Beinhauer IT

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen

Kunde (Verantwortlicher, nachfolgend „Auftraggeber“): wie im Auftragsformular angegeben

und

Beinhauer IT, Inhaber David Beinhauer, August-Wegmann-Str. 63, 44532 Lünen (Auftragsverarbeiter, nachfolgend „Auftragnehmer“)

§ 1 Gegenstand und Dauer

1. Der Auftragnehmer erbringt für den Auftraggeber IT-Dienstleistungen gemäß Betreuungsvertrag bzw. Einzelauftrag (Hauptvertrag). Dabei kann der Auftragnehmer Zugriff auf personenbezogene Daten erhalten, für die der Auftraggeber Verantwortlicher ist. Gegenstand, Art und Zweck der Verarbeitung, Art der Daten und Kategorien betroffener Personen ergeben sich aus Anlage 1.
2. Dieser Vertrag gilt für die Dauer des Hauptvertrags und darüber hinaus, solange der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet.

§ 2 Weisungen

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist durch Unionsrecht oder deutsches Recht dazu verpflichtet; in diesem Fall teilt er dem Auftraggeber diese Verpflichtungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.
2. Weisungen erfolgen grundsätzlich in Textform (E-Mail, Ticket im Kundenportal). Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform. Weisungsberechtigt sind die im Auftragsformular benannten Ansprechpartner.
3. Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, weist er den Auftraggeber unverzüglich darauf hin. Er darf die Ausführung bis zur Bestätigung oder Änderung aussetzen.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.
2. Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO gemäß Anlage 2. Er darf sie weiterentwickeln, solange das Schutzniveau nicht unterschritten wird.
3. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Beantwortung von Anträgen betroffener Personen (Art. 12–22 DSGVO) sowie bei den Pflichten nach Art. 32–36 DSGVO.
4. Der Auftragnehmer informiert den Auftraggeber unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, über Verletzungen des Schutzes personenbezogener Daten und unterstützt ihn bei Meldung und Benachrichtigung.
5. Ein Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzlichen Voraussetzungen nicht vorliegen. Ansprechpartner für den Datenschutz ist David Beinhauer, info@beinhauer.it.
6. Die Verarbeitung erfolgt in der Europäischen Union bzw. im Europäischen Wirtschaftsraum. Eine Verarbeitung in einem Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 4 Unterauftragsverarbeiter

1. Der Auftraggeber genehmigt den Einsatz der in Anlage 3 genannten Unterauftragsverarbeiter.
2. Der Auftragnehmer informiert den Auftraggeber mindestens 4 Wochen vorher in Textform über die beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Auftraggeber kann aus

wichtigem datenschutzrechtlichem Grund innerhalb dieser Frist widersprechen. Können sich die Parteien nicht einigen, kann der Auftraggeber die betroffene Leistung zum Zeitpunkt des Wechsels kündigen.

3. Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich auf ein gleichwertiges Datenschutzniveau.

§ 5 Rechte und Pflichten des Auftraggebers

1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung verantwortlich.
2. Der Auftraggeber kann sich von der Einhaltung dieses Vertrags überzeugen, vorrangig durch Einsicht in aktuelle Nachweise (z. B. Zertifikate, Prüfberichte, Selbstauskunft). Kontrollen vor Ort erfolgen nach Anmeldung mit angemessener Frist, während der Servicezeiten und ohne Störung des Betriebsablaufs. Der Aufwand für Kontrollen vor Ort kann zum Paket-Stundensatz berechnet werden, soweit sie nicht aufgrund eines Verstoßes des Auftragnehmers erforderlich sind.

§ 6 Löschung und Rückgabe

Nach Ende der Leistungserbringung löscht der Auftragnehmer alle personenbezogenen Daten des Auftraggebers oder gibt sie nach Wahl des Auftraggebers zurück, soweit keine gesetzliche Aufbewahrungspflicht besteht. Sicherungsdaten werden 30 Tage nach Vertragsende gelöscht, sofern der Auftraggeber sie nicht vorher abruft. Die Löschung wird auf Anfrage bestätigt.

§ 7 Haftung und Schlussbestimmungen

1. Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags.
2. Bei Widersprüchen geht dieser Vertrag den Regelungen des Hauptvertrags zum Datenschutz vor.
3. Änderungen bedürfen der Textform. Im Übrigen gelten die Schlussbestimmungen der AGB.

Auftraggeber	Auftragnehmer
Ort, Datum:	Lünen,
Unterschrift:	Unterschrift:
Name:	David Beinhauer

Anlage 1 – Gegenstand der Verarbeitung

Art der Leistungen	Betreuung, Überwachung und Wartung von IT-Systemen; Fernwartung; Installation und Aktualisierung von Software; Datensicherung und Wiederherstellung; E-Mail-Schutz und -Archivierung; Sicherung von Microsoft 365; Betrieb des Kundenportals BIT World.
Zweck	Sicherstellung von Betrieb, Sicherheit und Verfügbarkeit der IT des Auftraggebers.
Art der Daten	Alle Daten, die auf den betreuten Systemen gespeichert sind oder dort verarbeitet werden, insbesondere Kontakt- und Kommunikationsdaten, Vertrags- und Abrechnungsdaten, E-Mail-Inhalte, Dokumente, Benutzer- und Zugangsdaten, Protokoll- und Gerätedaten; je nach Branche des Auftraggebers auch besondere Kategorien (z. B. Gesundheitsdaten bei Praxen und Hörakustik).

