

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO (Datenschutz-Grundverordnung)

Vereinbarung

zwischen

Altenheim Friedrichsburg gGmbH
Offenbergstraße 19, 48151 Münster

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

Connex Communication GmbH
Balhorne Feld 11, D-33106 Paderborn

nachstehend Auftragnehmer genannt

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Hauptvertrag (21.10.2014) in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie ersetzt ggfs. bestehende, ältere Datenschutzvereinbarungen und findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten des Auftraggebers verarbeiten. Soweit der Auftraggeber den Regelungen des Datenschutzgesetzes der Evangelischen Kirche in Deutschland (DSG-EKD n.F.) oder des kirchlichen Datenschutzgesetzes (KDG) unterliegt, wird in Ergänzung zu den nachfolgenden Regelungen auf der Grundlage der DSGVO und dem BDSG n.F. festgehalten, dass für die Vertragsparteien auch die Bestimmungen des DSG-EKD n.F. und des KDG gelten. Das bedeutet u.a., dass sich der Auftragnehmer ggf. auch der Kontrolle kirchlicher Datenschutzbeauftragter unterwirft.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Hauptvertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen wird die Software Vivendi (und ergänzende Partnerprodukte, etwa für Rechnungs- und Personalwesen) zur Erfassung und Dokumentation personenbezogener Daten genutzt.

Gegenstand der Verarbeitung personenbezogener Daten sind dabei folgende Datenarten bzw. Datenkategorien:

- Personenstammdaten, Gesundheitsdaten, Kommunikationsdaten
- Vertragsstammdaten, Abrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Religion, Fotos, Emailadressen

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

- Kunden (Bewohner, Patienten, Klienten)
- Interessenten
- Beschäftigte
- Ansprechpartner

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrages.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutzgrundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Sollte § 203 StGB im Übrigen einschlägig sein, ist dieser ebenfalls zu berücksichtigen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen.

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO gilt §3 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Als Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, dienen

- aktuelle Berichte unabhängiger Instanzen: Bestätigungsvermerk des Abschlussprüfers (Wirtschaftsprüfer), zertifizierter Datenschutz gemäß OH-SOZ (Althammer und Kill GmbH), Zertifizierung ISO 9001:2015 (TÜV Rheinland)
- Durchführung von internen Selbstaudits

(2) 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.

Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn dies im Vertrag vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher schriftlich zugestimmt hat.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber. In Anlage 3 sind mögliche Unterauftragsverhältnisse zum Zeitpunkt der Auftragsvergabe aufgelistet.

Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt (als Option).

(3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

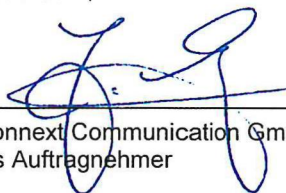
§ 8 Informationspflichten, Schriftformklausel, Rechtswahl, Sonstiges

- (1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.
- (2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
- (4) Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der EU/EWR in einem sog. sicheren „Drittstaat“ erbringen möchte bzw. die Leistungserbringung dorthin zu verlagern plant, wird der Auftragnehmer zuvor die schriftliche Zustimmung durch den Auftraggeber einholen.
- (5) Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftragnehmers.

§ 9 Haftung

Eine zwischen den Parteien im Leistungsvertrag (Hauptvertrag zur Leistungserbringung) vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart wurde.

Paderborn, 18.01.2018


Connext Communication GmbH
als Auftragnehmer

Münster, den 15. JAN. 2019

Münster, _____

ALTENHEIM FRIEDRICHSBURG gGmbH
HOPPENDAMM 33
48151 MÜNSTER

Altenheim Friedrichsburg gGmbH
als Auftraggeber (Stempel & Unterschrift)
D18077

Martin Runde
Geschäftsführer

Anlage 1:
Datenschutzbeauftragte/ Ansprechpartner

Beim Auftragnehmer ist folgende Person als Datenschutzbeauftragter bestellt:

