321MED

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN ZUM DATENSCHUTZ UND DATENSICHERHEIT

Auftraggeber:	Auftragnehmer:
_____ Vorname _____ Nachname _____ Straße _____ PLZ/Ort _____ Telefon _____ E-Mail	**321 MED GmbH** Am heimlichen Grund 5 92421 Schwandorf

1. GESPEICHERTE UND VERARBEITETE DATEN

321 MED speichert und verarbeitet öffentliche, aber auch personenbezogene/besondere Kategorien personenbezogener Daten und somit mitunter schützenswerte Daten. Insbesondere besondere Kategorien personenbezogener Daten (z.B. Gesundheitsdaten) unterliegen einer besonderen Schutzbedürftigkeit und bedürfen eines angemessenen Sicherheitsniveaus, um deren Sicherheit im Rahmen des Möglichen zu gewährleisten und nur befugten Zugriff sicherzustellen.

Bei der Bewertung des angemessenen Sicherheitsniveaus sowie verhältnismäßiger Maßnahmen werden im Rahmen einer Risikoanalyse und Risikobewertung regelmäßig alle relevanten Risiken berücksichtigt, die sich nachfolgenden Ausführungen ergeben.

321 MED setzt im Rahmen des Möglichen geeignete technische und organisatorische Maßnahmen um, um die Sicherheit aller (personenbezogenen) Daten in Übereinstimmung mit der DSGVO zu gewährleisten.

Trotz Analyse und Bewertung aller Risikoszenarien und Umsetzung angemessener Maßnahmen kann eine 100%-ige Sicherheit nie garantiert werden – es existiert immer ein gewisses Restrisiko (z.B. durch technische Limitationen), dem nur schwer zu begegnen ist. Insbesondere auch nutzerbedingte Risiken (z.B. Weitergabe von Daten durch Berechtigte) können nur bedingt kontrolliert und somit nicht vollständig verhindert werden.

Die Anwendungen der 321 MED GmbH werden im Rechenzentrum der Strato AG (Hoster) gehostet, welche für den reibungslosen, störungsfreien Betrieb, sowie die physische Sicherheit Sorge trägt. Das Rechenzentrum ist nach dem international anerkannten Standard für Informationssicherheit DIN 27001 zertifiziert.
Die Strato AG stellt sicher, dass auf Hoster-Seite in Übereinstimmung mit der DSGVO alle Sicherheitskriterien in Bezug auf Zutritts-, Zugangs- und Zugriffskontrolle nach höchsten Standards erfüllt werden.

2. VERTRAULICHKEIT (Art. 32 Abs.1 lit. b DSGVO)

2.1 Zutrittskontrolle

Die Zutrittskontrolle auf Hardware-Ebene bzw. Ebene der Datenverarbeitungsanlagen wird in Übereinstimmung mit der DSGVO durch den Hoster nach höchsten Standards sichergestellt.

2.2 Zugangskontrolle

Die Zugangskontrolle auf Hardware-Ebene bzw. Ebene der Datenverarbeitungsanlagen wird in Übereinstimmung mit der DSGVO durch den Hoster nach höchsten Standards sichergestellt.

Die Zugangskontrolle auf Software-Ebene seitens 321 MED erfolgt durch Identifikation und Authentifikation von Benutzern mittels Benutzerkennung und Passwort. Es existieren Vorgaben für die Mindestlänge und Komplexitätsanforderungen von Passwörtern. Der Zugriff auf 321 MED durch die Benutzer ist nur über eine SSL-verschlüsselte HTTPS-Verbindung möglich.

2.3 Zugriffskontrolle

Die Zugriffskontrolle auf Hardware-Ebene bzw. Ebene der Datenverarbeitungsanlagen wird in Übereinstimmung mit der DSGVO durch den Hoster nach höchsten Standards sichergestellt.

Die Zugangskontrolle auf Software-Ebene seitens 321 MED erfolgt durch strenge Nutzerberechtigungen. Es wird gewährleistet, dass die Nutzungsberechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Zugriff auf Gesundheits-/Patientendaten seitens 321 MED haben nur einzelne, durch 321 MED bestimmte und entsprechend qualifizierte Mitarbeiter der 321 MED GmbH. Alle Mitarbeiter sind zur Geheimhaltung verpflichtet. Regelmäßige Updates der Software-Komponenten werden durch die Administratoren durchgeführt, überwacht und automatisiert auf die Server verteilt.

