

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Stand: 3. September 2026

Dieser Vertrag regelt die Verarbeitung personenbezogener Daten, die der Anbieter beim Betrieb von Saniakte für den Kunden vornimmt. Er ist vor der ersten Verarbeitung abzuschließen und Bestandteil des Hauptvertrages.

Vertragsparteien

Verantwortlicher (Auftraggeber)

Angabe	Wert
Organisation	
Anschrift	
Vertreten durch	
E-Mail	
Datenschutzbeauftragter, falls benannt	

Auftragsverarbeiter (Auftragnehmer)

Angabe	Wert
Name	Lucas Paulick
Anschrift	Friedensallee 1, 16556 Borgsdorf
E-Mail	kontakt@saniakte.de
Telefon	015253780358

§ 1 Gegenstand und Dauer

(1) Gegenstand ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer beim Einrichten, Betreiben, Warten und Sichern der Installation der Anwendung Saniakte, die der Auftraggeber zur Dokumentation von Hilfeleistungen nutzt.

(2) Der Auftragnehmer verarbeitet die Daten ausschließlich im Auftrag und nach dokumentierter Weisung des Auftraggebers.

(3) Der Vertrag beginnt mit der Bereitstellung der Installation und läuft, solange der Hauptvertrag besteht. Er endet mit dessen Ende.

§ 2 Art, Umfang und Zweck der Verarbeitung

(1) **Art der Verarbeitung:** Erheben, Speichern, Ordnen, Auslesen, Verändern, Übermitteln an den Auftraggeber, Sichern, Einschränken und Löschen – jeweils im Rahmen des technischen Betriebs.

(2) **Zweck:** Bereitstellung und technischer Betrieb der Anwendung Saniakte für den Auftraggeber.

(3) **Betroffene Personen:**

- Personen, denen der Auftraggeber Hilfe leistet (Patientinnen und Patienten),
- Helferinnen und Helfer sowie sonstige Nutzerinnen und Nutzer des Auftraggebers,
- Ansprechpersonen bei Veranstaltern und Dritten, soweit im Einsatz erfasst.

(4) **Arten der Daten:**

- Stammdaten der betroffenen Person: Name, Geburtsdatum, Anschrift, Erreichbarkeit,
- **Gesundheitsdaten nach Art. 9 Absatz 1 DSGVO:** Beschwerdebild, Vorerkrankungen, Medikamente, Allergien, Messwerte, durchgeführte Maßnahmen, Verlauf, Übergabe,
- Einsatzdaten: Zeitpunkte, Einsatzort, beteiligte Kräfte, Dienst,
- Unterschriften als Bilddatei,
- Konto- und Anmeldedaten der Nutzerinnen und Nutzer des Auftraggebers,
- Protokolldaten des Servers nach § 8.

(5) Der Auftragnehmer greift auf Inhaltsdaten nur zu, wenn und soweit es für die Störungsbeseitigung erforderlich ist und der Auftraggeber dies im Einzelfall verlangt oder dem zugestimmt hat. Jeder solche Zugriff wird dem Auftraggeber auf Anforderung mitgeteilt.

§ 3 Weisungen

(1) Weisungen erteilt der Auftraggeber in Textform. Mündliche Weisungen bestätigt er unverzüglich in Textform.

(2) Weisungsberechtigt sind die vom Auftraggeber benannten Personen. Änderungen teilt er in Textform mit.

(3) Hält der Auftragnehmer eine Weisung für rechtswidrig, teilt er dies unverzüglich mit. Er darf die Ausführung aussetzen, bis der Auftraggeber sie bestätigt oder ändert.

§ 4 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die in der **Anlage 1** beschriebenen Maßnahmen nach Art. 32 DSGVO und hält sie während der Vertragslaufzeit aufrecht.

(2) Er darf die Maßnahmen fortentwickeln, solange das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen teilt er in Textform mit.

§ 5 Vertraulichkeit

(1) Der Auftragnehmer setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet und mit den einschlägigen Vorgaben des Datenschutzes vertraut sind. Die Verpflichtung wirkt über das Ende der Tätigkeit hinaus.