Alexander Overmann | Telefon +49-5251-771-157 | Fax +49-5251-771-33157 | datenschutz@connext.de

Beim Auftraggeber ist folgende Person als **Datenschutzbeauftragte/r** bestellt:

Vor- und Nachname	Telefon/ Fax	Emailadresse
Frau Antonia Becker	0251 - 8901-384 Fax: 0251 - 89014317	datenschutzbeauftragter @caritas-muenster.de

Sofern kein Datenschutzbeauftragter bestellt werden muss, wird beim Auftraggeber folgende Person als **Ansprechpartner** benannt:

Vor- und Nachname	Telefon/ Fax	Emailadresse

Anlage 2:

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

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

1. Zutrittskontrolle (Räume und Gebäude)

Ziel: Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.

- Zutrittskontrolle und Berechtigungsvergabe mittels gesichertem Transponder-System
- Der Zutritt zum Rechenzentrum ist auf einen kleinen Personenkreis beschränkt
- Alarmanlage mit direkter Anschaltung an den Wachschatz
- Eingezäuntes, kameraüberwachtes Betriebsgelände

2. Zugangskontrolle (IT-Systeme u. Anwendungen)

Ziel: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Benutztes Kennwortverfahren erfordert eine Mindestlänge und Komplexität
- Automatische Sperrung aller Bildschirmarbeitsplätze mit Kennwortabfrage bei Reaktivierung
- Zentrale Datenspeicherung auf gesicherten Serversystemen
- Sichere Verschlüsselung der Festplatten an/ in den Systemen aller Mitarbeiter

3. Zugriffskontrolle (Auf Daten und Informationen)

Ziel: Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

- Differenzierte Berechtigungen pro Benutzer nach seinen Aufgaben
- Zugriffsrechte im Dateisystem
- Überwachung der Logins der Benutzer (wann/ wo erfolgte das Login)

4. Trennbarkeit

Ziel: Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können.

- Zweckbindung der erhobenen Daten an einen Supportfall
- Funktionstrennung zwischen Produktions- und Testdaten

5. Pseudonymisierung

Ziel: die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzufügung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

- Pseudonymisierung von Klienten- und Mitarbeiterstammdaten in Vivendi für Fernwartungen
- Pseudonymisierung von Daten bei BI-Auswertungen möglich

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

6. Weitergabekontrolle

Ziel: Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

- Verschlüsselung der verwendeten Tunnelverbindungen (VPN = Virtual Private Network) bei externen Zugriffen
- Sichere Verschlüsselung der Festplatten an/ in den Systemen aller Mitarbeiter

7. Eingabekontrolle

Ziel: Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

- Permanente Protokollierung der Fernwartungssitzungen mittels Teamviewer
- Aufruf- und Änderungshistorie in Vivendi

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

8. Verfügbarkeitskontrolle

Ziel: Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

- Einsatz eines dreistufigen Backup-Verfahrens
- SAN-Spiegel in getrennten Gebäude-/ Brandabschnitten
- Räumlich getrennte Aufbewahrung der Backup-Medien
- Spiegeln aller in Serversystemen/SAN verwendeten HD/SSD durch geeignete RAID-Verfahren

- Unterbrechungsfreie Stromversorgung (USV) aller Servertechnik und umgebender Peripherie
- Virenschutz auf allen Clients und allen Servern
- Hardware-Firewall, redundant vorhanden
- Einsatz von Rauchmeldern im Serverraum und direkt mit der Feuerwehr verbundener Brandmeldeanlage
- Redundant vorhandene Klimatisierung des Rechenzentrums
- Netzersatzanlage: Diesel-Notstromaggregat integriert

9. Wiederherstellbarkeit

Ziel: Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können.

