smartprax

Auftragsverarbeitungsvertrag (AVV)

I. Parteien

- Auftraggeber: Nutzer der Software für Psychotherapie und Psychiatrie «smartprax»
- Auftragnehmer: smartcode Rico Leuthold, Hauptstrasse 31, 7247 Saas im Prättigau

II. Geltungsbereich, gesetzliche Grundlage

1. Der Auftragsverarbeitungsvertrag regelt die Bearbeitung von Personendaten durch den Auftragnehmer und die involvierten Subunternehmen.
2. Die Bearbeitung von Personendaten erfolgt primär nach dem schweizerischen Datenschutzgesetz (DSG) und der Verordnung über den Datenschutz (DSV).

III. Art und Dauer der Bearbeitung

1. Die Datenbearbeitung bezieht sich auf erstellen, bearbeiten, speichern & löschen von Personendaten.
2. Die Dauer für die Bearbeitung von Personendaten ergibt sich aus der Verwendung der Applikation «smartprax» und erlischt mit der Kündigung des Abonnementes.

IV. Bearbeitung von Personendaten

1. Die Bearbeitung betrifft die Daten von folgenden Personengruppen des Auftraggebers: Klienten und deren Akteure, sowie die der Auftraggeber.

2. Folgende Datenkategorien werden durch den Auftragnehmer bearbeitet: Personenstammdaten inklusive Daten zur Krankenversicherung oder beruflichen Angaben wie GLN oder ZSR Nummern, Verhaltensdaten, Bilder.

V. Pflichten des Auftragnehmers

1. Der Auftragnehmer darf die Daten nur nach dokumentierter Weisung des Auftraggebers für die genannten Zwecke bearbeiten. Vermutet der Auftragnehmer eine unzulässige Datenbearbeitung, teilt er dies dem Auftraggeber mit.
2. Der Auftragnehmer stellt die Geheimhaltung bei allen Mitarbeitenden und Hilfspersonen sicher, soweit dies nicht schon von Gesetzes wegen gegeben ist.
3. Der Auftragnehmer exportiert keine Personendaten (z. B. zusätzliche Speicherung, Weitergabe an Dritte), ohne die Erlaubnis des Auftraggebers. Wenn diese vorliegt, muss das geltende Datenschutzrecht eingehalten werden.
4. Der Auftragnehmer unterstützt den Auftraggeber bei Anfragen von betroffenen Personen und insgesamt bei der Einhaltung des Datenschutzrechts, soweit es dem Auftragnehmer möglich ist.
5. Nach Beendigung der Auftragsverarbeitung gibt der Auftragnehmer sämtliche Daten zurück und/oder löscht sie, soweit dies gesetzlich erlaubt ist.
6. Der Auftragnehmer kann nachweisen, dass er den Auftragsverarbeitungsvertrag einhält, der Auftraggeber kann dies umfassend prüfen.
7. Der Auftragnehmer sorgt stets dafür, eine angemessene Datensicherheit einzuhalten, die dem geltenden Datenschutzrecht entspricht. Die technischen und organisatorischen Massnahmen (TOM) sind diesem Auftragsverarbeitungsvertrag als Anhang beigefügt.
8. Der Auftragnehmer darf Subunternehmen nur mit Genehmigung des Auftraggebers einsetzen. Unter VI. werden die aktuellen Subunternehmen aufgeführt. Werden später weitere hinzugezogen, informiert der Auftragnehmer den Auftraggeber darüber. Ohne Widerspruch innert 30 Tagen gelten sie als genehmigt. Die Subunternehmen müssen das geltende Datenschutzrecht einhalten und werden wie der Auftragnehmer vertraglich verpflichtet.

VI. Subunternehmen

1. Mit folgenden Subunternehmen wurden Auftragsverarbeitungsverträge abgeschlossen und gegebenenfalls mit Standardvertragsklauseln abgesichert:

   - Medidoc AG, Bösch 69, 6331 Hünenberg CH, Verrechnung, Abfrage Klienten- & Ärztedaten
   - Hetzner Online GmbH, Gunzenhausen, Hosting

2. Mit Inkrafttreten der AGB gelten die oben genannten Subunternehmen als genehmigt.
3. Später hinzugefügte Subunternehmen können auf einer separaten Liste diesem Auftragsverarbeitungsvertrag hinzugefügt werden.

Anhang:

Technische und organisatorische Massnahmen (TOM)

smartprax

Technische und organisatorische Massnahmen (TOM)

Dieser Anhang beschreibt die technischen und organisatorischen Massnahmen, die der Auftragnehmer zur Gewährleistung der Sicherheit der Datenverarbeitung implementiert hat. Diese Massnahmen dienen dazu, die Vertraulichkeit, Integrität und Verfügbarkeit der Daten im Einklang mit dem Datenschutzgesetz der Schweiz zu schützen.

1. Zugriffskontrolle
   - Benutzername/Passwort-Authentifizierung oder Passkey
   - Zwei-Faktor-Authentifizierung (2FA)
   - Verwaltung von Zugriffsrechten und Rollen
   - Regelmässige Kontrolle von Berechtigungen
2. Weitergabekontrolle
   - Verschlüsselung von Daten bei der Übertragung über öffentliche Netzwerke
   - Sichere Kommunikationsprotokolle (wie TLS)
3. Verfügbarkeitskontrolle
   - Regelmässige Backups und Tests der Wiederherstellungsmechanismen
4. Aufbewahrungskontrolle
   - Richtlinien zur Datenminimierung und Löschung
   - Kontrolle von Zugängen zu Archiven und Datenspeichern
5. Trennungskontrolle
   - Trennung produktiver und nicht produktiver Systeme
   - Einsatz von Virtualisierungstechnologien
6. Organisatorische Massnahmen
   - Implementierung von Datenschutzvorgaben

7. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

- Verschlüsselung der Daten und Backups
- Einsatz von Pseudonymisierungstechniken
- Datenschutzfreundliche Grundeinstellungen in IT-Systemen
- Datenschutz durch Design bei der Entwicklung neuer Produkte

8. Weitere Massnahmen

- Regelmässige Überprüfung und Aktualisierung Softwarekomponenten