanden sein.

b) Umsetzung der Eingabekontrolle

Im Rahmen der Nutzung von Microsoft Online Diensten, liegt die Umsetzung der Eingabekontrolle bei Microsoft. Microsoft bietet seinen Nutzern über das Trust Center einen Protokolldienst an. Mit diesem können Zugriffsberichte ausgeführt werden. An Hand dieser Berichte kann eine Eingabekontrolle nachgewiesen werden.

7. Auftragskontrolle

a) Die Kategorie Auftragskontrolle stellt sicher, dass die Daten, die im Auftrag des Kunden verarbeitet werden, auch nur dementsprechend verarbeitet werden können und keine fremden oder ungewollten Verarbeitungen stattfinden Der Auftragnehmer muss gewährleisten, dass personenbezogene Daten vom Auftraggeber nur gemäß deren Weisungen verarbeitet werden. Beschäftigt der Partner einen Unterauftragnehmer, so muss er diesen in gleicher Weise zur Erfüllung der Weisungen und zur Einhaltung des Datenschutzes verpflichten.

b) Umsetzung der Auftragskontrolle bei Teamdb/Wortmann

Der Auftragnehmer hat die folgenden Maßnahmen zur Auftragskontrolle umgesetzt:

☒ Die Mitarbeiter werden schriftlich auf das Datengeheimnis verpflichtet

☒ Die Mitarbeiter erhalten Schulungen zum Datenschutz

c) Umsetzung der Auftragskontrolle bei Microsoft

Desweitern ist auf die spezifischen Sicherheitsmaßnahmen von Microsoft zu verweisen. Die konkreten Maßnahmen hinsichtlich der Auftragskontrolle sind in den Online Services Terms beschrieben.

8. Verfügbarkeitskontrolle

a) Der Auftragnehmer muss dafür sorgen, dass personenbezogene Daten vom Auftraggeber gegen zufällige Zerstörung oder Verlust geschützt sind.

b) Umsetzung der Verfügbarkeitskontrolle bei Teamdb/Wortmann

Der Auftragnehmer hat die folgenden Maßnahmen zur Verfügbarkeitskontrolle umgesetzt:

Häufigkeit der Datensicherungsmaßnahmen:

☒ täglich ☐ monatlich ☐ jährlich

Aufbewahrungsort von Sicherungsdatenträgern:

☐ Safe ☒ externe Auslagerung in der Cloud

c) Umsetzung der Verfügbarkeitskontrolle bei Microsoft

Desweitern ist auf die spezifischen Sicherheitsmaßnahmen von Microsoft zu verweisen. Die konkreten Maßnahmen hinsichtlich der Verfügbarkeitskontrolle sind in den Online Services Terms beschrieben.

9. Trennungsgebot

a) Es ist dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden. Die Trennung der Daten muss so gestaltet sein, dass eine „Vermischung" mit Daten anderer Vertragspartner / Auftraggeber des Auftragnehmers und auch unbefugte Zugriffe Dritter (auch versehentlich) unmöglich sind. Sollten Daten anderer Vertragspartner / Auftraggeber des Auftragnehmers von behördlichen Zugriffen bzw. Beschlagnahme betroffen sein, muss gewährleistet sein, dass die Daten vom Auftraggeber davon unberührt bleiben. Die Daten dürfen nicht zu Testzwecken herangezogen werden, welche nicht Bestandteil der Leistungen des Hauptvertrages sind.

b) Umsetzung des Trennungsgebotes bei Teamdb/Wortmann

Der Auftragnehmer hat die folgenden Maßnahmen zum Trennungsgebot umgesetzt:

☒ Daten des Auftraggebers werden in einem eigenen Mandat vorgehalten

☒ Mitarbeiter werden schriftlich dazu verpflichtet, Informationen aus Datenbeständen des Auftraggebers nicht in andere Projekte mit einzubringen

c) Umsetzung des Trennungsgebotes bei Microsoft

Desweitern ist auf die spezifischen Sicherheitsmaßnahmen von Microsoft zu verweisen. Die konkreten Maßnahmen hinsichtlich des Trennungsgebotes sind in den Online Services Terms beschrieben.