(2) Der Auftragnehmer beachtet, dass die verarbeiteten Gesundheitsdaten der Schweigepflicht unterliegen können, und behandelt sie entsprechend.

§ 6 Unterauftragsverhältnisse

(1) Der Auftraggeber stimmt der Beauftragung folgender Unterauftragnehmer zu:

Unterauftragnehmer	Leistung	Ort der Verarbeitung
OVH SAS, 2 rue Kellermann, 59100 Roubaix, Frankreich	Bereitstellung des Servers, Rechen-, Speicher- und Netzkapazität, Rechenzentrumsbetrieb	Frankfurt am Main, Deutschland

(2) Weitere Unterauftragnehmer darf der Auftragnehmer nur nach vorheriger Mitteilung in Textform einsetzen. Der Auftraggeber kann binnen 14 Tagen aus wichtigem Grund widersprechen. Widerspricht er, darf jede Seite den Vertrag mit einer Frist von einem Monat kündigen.

(3) Der Auftragnehmer verpflichtet Unterauftragnehmer schriftlich auf Pflichten, die diesem Vertrag entsprechen, und prüft ihre Eignung vor der Beauftragung.

(4) Eine Verarbeitung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums findet nicht statt.

(5) Nicht als Unterauftragsverhältnis gelten Nebenleistungen wie Telekommunikation, Post oder Wartung von Endgeräten des Auftragnehmers.

§ 7 Unterstützung des Auftraggebers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Beantwortung von Anträgen betroffener Personen nach Kapitel III der DSGVO. Wendet sich eine betroffene Person unmittelbar an ihn, leitet er die Anfrage unverzüglich weiter und antwortet nicht selbst.

(2) Die Anwendung erzeugt für Betroffenenanfragen ein Auskunftspaket: alle gespeicherten Felder in maschinenlesbarer Form, gebündelt mit dem Protokoll-PDF. Der Auftraggeber kann es selbst abrufen.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Art. 32 bis 36 DSGVO, insbesondere bei der Meldung von Verletzungen des Schutzes personenbezogener Daten und bei einer Datenschutz-Folgenabschätzung.

(4) Wird dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt, meldet er sie dem Auftraggeber **unverzüglich, spätestens innerhalb von 24 Stunden** nach Kenntnis, mit allen ihm vorliegenden Angaben nach Art. 33 Absatz 3 DSGVO.

§ 8 Protokollierung

(1) Auf Serverebene fallen Protokolldaten an (Zeitpunkt, IP-Adresse, aufgerufene Adresse, Statuscode, Browserkennung). Sie dienen dem Betrieb und der Abwehr von Angriffen und werden nach spätestens 14 Tagen gelöscht.

(2) Innerhalb der Anwendung wird festgehalten, welches Konto einen Datensatz angelegt oder geändert hat. Diese Angaben gehören zum Datenbestand des Auftraggebers und unterliegen dessen Löschfristen.

§ 9 Kontrollrechte

(1) Der Auftraggeber darf sich von der Einhaltung dieses Vertrages überzeugen. Der Auftragnehmer erteilt dazu Auskunft und stellt die Nachweise nach Art. 28 Absatz 3 Buchstabe h DSGVO zur Verfügung.

(2) Vor-Ort-Kontrollen sind nach Ankündigung mit angemessener Frist, in der Regel zwei Wochen, während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs zulässig. Der Auftragnehmer darf sie von einer Verschwiegenheitsverpflichtung abhängig machen.

(3) Für Kontrollen, die über eine jährliche hinausgehen und nicht durch einen konkreten Anlass veranlasst sind, darf der Auftragnehmer den Aufwand nach Zeit berechnen.

§ 10 Löschung und Rückgabe

(1) Nach Ende des Vertrages stellt der Auftragnehmer die Daten auf Anforderung binnen 14 Tagen in einem gängigen Format bereit.

(2) 30 Tage nach Vertragsende löscht er die Installation samt aller Daten und Sicherungen, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Die Löschung bestätigt er auf Wunsch in Textform.

(3) Der Auftraggeber ist dafür verantwortlich, die Daten vor Ablauf dieser Frist zu sichern.

§ 11 Haftung

(1) Für die Haftung im Verhältnis der Parteien gilt Art. 82 DSGVO.

(2) Die Haftungsregelung des Hauptvertrages bleibt im Übrigen unberührt, soweit sie nicht die Ansprüche betroffener Personen betrifft.

§ 12 Schlussbestimmungen

(1) Änderungen bedürfen der Textform.

(2) Widersprechen sich dieser Vertrag und der Hauptvertrag in Fragen der Verarbeitung personenbezogener Daten, geht dieser Vertrag vor.

(3) Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam.

Anlage 1: Technische und organisatorische Maßnahmen

Vertraulichkeit

- **Zugang zur Anwendung** nur nach Anmeldung mit Konto und Passwort. Passwörter werden nicht im Klartext gespeichert, sondern mit einem für diesen Zweck bestimmten Verfahren abgelegt. Ein zweiter Faktor nach dem Zeitverfahren steht bereit und kann für einzelne Konten oder die ganze Organisation verpflichtend gemacht werden. Nach mehreren Fehlversuchen wird das Konto vorübergehend gesperrt.
- **Zugriff innerhalb der Anwendung** über Rollen und Rechte. Jede Abfrage prüft serverseitig, ob das Konto den Datensatz sehen oder ändern darf; die Prüfung liegt an einer Stelle und gilt für Anzeige, Ausgabe und PDF gleichermaßen. Konten mit eingeschränkter Sicht erhalten nur die Hilfeleistungen ihrer eigenen Dienste.
- **Sitzungen** laufen über signierte Sitzungsmerkmale mit begrenzter Gültigkeit. Ein Wechsel des Passworts entwertet bestehende Sitzungen.
- **Trennung** der Kunden auf Ebene der Installation: eigene Anwendung, eigene Datenbank, eigene Anmeldung. Eine gemeinsame Datenhaltung mehrerer Kunden gibt es nicht.
- **Verwaltungszugang zum Server** ausschließlich über einen verschlüsselten Kanal mit Schlüsselverfahren.

Integrität

- **Übertragung** ausschließlich verschlüsselt über TLS; unverschlüsselte Aufrufe werden umgeleitet. Die Anwendung fordert den verschlüsselten Aufruf über HSTS an.
- **Eingaben** werden serverseitig geprüft und typisiert. Datenbankzugriffe erfolgen ausschließlich über eine Abfrageschicht mit gebundenen Werten; zusammengesetzte Abfragen aus Nutzereingaben gibt es nicht.
- **Änderungen** an Einsätzen werden mit Konto und Zeitpunkt festgehalten.
- **Ausgaben in Dateien** werden gegen die Ausführung von Formeln im Tabellenprogramm entschärft.

Verfügbarkeit und Belastbarkeit

- Tägliche Sicherung der Datenbank, 30 Tage Vorhaltezeit.
- Betrieb in einem Rechenzentrum in Deutschland mit unterbrechungsfreier Stromversorgung, redundanter Anbindung und Zutrittskontrolle durch den Betreiber.
- Aktualisierungen von Betriebssystem und Anwendung werden zeitnah eingespielt; sicherheitsrelevante sofort.
- Die Anwendung arbeitet bei Verbindungsabbruch auf dem Gerät weiter und reicht Eingaben nach, sobald die Verbindung zurück ist.

Löschung und Speicherbegrenzung

- Einsätze werden nach Ablauf der eingestellten Frist – voreingestellt zehn Jahre – durch einen täglich laufenden Vorgang hart gelöscht, samt PDF, Unterschriften und Freigabelinks. Erhalten bleibt eine Zählzeile je Monat ohne Namen und ohne Kennungen.
- Serverprotokolle werden nach spätestens 14 Tagen gelöscht.

Nachvollziehbarkeit

- Der Programmstand jeder Installation ist über die Versionsverwaltung nachvollziehbar; ausgerollt wird nur, was dort festgehalten ist.
 - Änderungen an den Maßnahmen werden dokumentiert.
-

Unterschriften

Verantwortlicher

Ort, Datum

Unterschrift

Name in Druckbuchstaben

Auftragsverarbeiter

Ort, Datum

Unterschrift

Name in Druckbuchstaben