Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO

zwischen

Kunden

Verantwortlicher – nachstehend Auftraggeber genannt

und dem / der

blue connect GmbH
Barbarossahof 19
99092 Erfurt

Auftragsverarbeiter – nachstehend Auftragnehmer genannt

1. Präambel

Der Auftraggeber möchte den Auftragnehmer mit bestimmten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

2. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand dieser Vereinbarung ist die Regelung der Rechte und Pflichten des Verantwortlichen und des Auftragsverarbeiters. Die Vereinbarung gilt unter der Bedingung, dass im Rahmen einer Leistungserbringung (nach mitgeltenden Dokumenten) eine Verarbeitung von personenbezogenen Daten durch die blue connect GmbH für den Kunden im Sinne der anwendbaren Datenschutzrechte erfolgt. Sie gilt für Serviceleistungen und Fernwartungen, sowie Konfigurationsarbeiten automatisierter Verfahren oder an Datenverarbeitungsanlagen, wenn der Zugriff auf personenbezogene Daten dabei nicht auszuschließen ist. Aus den Dokumenten und Anlagen der jeweiligen Vorgänge ergeben sich Gegenstand, Dauer, Rechtsgrundlage und Art und Zweck sowie Kategorien der betroffenen Personen.

(2) Dauer

Die Laufzeit dieses Ergänzungsvertrages richtet sich nach der jeweiligen Laufzeit der Hauptverträge oder ist in den weiteren Dokumenten zum Auftrag festgehalten.

3. Begriffsbestimmungen

(1) Verantwortlicher

Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein oder gemeinsam mit allen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter

Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO die Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Auftragsverarbeiter ist die blue connect GmbH.

(3) Personenbezogene Daten

Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Verarbeitung

Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

4. Zuständige Aufsichtsbehörde

Die für den Auftragnehmer zuständige Aufsichtsbehörde ist „Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit“. Der Auftraggeber und der Auftragnehmer und ggf. deren Vertreter arbeiten auf Anfrage mit der zuständigen Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5. Rechte und Pflichten der blue connect GmbH

(1) Datenverarbeitung

Die blue connect GmbH verarbeitet die personenbezogenen Daten ausschließlich im Rahmen der getroffenen Verträge, Aufträge, Vereinbarungen und nach Weisung des Kunden. Außerdem verarbeitet die blue connect GmbH personenbezogene Daten ausschließlich für die beschriebenen Zwecke und gibt die Daten nicht an unberechtigte Dritte weiter. Die blue connect GmbH verpflichtet sich, die Daten nur an berechtigte und nach dem Datenschutzrechten auf Vertraulichkeit geschulten und verpflichteten Mitarbeiter zu übergeben und diese nur durch die entsprechenden Mitarbeiter zu verarbeiten.

(2) Datenschutzbeauftragter

Es erfolgte die schriftliche Bestellung eines Datenschutzbeauftragten durch die blue connect GmbH, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

(3) Technische und organisatorische Maßnahmen

Die blue connect GmbH verpflichtet sich die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO durchzuführen. [Einzelheiten in Anlage 1]

(4) Information bei Kontrollen der Aufsichtsbehörde

Der Auftraggeber wird unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informiert, 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.

(5) Überprüfung der Schutzmaßnahmen

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.

6. Rechte und Pflichten des Kunden

(1) Zulässigkeit der Datenverarbeitung

Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Kunde verantwortlich. Der Kunde wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z.B. durch Einholung von Einwilligungserklärungen) geschaffen werden, damit die blue connect GmbH die vereinbarten Leistungen auch insoweit gesetzeskonform erbringen kann.

(2) Unterstützung

Der Kunde wird in Betracht auf die betreffende Verarbeitung die blue connect GmbH bei Verdacht auf Datenschutzverletzungen und anderen Unregelmäßigkeiten bei der Verarbeitung von personenbezogenen Daten unverzüglich und vollständig darüber informieren. Außerdem wird der Kunde in Betracht auf die ihn betreffende Verarbeitung die blue connect GmbH bei der Prüfung möglicher Verstöße und bei der Abwehr von Ansprüchen Betroffener durch Aufsichtsbehörden zeitnah und umfänglich unterstützen.

