Burgnetz IT Solutions · Inh. Michael Stephan
Diebacher Straße 35b · 63549 Ronneburg
06048 5449983 · info@burgnetz-it.de

Vertrag über die Auftragsverarbeitung

gemäß Art. 28 DSGVO · mit Verpflichtung zur Verschwiegenheit nach § 203 StGB · Muster, Stand 11/2026

VERANTWORTLICHER (AUFTRAGGEBER)

Name / Praxis / Firma

Anschrift

AUFTRAGSVERARBEITER (AUFTRAGNEHMER)

Burgnetz IT Solutions
Inhaber: Michael Stephan
Diebacher Straße 35b, 63549 Ronneburg
USt-IdNr.: DE420565253

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer erbringt für den Auftraggeber IT-Dienstleistungen, insbesondere Einrichtung, Wartung, Fehlerbehebung und Betreuung von IT-Systemen, Netzwerken, Servern und Praxis-IT einschließlich der Anbindung an die Telematikinfrastruktur, vor Ort und per Fernwartung (Hauptvertrag bzw. Einzelaufträge).

(2) Dabei kann der Auftragnehmer Zugriff auf personenbezogene Daten erhalten, die der Auftraggeber verantwortet. Eine Verarbeitung dieser Daten ist nicht Ziel der Leistung, lässt sich aber nicht ausschließen. Dieser Vertrag regelt die datenschutzrechtlichen Pflichten der Parteien hierfür.

(3) Der Vertrag gilt, solange der Auftragnehmer für den Auftraggeber tätig ist. Er endet mit dem Ende der letzten Leistung, ohne dass es einer Kündigung bedarf. Pflichten zur Vertraulichkeit gelten darüber hinaus fort.

§ 2 Art und Zweck der Verarbeitung, Daten und Betroffene

Art der Verarbeitung	Einsicht, Zugriff, Speichern, Kopieren, Übertragen, Wiederherstellen und Löschen im Rahmen von Wartung, Support, Fernwartung, Datensicherung, Migration und Fehlerbehebung
Zweck	Sicherstellung des ordnungsgemäßen Betriebs der IT-Systeme des Auftraggebers
Arten von Daten	Stammdaten, Kontaktdaten, Kommunikationsdaten, Vertrags- und Abrechnungsdaten; bei Arztpraxen zusätzlich Gesundheitsdaten (Art. 9 DSGVO) wie Behandlungs-, Befund- und Abrechnungsdaten; Zugangs- und Protokolldaten
Betroffene Personen	Patienten, Kunden, Interessenten, Beschäftigte, Lieferanten und sonstige Kontaktpersonen des Auftraggebers
Ort der Verarbeitung	Räume des Auftraggebers, Räume des Auftragnehmers in Deutschland sowie per verschlüsselter Fernwartung. Eine Verarbeitung außerhalb der EU/des EWR findet nicht statt.

§ 3 Weisungen des Auftraggebers

1. Der Auftragnehmer verarbeitet Daten nur auf dokumentierte Weisung des Auftraggebers. Weisungen erfolgen in der Regel durch die Beauftragung selbst, per E-Mail, Ticket oder telefonisch; telefonische Weisungen bestätigt der Auftragnehmer auf Wunsch in Textform.
2. Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen Datenschutzrecht verstößt, weist er den Auftraggeber unverzüglich darauf hin.
3. Daten werden nicht für eigene Zwecke des Auftragnehmers genutzt. Kopien werden nur erstellt, soweit dies für die Leistung zwingend erforderlich ist (z. B. Datensicherung, Migration), und danach gelöscht.

§ 4 Vertraulichkeit und Verschwiegenheit (§ 203 StGB)

1. Der Auftragnehmer setzt nur Personen ein, die schriftlich zur Vertraulichkeit verpflichtet wurden und mit den Anforderungen des Datenschutzes vertraut sind.
2. Ist der Auftraggeber Berufsgeheimnisträger (z. B. Arzt), ist dem Auftragnehmer bekannt, dass er als mitwirkende Person im Sinne von § 203 Abs. 3 und 4 StGB tätig wird. Er verpflichtet sich und alle eingesetzten Personen zur Geheimhaltung der ihm bekannt werdenden fremden Geheimnisse und kennt die strafrechtlichen Folgen einer Verletzung. Er verschafft sich Kenntnis von solchen Geheimnissen nur, soweit es für die Leistung erforderlich ist.

§ 5 Sicherheit der Verarbeitung

Der Auftragnehmer trifft die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Er darf sie an den technischen Fortschritt anpassen, sofern das Schutzniveau nicht sinkt.

§ 6 Fernwartung

1. Fernwartung erfolgt nur nach Freigabe durch den Auftraggeber im Einzelfall oder nach einer schriftlich vereinbarten Regelung für dauerhafte Zugänge.
2. Es werden ausschließlich verschlüsselte Verbindungen genutzt, insbesondere die vom Auftraggeber bereitgestellten oder mit ihm abgestimmten Werkzeuge (z. B. TeamViewer, AnyDesk, RDP über VPN).
3. Der Auftraggeber kann jede Sitzung am Bildschirm verfolgen und jederzeit beenden. Der Auftragnehmer beendet Sitzungen nach Abschluss der Arbeiten.

§ 7 Unterauftragsverhältnisse

1. Der Auftraggeber stimmt den in **Anlage 2** genannten Unterauftragnehmern zu.
2. Über neue oder geänderte Unterauftragnehmer informiert der Auftragnehmer vorab in Textform. Der Auftraggeber kann innerhalb von 14 Tagen aus wichtigem datenschutzrechtlichem Grund widersprechen.
3. Der Auftragnehmer verpflichtet Unterauftragnehmer vertraglich auf ein gleichwertiges Datenschutzniveau.