- Geregelte Befugnisse für Beschaffung und Einkauf
- Urlaub- und Stellvertreterregelung unternehmensweit
- Einsatz eines mehrstufigen Backup-Verfahrens mit umfassender Rücksicherung
- Einheitlich gültiges Backup-Verfahren vereinfacht ggf. nötige Rücksicherungen

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

10. Leitlinie(n), Richtlinien, Arbeitsanweisungen und Sicherheitskonzepte

- jährliche Auditierung durch Rezertifizierung der ISO 9001:2015 und Wirtschaftsprüfer
- Kontinuierliches Monitoring von Netzwerkkomponenten mittels zentraler Auditinglösung inkl. Alerting
- Datenschutzhandbuch, Arbeitsanweisungen, Verfahrensanweisungen integriert im QMS
- Videoüberwachung im Rechenzentrum
- Überwachung des Gebäudes außerhalb der Arbeitszeiten durch eine Alarmanlage mit direkter Anschaltung an den Wachschutz

11. Regelmäßige Kontrollen, Dokumentation und ggf. Optimierung

- Dokumentation über erfolgte Sicherungen
- Regelmäßige Kontrolle der Sicherungen
- Jährliches Datenschutz-Selbstaudit
- dokumentierte Standardvorgabe zu Konfigurationen im Intranet

12. Datenschutzfreundliche Voreinstellung (Art. 25 DSGVO)

- Datenschutzkonforme Softwarelösung (Privacy by Design)
- Datenschutzfreundliche Grundkonfiguration (Privacy by Default)
- Umfassendes Rechte- und Rollenkonzept

13. Kontrolle der Unterauftragnehmer

- Formalisiertes Vertragsverhältnis und Kontrolle der TOMs

Anlage 3:**Unterauftragsverhältnis beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe**

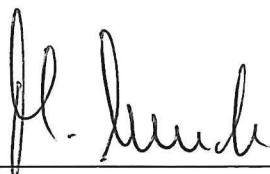
Subunternehmer ist jedes im Rahmen des Auftrages tätig werdende Unternehmen, das nicht mit dem Auftragnehmer identisch ist. Beauftragt der Auftraggeber selbst eine Teilleistung direkt bei einem anderen Unternehmen, wird dieses Unternehmen nicht Subunternehmer im Sinne dieser Vereinbarung.

Folgenden Unterauftragsverhältnisse bestehen beim Auftragnehmer zum derzeitigen Zeitpunkt:

Nr.	Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung	Verantwortlicher
1	Ralph Klee e.K., Elisabethstr. 6, 51429 Bergisch Gladbach	Support/ Consulting Diamant	Vor Ort beim Kunden, Support und Datenübernahme per Fernwartung	Ralph Klee
2	Sten-Eike Buda Consulting, Roomersheide 99, 44797 Bochum	Support/ Consulting Diamant	Vor Ort beim Kunden, Support und Datenübernahme per Fernwartung	Sten-Eike Buda
3	TraiCon Schmidt GmbH, Im Orot 3, 45711 Datteln	Support/ Consulting Diamant	Vor Ort beim Kunden, Support und Datenübernahme per Fernwartung	Markus Schmidt
4	rocon GmbH, Heinrich-Schelper-Straße 2, 27356 Rotenburg	Support/ Consulting Sage HR	Vor Ort beim Kunden, Support und Datenübernahme per Fernwartung	Steffen Rost, GF
5	Diamant Software GmbH & Co. KG, Stadtring 2, 33647 Bielefeld	3rd Level Support Diamant	Vor Ort beim Kunden, Support und Datenübernahme per Fernwartung	Roland Hofstetter, GF
/	/	/	/	/

Der Auftraggeber stimmt zu, dass die genannten Subunternehmer im Bereich der aufgeführten Teilleistung tätig werden können. Bei Nicht-Zustimmung betreffenden Subunternehmer streichen – bitte beachten Sie, dass dies u.U. verlängerten Bearbeitungszeiten und/ oder eingeschränkten Services in den jeweiligen Teilbereichen führen kann.

Münster, 16.01.2019



Altenheim Friedrichsburg gGmbH
als Auftraggeber (Stempel und Unterschrift)
D18077

ALTENHEIM FRIEDRICHSBURG gGmbH
HOPPENDAMM 33
48151 MÜNSTER