2.4 Verschlüsselung

Die Nutzung von 321 MED seitens Patient:innen erfordert nicht in allen Fällen die Erfassung von personenbezogenen, Gesundheits- oder Patientendaten. 321 MED ist darauf ausgelegt, die Erfassung und

Verarbeitung personenbezogener, Gesundheits- oder Patientendaten auf das absolute Minimum zu reduzieren.
Sämtliche von 321 MED erfassten Daten (insbesondere Gesundheits-/Patientendaten) sind durch mehrfache Verschlüsselungsprozesse (im Rahmen des technisch Möglichen) geschützt:

- Ende-zu-Ende-Verschlüsselung nach dem Standard AES-256
- Verschlüsselung bei Übertragung mittels TLS/SSL
- Verschlüsselung bei Speicherung nach dem Standard AES-256

2.5 Trennungskontrolle, Pseudonymisierung

Die Datenspeicherung erfolgt nach einem dezentralen Datenbankkonzept. Die Daten jeder Praxis/Klinik als Kunde von 321 MED werden in einer eigenen Datenbank gespeichert. Es besteht ein Berechtigungskonzept sowie eine Festlegung von Datenbankrechten. Jede Praxis/Klinik bzw. deren Mitarbeiter:innen haben lediglich Zugriff auf die eigenen Daten. Eine Aggregation bzw. Zusammenführung von Daten (insbesondere Gesundheits-/Patientendaten) aus verschiedenen Praxen/Kliniken findet nicht statt.

Alle Daten werden nach Pseudonymisierungs- und Trennungskonzept gespeichert, sodass eine unberechtigte Zuordnung (im Rahmen des technisch Möglichen) verhindert wird und Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Es wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

3. INTEGRITÄT (Art. 32 Abs.1 lit. b DSGVO)

3.1 Weitergabekontrolle/Aufbewahrung/Vernichtung

Die Weitergabekontrolle/Aufbewahrung/Vernichtung auf Hardware-Ebene bzw. Ebene der Datenverarbeitungsanlagen wird in Übereinstimmung mit der DSGVO durch den Hoster nach höchsten Standards sichergestellt.

Die Datenweitergabe auf Software-Ebene seitens 321 MED beruht auf einheitlichen Systemen zur Authentifizierung von Benutzern durch Benutzerkennung und Passwort. Alle Kanäle über unsichere Medien werden mittels kryptographischer Verschlüsselung (SSL) gesichert.

Daten (insbesondere Gesundheits-/Patientendaten) werden nur für die kürzestmögliche, für die Verarbeitung nötige Zeit gespeichert und anschließend restlos wieder gelöscht.

Nicht mehr benötigte Datenträger/Festplatten werden sicher vernichtet oder gelöscht. Zuständig für die Vernichtung oder Löschung ist der Geschäftsführer, Herr Dr. Magnus Baringer.

3.2 Eingabekontrolle

Die Eingabekontrolle auf Hardware-Ebene bzw. Ebene der Datenverarbeitungsanlagen wird in Übereinstimmung mit der DSGVO durch den Hoster nach höchsten Standards sichergestellt.

Die Eingabekontrolle auf Software-Ebene seitens 321 MED erfolgt durch Identifikation und Authentifikation von Benutzern mittels Benutzerkennung und Passwort sowie strenge Nutzerberechtigungen (siehe oben). Die Dateneingabe ist nur über eine SSL-verschlüsselte HTTPS-Verbindung möglich.
Personenbezogene/besondere Kategorien personenbezogener Daten können durch Patient:innen über das Programm 321 MED eingegeben, geändert oder gelöscht werden.

4. VERFÜGBARKEIT UND BELASTBARKEIT (Art. 32 Abs.1 lit. b DSGVO)

4.1 Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle auf Hardware-Ebene bzw. Ebene der Datenverarbeitungsanlagen wird in Übereinstimmung mit der DSGVO durch den Hoster nach höchsten Standards sichergestellt.

Die Verfügbarkeitskontrolle auf Software-Ebene bzw. der Betrieb seitens 321 MED wird durch Personal von 8:00 Uhr bis 18:00 Uhr, Montag bis Freitag sichergestellt. Die IT-Systeme werden rund um die Uhr mittels einer Überwachungslösung überwacht.