(3) Überprüfungen

Der Kunde kann auf eigene Kosten die Einhaltung der Vorschriften über den Datenschutz und der in dieser Vereinbarung beschriebenen Pflichten durch die Einholung von Auskünften und die Kontrolle vor Ort überprüfen. Er kann die Kontrollen selbst durchführen oder durch einen von ihm beauftragten Dritten auf seine Kosten durchführen lassen. Die vom Kunden mit der Kontrolle beauftragten Personen oder Dritte sind nachweislich zur Wahrung der Vertraulichkeit zu verpflichten. Die vom Kunden durchgeführten Kontrollen sind mit der blue connect GmbH in Voraus abzusprechen und müssen legitimiert werden. Dritte dürfen hierbei keine Vertreter von Wettbewerbern der blue connect GmbH sein. Die Kontrollen dürfen den Betriebsablauf der blue connect GmbH nicht stören.

(4) Weisungen

Die blue connect GmbH wird personenbezogene Daten nur auf dokumentierte Weisung des Kunden erheben, verarbeiten oder nutzen. Dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine Internationale Organisation. Wird die blue connect GmbH durch das Recht der Europäischen Union oder der Mitgliedsstaaten, dem sie unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt sie dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit. Alle Weisungen des Kunden werden durch diesen Vertrag festgelegt und können vom Auftraggeber in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen sind der blue connect im Voraus zu benennen.

Der Auftraggeber hat dafür zu sorgen, dass seine Mitarbeiter, die Weisungen an die blue connect GmbH erteilen, auch dazu berechtigt sind. Bei einem Wechsel oder Ausfall der weisungsberechtigten Person ist die blue connect GmbH umgehend schriftlich zu informieren. Die blue connect GmbH darf eine Durchführung von offensichtlich rechtswidrigen Weisungen ablehnen.

7. Technisch-organisatorische Maßnahmen

(1) Die blue connect GmbH hat die Umsetzung die in Anlage 1 dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung stehts einzuhalten

(2) Die blue connect GmbH hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

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

8. Unterauftragsverhältnisse

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 die blue connect GmbH 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. Die blue connect GmbH 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.

(1) Befugnis

Die blue connect GmbH darf zur Erfüllung der in diesem Vertrag beschriebenen Aufgaben weitere Auftragsverarbeiter (Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter) einsetzen.

(2) Genehmigung

Für alle in der Anlage 2 aufgeführten Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter und die genannten Gegenstände gilt die Genehmigung des Kunden als erteilt. Der Kunde erteilt hiermit der blue connect ebenso die Genehmigung für den zukünftigen Einsatz weiterer Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter.

9. Schlussbestimmungen

(1) Gültigkeit

Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(2) Gerichtsstand

Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Erfurt.

(3) Rechtsgrundlage

Dieser Vereinbarung zur Auftragsverarbeitung liegen die Bestimmungen der EU-Datenschutzgrundverordnung (DS-GVO) zugrunde.

(4) Vorrang

Bei Wiedersprüchen zwischen den Bestimmungen dieser Vereinbarung und Bestimmungen sonstiger Vereinbarung zwischen blue connect GmbH und Kunden, sind die Bestimmungen dieser Vereinbarung maßgebend.

(5) Verantwortung

Der Kunde gewährleistet in seinem Verantwortungsbereich die Umsetzung der sich auf geltenden rechtlichen Bestimmungen ergebenden Pflichten bei der Verarbeitung personenbezogener Daten.

(6) Haftung

Für den Ersatz von Schaden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich. Die Parteien stellen sich jeweils von Haftungsansprüchen frei, wenn eine der Parteien nachweisen kann, dass sie in Keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

Anlage 1 – Technisch-organisatorische Maßnahmen (TOMs) der blue connect GmbH (Art. 32 DSGVO)

Um einen gerechten Schutz personenbezogener Daten zu gewährleisten, wurden technische und organisatorische Maßnahmen eingeleitet. Nach der DSGVO müssen sich TOMS nun nach dem Zweck der Verarbeitung sowie dem Stand der Technik richten. Diese sind gegliedert in Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit:

Vertraulichkeit

Zutrittskontrolle:

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene/betriebliche Daten verarbeitet oder genutzt werden, zu verwehren:

- Schlüsselvergabe mit Protokollierung (Schlüsselliste)
- Server im abschließbaren Raum
- Schränke mit Personenstammdaten und Vertragsdaten/Buchhaltung verschlossen

Zugangskontrolle:

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Einrichtung eines Benutzeraccounts pro Mitarbeiter
- Vergabe von Passwörtern im CRM
- Absicherung der Systeme und Netzwerke gegen Zugänge von außen (Firewall)
- Passwortrichtlinie
- Automatische Bildschirm-Sperre
- Sicherung der Arbeitsplätze bei Abwesenheit
- Clean-Desk-Policy
- Freigabe über Netzwerk für Zugang von außen nur für befugte Mitarbeiter (Server)

Zugriffskontrolle:

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverabeitungssystems Berechtigten ausschließlich auf die Ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene/betriebliche Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Berechtigungskonzepte
- Zugriffslisten an Mitarbeiter zugeteilt
- Löschbefugnisse nur begrenzt verfügbar
- Adminrechte auf BL und GF begrenzt
- Personalstammdaten und Geschäftsdaten auf Server nur für GF, QMB und BL zugänglich
- Regelmäßige Kontrolle der Gültigkeit der zugewiesenen Berechtigungen
- Clean-Desk-Policy
- Passwortgesicherte Drucker geben Dokumente nur nach Authentifizierung aus (Kennwort)
- Mitarbeiter zur Einhaltung des Datenschutzes verpflichtet

Trennungskontrolle:

Maßnahmen, die gewährleistet, dass eine getrennte Verarbeitung von Daten geschieht, die zu unterschiedlichen Zwecken dienen:

- CRM trennt die Daten nach Verarbeitungszweck
- Funktionstrennung durch Zugriffslisten geregelt (Innendienst, Außendienst direkt/Indirekt, GF, Admin)

Integrität

Weitergabekontrolle:

Maßnahmen, die gewährleisten, dass personenbezogene/betriebliche Daten 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 welche Stellen eine Übermittlung personenbezogener/betrieblicher Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Eingabe von Auftragsdaten in festgelegten Portalen der Netzbetreiber
- Export von Kundendaten nur durch befugte Mitarbeiter möglich (Steuerung durch Zugriffsrechte in der Benutzerverwaltung CRM)
- In den Managementdaten werden Änderungen erfasst

Eingabekontrolle:

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene/betriebliche Daten und Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Der Admin hat die Möglichkeit, über Aktivitätslisten Login-Daten nachzuvollziehen.
- Im CRM werden erstellte und geänderte Daten dokumentiert, der Verfasser wird angezeigt.

Auftragskontrolle:

Maßnahmen, die gewährleisten, dass personenbezogene/betriebliche Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Datenschutzvereinbarungen mit Lieferanten und Partnern
- Vereinbarung zu Auftragsverarbeitung

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle:

Maßnahmen, die gewährleisten, dass personenbezogene/betriebliche Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Regelmäßige Datensicherung
- Virenschutz
- Regelmäßige Software-Updates
- Eingeschränkte Löschbefugnisse über Zugriffslisten geregelt
- jährliche Überwachungsaudits gemäß DIN ISO 9001

Anlage 2 – Bestehende Subunternehmer

Folgende Unterauftragnehmer agieren für die blue connect GmbH und könnten sich ggf. auf den Auftrag zwischen Kunde und blue connect GmbH beziehen.

Unternehmer / Unternehmen	Gegenstand der Unterbeauftragung
Torsten Steinbrück	Vertriebspartner
STH Stefan Töppler Handelsagentur	Vertriebspartner
Martin Kaliner	Vertriebspartner
Franz Heinze	Vertriebspartner
Gerald Saworra	Vertriebspartner
Blueline Communications Ralf Hochbach	Vertriebspartner
Gino Käthner	Vertriebspartner
Volker Schulz	Vertriebspartner
Seven Principles AG	Bereitstellung MDM
NTT Europe Limited	Hosting
TAKENET GmbH	Hosting
Host Europe GmbH	Hosting
Charalis	Callcenter
TeamViewer GmbH	Fernwartungstool
ENO Telecom	Logistikleistungen
KOMSA Kommunikation Sachsen AG	Logistikleistungen
Wortmann	Logistikleistungen