Wir versichern, dass die hier getätigten Angaben dem aktuellen Stand der bei uns umgesetzten technischen und organisatorischen Maßnahmen zum Datenschutzniveau und zur Datensicherheit entsprechen. Abweichungen der hier getätigten Angaben sind dem Auftraggeber unmittelbar zu melden.

A 4 Genehmigte Subunternehmer

Nr.	Unterauftragnehmer (Firma, Anschrift, Ansprechpartner)	Verarbeitete Datenkategorien	Verarbeitungsschritte / Zweck der Unterauftragsdatenverarbeitung
01	Microsoft Ireland Operations Ltd. Building 3, Carmanhall Road Sandyford Industrial Estate 18 Dublin, Ireland	Die Datenkategorien sind jeweils in Punkt 2 „Konkretisierung des Auftragsinhaltes“ zu finden.	Die Zurverfügungstellung und Erbringung von Wartungsleistungen der Plattform Microsoft Azure
02	Microsoft Corporation One Microsoft Way Redmond, WA 98052, USA	Die Datenkategorien sind jeweils in Punkt 2 „Konkretisierung des Auftragsinhaltes“ zu finden.	Die Erbringung von möglichen Wartungsarbeiten an der Plattform Microsoft Azure
03	QBS (CSP) Quattro Business Solutions DACH GmbH Schellerdamm 4 21079 Hamburg, Germany	CSP Vertragsdaten	Verwalten der Verträge
04	ADN (CSP) Distribution GmbH Josef-Haumann-Str. 10 44866 Bochum, Germany	CSP Vertragsdaten	Verwalten der Verträge
05	Also (CSP)	CSP Vertragsdaten	Verwalten der Verträge

	Deutschland GmbH Lange Wende 43 59494 Soest, Germany		
06	Ascendit GmbH Wittland 2-4 24109 Kiel, Germany	ISV für D365 CRM	Softwareerweiterung/Support
07	Anveo conion media GmbH Fruchtallee 23a 20259 Hamburg, Germany	ISV für D365 NAV	Softwareerweiterung/Support
08	Wortmann AG Bredenhop 20 32609 Hüllhorst, Germany	CSP/Rechenzentrum	Zurverfügungsstellung von Server und Plattformdiensten
09	SolarWinds MSP Europe Headquarter Unit 1101, Building 1000 City Gate, Mahon Cork, Ireland	Managed Services Portal Mitarbeiter	Daten für Managed Services Virenschutz Datensicherung (Rechenzentrum Frankfurt/Main)
10	Securepoint GmbH Bleckeder Landstr. 28 21337 Lüneburg, Germany	Mitarbeiterdaten	Firewall, Zugriffsbeschränkung Service/Kunde
11	QuoHotel Parc Bit, C/Sophie Germain,Lleret Planta 1, 07121 Palma, Spain	ISV Hotelbereich Die Datenkategorien sind jeweils in Punkt 2 „Konkretisierung des	Software und Service Hotellösung NAV

		Auftragsinhaltes“ zu finden	
12	KK/Bröring Kniggendorf + Kögler GmbH Hamburger Str. 4 30880 Laatzen, Germany	Service für Schlüsseldepot Kundendaten	Software und Service (Datenzugriff)
13	WordPress **Aut O’Mattic A8C Ireland Ltd.** Business Centre, No.1 Lower Mayor Street International Financial Services Centre Dublin 1, Irland	Webseiten und Anmeldedaten	Onlinemarketing
14	MailChimp The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA	E-Mail, Adresse, Anschrift, Kontaktdaten	E-Mail Marketing
15	SIEVERS-GROUP Hans-Wunderlich-Str. 8 49078 Osnabrück	ISV für 365 BC und ELO	Softwarewartung und Support

☐ Zum Zeitpunkt des Vertragsschlusses liegt keine Beauftragung von Subunternehmern seitens des Auftragnehmers vor. (**Bitte obige Tabelle streichen**)