§ 8 Unterstützungspflichten

1. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei Anfragen betroffener Personen (Art. 12–22 DSGVO) und bei den Pflichten aus Art. 32–36 DSGVO. Anfragen, die direkt beim Auftragnehmer eingehen, leitet er unverzüglich weiter.
2. Verletzungen des Schutzes personenbezogener Daten, die der Auftragnehmer bemerkt, meldet er dem Auftraggeber unverzüglich, möglichst innerhalb von 24 Stunden, mit den ihm bekannten Informationen.

§ 9 Kontrollrechte

Der Auftraggeber kann sich nach Absprache und mit angemessener Vorankündigung von der Einhaltung dieses Vertrags überzeugen. Der Auftragnehmer stellt die dafür nötigen Informationen bereit. Die Prüfung soll den Geschäftsbetrieb nicht unverhältnismäßig stören.

§ 10 Löschung und Rückgabe

Nach Abschluss der Leistungen löscht der Auftragnehmer alle Daten des Auftraggebers, die sich noch bei ihm befinden, oder gibt sie nach Wahl des Auftraggebers zurück, soweit keine gesetzliche Pflicht zur Aufbewahrung besteht. Datenträger werden sicher vernichtet. Die Löschung bestätigt er auf Wunsch in Textform.

§ 11 Haftung und Schlussbestimmungen

1. Für die Haftung gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregeln des Hauptvertrags.
2. Änderungen und Ergänzungen bedürfen der Textform. Bei Widersprüchen geht dieser Vertrag dem Hauptvertrag in Fragen des Datenschutzes vor.
3. Sollte eine Bestimmung unwirksam sein, bleibt der übrige Vertrag wirksam. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragnehmers.

Ort, Datum · Unterschrift / Stempel Auftraggeber	Ronneburg, Datum · Michael Stephan, Burgnetz IT Solutions

Technische und organisatorische Maßnahmen

nach Art. 32 DSGVO

1. Vertraulichkeit

- **Zutritt:** Büro- und Lagerräume sind verschlossen; Besucher haben keinen unbegleiteten Zutritt.
- **Zugang:** Arbeitsgeräte sind mit individuellen, starken Passwörtern geschützt und sperren sich bei Inaktivität automatisch. Wo möglich, ist eine Zwei-Faktor-Anmeldung aktiv.
- **Zugangsdaten von Kunden** werden ausschließlich in einem verschlüsselten Passwortmanager gespeichert, nie auf Papier oder in unverschlüsselten Dateien.
- **Zugriff:** Mitarbeiter erhalten nur die Rechte, die sie für ihre Aufgabe brauchen.
- **Verschlüsselung:** Datenträger von Notebooks und mobilen Geräten des Auftragnehmers sind verschlüsselt.

2. Integrität

- **Übertragung:** Fernwartung nur über verschlüsselte Verbindungen (TeamViewer/AnyDesk mit Ende-zu-Ende-Verschlüsselung, RDP nur über VPN oder vergleichbar abgesichert, nicht offen im Internet).
- **Freigabe:** Jede Fernwartungssitzung erfolgt nach Freigabe durch den Auftraggeber; dauerhafte unbeaufsichtigte Zugänge nur nach schriftlicher Vereinbarung.
- **Dokumentation:** Durchgeführte Arbeiten werden je Auftrag dokumentiert (Datum, Person, Tätigkeit).
- **Datentransport:** Werden Daten auf Datenträgern transportiert, sind diese verschlüsselt.

3. Verfügbarkeit und Belastbarkeit

- Eigene Systeme werden regelmäßig aktualisiert und mit aktuellem Virenschutz betrieben.
- Vor Eingriffen mit Risiko für Datenverlust (z. B. Migration, Update) wird eine Sicherung erstellt oder deren Vorhandensein geprüft.

4. Verfahren zur Überprüfung und Organisation

- Alle Mitarbeiter sind schriftlich auf Vertraulichkeit, Datenschutz und – bei Arztpraxen – auf § 203 StGB verpflichtet und werden regelmäßig sensibilisiert.
- Datenträger mit Kundendaten werden nach Ende der Nutzung sicher gelöscht bzw. nach DIN 66399 vernichtet.
- Die Maßnahmen werden mindestens jährlich überprüft und angepasst.
- Ansprechpartner Datenschutz: Michael Stephan, info@burgnetz-it.de, 06048 5449983.

Unterauftragnehmer

nach § 7 dieses Vertrags

Unterauftragnehmer	Leistung	Ort
ALL-INKL.COM – Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf	E-Mail-Postfach und Website des Auftragnehmers (Eingang von Anfragen und Tickets)	Deutschland
TeamViewer Germany GmbH, Bahnhofsplatz 2, 73033 Göppingen	Fernwartungssoftware (Verbindungsaufbau), nur sofern genutzt	EU
AnyDesk Software GmbH, Türlenstraße 2, 70191 Stuttgart	Fernwartungssoftware (Verbindungsaufbau), nur sofern genutzt	EU

Stellt der Auftraggeber selbst ein Fernwartungswerkzeug bereit (eigene Lizenz), ist dessen Anbieter Dienstleister des Auftraggebers und nicht Unterauftragnehmer des Auftragnehmers.

Muster. Dieses Dokument ersetzt keine Rechtsberatung. Stand: November 2026 · Burgnetz IT Solutions · burgnetz-it.de