



## Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

### Vereinbarung

zwischen dem/der

[Redacted area containing four horizontal white bars for signature or identification]

- Verantwortlicher - nachstehend Auftraggeber genannt -  
und dem/der

**bugsupport Inh. Till Heppner**  
**Neugasse 15-19**  
**65183 Wiesbaden**

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

### 1. Gegenstand und Dauer des Auftrags

#### (1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

- Wartung & Pflege der Server- und Clientsysteme
- Hosting der Cloud-Telefonanlage

#### (2) Dauer

Der Auftrag ist unbefristet erteilt. Die Kündigungszeiten ergeben sich aus den Allgemeinen Geschäftsbedingungen. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

### 2. Konkretisierung des Auftragsinhalts

#### (1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck

der Aufgaben des Auftragnehmers:

- Wartung & Pflege der Server- und Clientsysteme
- Hosting der Cloud-Telefonanlage

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. DS-GVO erfüllt sind. Das angemessene Schutzniveau wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO).

#### (2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

- Personenstammdaten
- Kommunikationsdaten (z. B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

#### (3) Kategorien betroffener Personen

- Die Kategorie der durch die Verarbeitung betroffenen Personen umfassen:
  - Kunden
  - Interessenten
  - Abonnenten
  - Beschäftigte
  - Lieferanten
  - Handelsvertreter
  - Ansprechpartner

### **3. Technisch-organisatorische Maßnahmen**

(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.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 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 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**

(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.

(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 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr Till Heppner, +49 611 94588270, hallo@bugsupport.de benannt.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Einzelheiten in Anlage 1).

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

e) 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.

f) 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.

g) 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.

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

## **6. Unterauftragsverhältnisse**

(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.

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

## **7. Kontrollrechte des Auftraggebers**

(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.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

## **8. Mitteilung bei Verstößen des Auftragnehmers**

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen 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

d) Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen

e) f) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

## **9. Weisungsbefugnis des Auftraggebers**

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(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 solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert

wird.

## 10. Löschung und Rückgabe von personenbezogenen Daten

(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.

(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.

(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.

[Redacted]

Wiesbaden, den

[Redacted]

Name Auftraggeber



Till Heppner, bugsupport

[Redacted]

Unterschrift Auftraggeber

## Anlage:

### Technische und organisatorische Maßnahmen des Verantwortlichen nach Art. 32 DSGVO

Die bugsupport, Neugasse 15-19, 65183 Wiesbaden, DE setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt.

#### Datenschutz bei den Subunternehmern

Folgende Maßnahmen stellen sicher, dass sich die von der Verantwortlichen ausgewählten Subunternehmer datenschutzkonform verhalten:

- Abschluss von DSGVO-konformen Auftragsverarbeitungsverträgen mit dem Subunternehmer
- Auswahl der Subunternehmer unter Sorgfaltsgesichtspunkten (insb. hinsichtlich Datensicherheit) laufende und anlassbezogene Prüfung des Subunternehmers
- Sicherstellung der Vernichtung der Daten beim Subunternehmer nach Beendigung des Auftrags

#### Datensicherung und Backups (Verfügbarkeit und Wiederherstellbarkeit)

Folgende Maßnahmen stellen sicher, dass die vertragsgegenständlichen Daten jederzeit verfügbar sind:

- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Backup- & Wiederherstellungskonzept
- Feuer- und Rauchmeldeanlagen in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Klimatisierung der Serverräume
- Schutzsteckdosenleisten in Serverräumen
- Serverräume nicht unter sanitären Anlagen
- Sicherung der Serverräume
- Testen der Datenwiederherstellung

#### Protokollierung von Datenverarbeitungsprozessen (Eingabekontrolle)

Folgende Maßnahmen stellen sicher, dass die Verantwortliche jederzeit erkennen kann, welche Datenverarbeitungsprozesse in ihren Datenverarbeitungssystemen stattgefunden haben (z.B. Eingabe, Veränderung, Sperrung oder Löschung):

- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch

- individuelle Benutzernamen
- Protokollierung der Aktionen einzelner Nutzer
- Protokollierung von Eingaben, Änderungen und Löschungen (Log-Protokolle)
- Protokollierung von Zugriffen auf die IT-Systeme des Auftragsverarbeiter (Log-Protokolle)

## **Sichere Löschung von Daten**

Folgende Maßnahmen stellen die ordnungsgemäße Löschung der vertragsgegenständlichen Daten sicher:

- Beauftragung von spezialisierten Unternehmen für die Vernichtung von Akten und Datenträgern
- Einsatz von Aktenvernichtern (mindestens Stufe P-4)
- ordnungsgemäße Bereinigung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von ausgemusterten Datenträgern (DIN 66399)

## **Sicherung der Arbeitsstätte (Zutrittskontrolle)**

Die Arbeitsstätte wird in folgender Weise gegen Einbruch und sonstige unbefugte Zutritte gesichert:

- Chipkarten-/Transponder-Schließsystem
- Manuelles Schließsystem / Türschlösser
- Schließsystem mit Codesperre
- Schlüsselregelung (Protokollierung der Schlüsselausgabe)
- Sicherheitsschlösser
- Sorgfältige Auswahl von Reinigungspersonal
- Zutrittskonzept / Besucherregelung

## **Sicherung der IT-Systeme (Zugangskontrolle)**

Die IT-Systeme werden in folgender Weise gegen unbefugte Zugriffe (z.B. Hackerangriffe) gesichert:

- Anzahl der Systemadministratoren ist auf das „Notwendigste“ reduziert
- Einsatz einer Hardware-Firewall
- Einsatz von Anti-Viren-Software
- Einsatz von Intrusion-Detection-Systemen
- Erstellen von Benutzerprofilen in den IT-Systemen
- Festplattenverschlüsselung
- Login in die IT-Systeme mit individuellem Benutzernamen und Passwort
- Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
- Passwortvergabe
- regelmäßige und anlassbezogene Aktualisierung und Überprüfung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)
- Sichere Aufbewahrung von Datenträgern
- Verschlüsselung der Datensicherungssysteme
- Verschlüsselung externer Datenträger (externe Festplatten, USB-Sticks)

- etc.)
- Verschlüsselung mobiler Datenträger (Handys, Laptops etc.)
- Verwaltung der Berechtigungen durch Systemadministratoren
- Zugriffsregeln für Benutzer / Benutzergruppen in den IT-Systemen (Berechtigungskonzept)

### **Sicherung von Daten bei Transport und Übermittlung (Weitergabekontrolle)**

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) vor unbefugten Dritten geschützt werden:

- Verschlüsselung der sonstigen Kommunikationswege
- Verschlüsselung des E-Mail-Verkehrs
- Verschlüsselung physischer Datenträger beim Transport
- Einsatz von VPN-Tunneln

### **Sonstige Datenschutzmaßnahmen**

Folgende weitere Datenschutzmaßnahmen wurden implementiert:

- interne Verhaltensregeln
- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem