Stänz Informatik AG
Tösstalstrasse 14 | 8360 Wallenwil
071 971 24 74 | support@sin.ch

Vereinbarung zur Auftragsbearbeitung (AVV) für Berufsgeheimnisträger

gemäss nDSG (Schweiz) und unter Berücksichtigung von Art. 321 StGB

zwischen der
Stänz Informatik AG, Tösstalstrasse 14, 8360 Wallenwil
(nachfolgend «Auftragnehmer»)

und dem Kunden (nachfolgend «Auftraggeber»)

1. Gegenstand und Geltungsbereich

1. Diese Vereinbarung regelt die datenschutzrechtlichen Verpflichtungen der Parteien im Rahmen von IT-Dienstleistungen (Support, Fernwartung, Netzwerk, Cloud-Services).
2. Der Anbieter wird als Hilfsperson des Kunden im Sinne von Art. 321 StGB tätig. Diese Vereinbarung gilt für alle Tätigkeiten, bei denen der Anbieter mit besonders schützenswerten Personendaten (Gesundheitsdaten) in Berührung kommen kann.

2. Verantwortlichkeiten und Risikoabgrenzung (Stänz-Schutz)

1. Der Kunde ist als Verantwortlicher allein für die Rechtmässigkeit der Datenbearbeitung sowie für die Einholung notwendiger Patienteneinwilligungen verantwortlich.
2. Der Kunde trägt die alleinige Verantwortung für die Integrität und Sicherung (Backup) der Daten. Der Anbieter übernimmt keine Haftung für Datenverluste, die auf unzureichende oder fehlende kundenseitige Backup-Konzepte zurückzuführen sind.

3. Wahrung des Berufsgeheimnisses (Art. 321 StGB)

1. Der Anbieter verpflichtet sich zur Wahrung des Berufsgeheimnisses. Er stellt sicher, dass alle eingesetzten Mitarbeiter schriftlich über die strafrechtlichen Folgen einer Verletzung des Patientengeheimnisses belehrt und zur absoluten Verschwiegenheit (auch über das Ende des Arbeitsverhältnisses hinaus) verpflichtet wurden.
2. Der Anbieter verschafft sich nur insoweit Kenntnis von Patientendaten, als dies zur Erfüllung der technischen Aufgaben zwingend erforderlich ist.

4. Unterauftragsverhältnisse (Administrative Entlastung)

4.1 Der Kunde erteilt die allgemeine Genehmigung zum Beizug spezialisierter Drittanbieter (z. B. AnyDesk, Microsoft, ALSO, Hostpoint).
4.2 Der Anbieter informiert über Änderungen (z. B. via E-Mail oder Website). Widerspricht der Kunde nicht innerhalb von 14 Tagen, gilt die Änderung als genehmigt. Ein Widerspruch des Kunden berechtigt den Anbieter zur Einstellung der entsprechenden Leistung ohne Rückerstattungspflicht.

5. Unterstützungspflichten und Vergütung
5.1 Der Anbieter unterstützt den Kunden bei Auskunftsbegehren oder Datenschutz-Folgenabschätzungen.
5.2 Da diese Leistungen nicht Teil der IT-Grundversorgung sind, werden sie als kostenpflichtige Zusatzleistungen nach tatsächlichem Aufwand (gemäss aktueller Stundensatzliste des Anbieters) verrechnet.

6. Kontrollrechte und Audits (Schutz vor Zeitverlust)
6.1 Der Kunde kann die Einhaltung der Massnahmen maximal einmal jährlich prüfen. Audits sind mind. 10 Arbeitstage im Voraus anzumelden.
6.2 Der Kunde trägt die vollständigen Kosten des Audits sowie den beim Anbieter anfallenden personellen Aufwand, sofern keine schwerwiegenden Sicherheitsmängel festgestellt werden.

7. Fernwartung (Protokollierung)
7.1 Fernzugriffe (z. B. via AnyDesk) erfolgen ausschliesslich nach Freigabe durch den Kunden.
7.2 Der Anbieter protokolliert die Zugriffe innerhalb der Support-Systeme. Der Kunde ist dafür verantwortlich, dass während der Sitzung keine unbefugten Dritten in der Praxis Einblick in den Monitor haben.

8. Haftungsbeschränkung
Die Haftung des Anbieters ist auf Schäden beschränkt, die nachweislich durch grobe Fahrlässigkeit oder Vorsatz des Anbieters verursacht wurden. Jegliche Haftung für indirekte Schäden, Folgeschäden (z.B. Praxisstillstand) oder entgangenen Gewinn ist ausgeschlossen.

9. Schlussbestimmungen und Gerichtsstand
9.1 Es gilt ausschliesslich Schweizer Recht.
9.2 Ausschliesslicher Gerichtsstand für alle Streitigkeiten ist der Sitz des Anbieters (8360 Wallenwil).

Anhang 1: Technische und organisatorische Massnahmen (TOM)

Die Stänz Informatik AG garantiert für Medizinalkunden folgende Sicherheitsstandards:
1. Vertraulichkeit (Schutz vor unbefugter Einsicht)
- Zutritt: Geschäftsräume in Wallenwil sind durch mechanische Schliesssysteme gesichert; kein unbefugter Zutritt während Fernwartungssitzungen.
- Zugang: Personenbezogene Logins, strikte Passwort-Richtlinien und Multi-Faktor-Authentifizierung (MFA) für Support-Infrastruktur.
- Zugriff: Berechtigungsvergabe nach dem Minimalprinzip („Need-to-know“).

2. Integrität (Schutz vor Datenmanipulation)
    - Verschlüsselung: Fernwartungsverbindungen sind nach TLS 1.2 / AES-256 Standard verschlüsselt.
    - Datentransport: Nutzung von gesicherten Kanälen (VPN/HTTPS) für jeglichen Datenaustausch.
3. Verfügbarkeit und Nachvollziehbarkeit
    - Systemschutz: Einsatz von Endpoint Protection (Antivirus/Firewall) auf allen Support-Geräten.
    - Patching: Zeitnahes Einspielen von Sicherheitsupdates auf allen Systemen des Anbieters.
    - Logging: Nachvollziehbarkeit von Support-Sitzungen durch systemseitige Protokollierung.
4. Datenschutz-Management
    - Schriftliche Verpflichtung aller Techniker auf das Berufsgeheimnis (Art. 321 StGB).
    - Prozess zur Meldung von Sicherheitsvorfällen (Data Breaches) innerhalb von 72 Stunden an den Kunden.

Was du jetzt tun solltest:

1. Layout: Kopiere diesen Text in ein separates Dokument ("AVV für Medizinalberufe").
2. Unterschrift: Im Gegensatz zum Standard-KMU-Vertrag solltest du diesen von Ärzten unterschreiben lassen. Das gibt dem Arzt die notwendige Sicherheit für seine Dokumentationspflicht (FMH-Konformität).
3. Interner Check: Stelle sicher, dass du für jeden Mitarbeiter eine unterschriebene Erklärung zur Wahrung des Berufsgeheimnisses in den Personalakten hast.