Betroffene Personen	Beschäftigte, Kunden, Patienten, Interessenten, Lieferanten und sonstige Kommunikationspartner des Auftraggebers.
Art der Verarbeitung	Einsehen, Speichern, Kopieren (Sicherung), Übermitteln, Wiederherstellen, Löschen im Rahmen der beauftragten Leistungen. Eine inhaltliche Auswertung findet nicht statt.

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit

- Zutritt: Büroräume verschlossen, Schlüsselregelung, Besucher nur in Begleitung.
- Zugang: persönliche Benutzerkonten, Multi-Faktor-Authentifizierung für Fernwartung, Überwachungsplattform, Kundenportal und Cloud-Dienste; Passwortrichtlinie; automatische Bildschirmsperre.
- Zugriff: Berechtigungen nach dem Erforderlichkeitsprinzip; Zugangsdaten der Kunden in einem verschlüsselten Passwort-Tresor; Protokollierung von Fernwartungssitzungen.
- Trennung: mandantengetrennte Verwaltung der Kunden in Überwachungs-, Sicherungs- und Portal-Systemen.
- Verschlüsselung: Transportverschlüsselung (TLS) für Fernwartung, Portal und Datensicherung; Datensicherungen verschlüsselt gespeichert; Festplattenverschlüsselung auf allen Geräten des Auftragnehmers.

Integrität

- Weitergabe: Übertragung nur verschlüsselt; keine Nutzung unverschlüsselter Wechseldatenträger für Kundendaten.
- Eingabekontrolle: Protokollierung administrativer Änderungen und Fernwartungssitzungen, Ticket-Dokumentation.

Verfügbarkeit und Belastbarkeit

- Sicherung eigener Systeme nach der 3-2-1-Regel; regelmäßige Wiederherstellungstests.
- Virenschutz und zeitnahes Einspielen von Sicherheitsupdates auf allen Systemen des Auftragnehmers.
- Rechenzentren der Unterauftragsverarbeiter mit Zertifizierung nach ISO 27001 bzw. gleichwertig.

Verfahren zur regelmäßigen Überprüfung

- Jährliche Überprüfung der Maßnahmen; Verpflichtung der Mitarbeiter auf Vertraulichkeit; Schulung zu Datenschutz und Informationssicherheit.
- Prozess für die Meldung von Datenschutzverletzungen.

Anlage 3 – Genehmigte Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Hosting von Webseite, Kundenportal BIT World, Software-Verteilung und eigenen Servern	Deutschland
Microsoft Ireland Operations Ltd., Dublin	Microsoft 365 (E-Mail, Terminbuchung, Dokumente), Mehrfaktor-Anmeldung, Verwaltung von Smartphones und Tablets (Microsoft Intune)	EU (EU-Datengrenze)

Unternehmen	Leistung	Ort der Verarbeitung
N-able (Vertragsgesellschaft gemäß N-able Data Processing Addendum)	Überwachung, Updates, Fernwartung (RMM), verwalteter Virenschutz, EDR, Web-Schutz, tägliche Online-Datensicherung und Sicherung Microsoft 365 (Cove Data Protection), E-Mail-Schutz und E-Mail-Archiv, Passwortmanager (Passportal)	Deutschland
Ubiquiti Inc., New York (USA)	Fernverwaltung und Überwachung von Firewall und Netzwerkgeräten (UniFi Site Manager) im Zusatzbaustein „Firewall & Netzwerk“; verarbeitet werden Geräte- und Verbindungsdaten (z. B. IP- und MAC-Adressen, Gerätenamen)	USA; Übermittlung auf Grundlage des EU-US Data Privacy Framework bzw. der EU-Standardvertragsklauseln
TeamViewer Germany GmbH, Göppingen	Fernwartung auf Anforderung	Deutschland
sipgate GmbH, Düsseldorf	Telefonie der Hotline, Weiterleitung an den KI-Telefon-Assistenten	Deutschland
OpenAI Ireland Ltd., Dublin	KI-Telefon-Assistent der Hotline (Sprachverarbeitung); Einordnung von Ticket-Texten für die Abrechnung	EU/USA; Übermittlung in die USA auf Grundlage des EU-US Data Privacy Framework bzw. der EU-Standardvertragsklauseln; keine Nutzung der Daten zum Training

Das Kundenportal BIT World einschließlich Software-Katalog und automatischer Software-Verteilung (u. a. FOG Project) betreibt der Auftragnehmer selbst auf eigenen Servern bei der Hetzner Online GmbH in Deutschland; hierfür werden keine weiteren Unterauftragsverarbeiter eingesetzt.