Es findet eine regelmäßige Sicherung der Daten (Backups) statt.

Alle systemrelevanten Datenverarbeitungsanlagen sind mit einer ausreichend dimensionierten unterbrechungsfreien Stromversorgung versehen.

4.2 Wiederherstellbarkeit

Die Wiederherstellbarkeit auf Hardware-Ebene bzw. Ebene der Datenverarbeitungsanlagen wird in Übereinstimmung mit der DSGVO durch den Hoster nach höchsten Standards sichergestellt.

Auf Software-Ebene seitens 321 MED findet regelmäßig ein Wiederherstellungstest statt. Es existieren adäquate Notfallkonzepte.

5. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (Art. 32 Abs.1 lit. b DSGVO, Art. 25 Abs.1 DSGVO)

5.1 Datenschutzmanagement

Die Anwendungen der 321 MED GmbH werden im Rechenzentrum der Strato AG (Hoster) gehostet. Das Datenschutzmanagement auf Hardware-Ebene bzw. Ebene der Datenverarbeitungsanlagen wird somit in Übereinstimmung mit der DSGVO durch den Hoster nach höchsten Standards sichergestellt.

Seitens 321 MED wird ein strenges Datenschutzmanagement zur Einhaltung von Datenschutzbestimmungen eingesetzt. In das Datenschutzmanagement ist die Geschäftsführung als Verantwortliche sowie der Datenschutzbeauftragte als Erfüllungsgehilfe eingebunden.

Datenschutzbeauftragter der 321 MED GmbH ist Herr Stephan Hendel, der nach der DSGVO folgende Aufgaben übernimmt:

- Hinwirken auf Einhaltung der Datenschutzbestimmungen
- Überwachung der Datenverarbeitung
- Durchführen von Vorabkontrollen
- Vertrautmachen der Mitarbeiter mit geltenden Vorschriften und besonderen Erfordernissen
- Ansprechpartner für Geschäftsleitung, Mitarbeiter, Kunden, Dritte

Seitens 321 MED werden alle Mitarbeiter und Anwender hinsichtlich relevanter Datenschutzregulationen und geltender Vorschriften geschult und dabei ein Bewusstsein für den Umgang mit sensiblen Daten gewährleistet. Eine Verpflichtung der 321 MED-Mitarbeiter:innen zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes erfolgt bezugnehmend auf Art. 28 Abs. 3 S. 2 lit. b DSGVO, §88 TKG und §17 UWG mit Belehrung über strafrechtliche Konsequenzen im Sinne von Art. 84 DSGVO, §42 DSAnpUG-EU (BDSG- neu) und §206 StGB.

5.2 Kontrollprozesse

Die geltenden Regelungen werden laufend überwacht und alle Mitarbeiter zur Einhaltung der Regeln verpflichtet. Eine Überprüfung der Wirksamkeit der technischen und organisatorischen Schutzmaßnahmen wird mindestens jährlich durchgeführt.

5.3 Auftragskontrolle

Soweit 321 MED GmbH Auftragsverarbeiter einsetzt, wird gewährleistet, dass personenbezogene Daten/besondere Kategorien personenbezogener Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen von 321 MED GmbH als Auftraggeber verarbeitet werden können.

321 MED wählt den jeweiligen Auftragsverarbeiter (Auftragnehmer) unter Sorgfaltsgesichtspunkten aus. Seitens 321 MED erfolgt eine vorherige Prüfung der vom jeweiligen Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation. 321 MED schließt mit dem Auftragnehmer notwendige Vereinbarungen zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln ab und verpflichtet die Mitarbeiter des Auftragnehmers zur Vertraulichkeit. 321 MED erbringt schriftliche Weisungen an den Auftragnehmer und vereinbart Kontrollrechte gegenüber dem Auftragnehmer. 321 MED stellt eine Vernichtung/Löschung von Daten durch den Auftragnehmer nach Beendigung des Auftrags sicher.

Ort, Datum

Unterschrift / Stempel Auftraggeber

321 MED GmbH · Am heimlichen Grund 5 · 92421 Schwandorf
Geschäftsführer: Dr. Magnus Baringer · HRB 5603 · USt-IdNr. DE299398795