321MED

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUM DATENSCHUTZ UND DATENSICHERHEIT

Auftraggeber:	Auftragnehmer:
Vorname Nachname Straße PLZ/Ort Telefon E-Mail	321 MED GmbH (im folgenden 321 MED oder Auftragnehmer) Ohmstraße 1a 93055 Regensburg

1. Vertraulichkeit

Maßnahmen, um Unbefugten den Zugang zu Daten und Systemen zu verwehren und unberechtigte Datennutzung zu verhindern.

1.1 Zutrittskontrolle

Die physischen Zugänge zu den IT-Systemen und Datenspeicherorten der 321 MED GmbH sind streng geschützt. Die Serverinfrastruktur wird in hochsicheren, ISO/IEC 27001-zertifizierten Rechenzentren des Hosting-Partners Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen betrieben. Diese Rechenzentren verfügen über umfassende Sicherheitsvorkehrungen wie mehrstufige elektronische Zutrittskontrollsysteme, Überwachungskameras, 24/7-Überwachung durch Sicherheitspersonal und alarmgesicherte Zugangsbereiche, um unbefugten Zutritt effektiv zu verhindern.

Zusätzlich sind die Büroräume der 321 MED GmbH in Regensburg und München durch mechanische und elektronische Schließsysteme gesichert. Der Zutritt zu den Geschäftsräumen ist nur befugten Mitarbeitern mit personengebundenen Schlüsseln bzw. Zugangskarten gestattet. In sensiblen Bereichen erfolgt eine Videoüberwachung der Eingänge, und ein definiertes Schlüsselmanagement stellt sicher, dass Schlüssel regelmäßig inventarisiert und bei Verlust sofort gesperrt bzw. ausgetauscht werden. Besucher werden nur in Begleitung autorisierter Personen eingelassen und in Besuchsprotokollen erfasst.

1.2 Zugangskontrolle

321 MED setzt strikte Authentifizierungsverfahren ein, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden. Der Zugriff auf alle internen Systeme und Anwendungen erfordert individuelle Benutzerkonten mit starken Passwörtern. Es gelten verbindliche Passwort-Richtlinien, die unter anderem eine hohe Komplexität und eine Mindestlänge von 30 Zeichen vorschreiben. Fehlgeschlagene Anmeldeversuche werden gezählt und das Benutzerkonto nach 4 aufeinanderfolgenden Fehlversuchen automatisch gesperrt (Brute-Force-Angriffe zu unterbinden; Schutz vor DDoS-Angriffen erfolgt netzseitig). Benutzer-Sessions verfügen über einen automatischen Timeout: Eine Sitzung wird spätestens nach 8 Stunden Inaktivität (bzw. auch nach 8 Stunden ununterbrochener Nutzung) automatisch abgemeldet, sodass ein vergessener Login keinen Dauerzugang ermöglicht. Für alle Mitarbeiter ist eine Zwei-Faktor-Authentisierung (2FA) verpflichtend, wodurch neben dem Passwort ein zweites Authentisierungsmerkmal (z.B. Einmalcode per App oder SMS) zum Login erforderlich ist. Administratorische Zugriffe auf Server und kritische Infrastrukturkomponenten erfolgen zudem ausschließlich durch besonders befugte Mitarbeitende und sind zusätzlich abgesichert (z.B. mittels spezieller Admin-Konten). Standard- bzw. Gemeinschaftskonten werden nicht verwendet – jede Anmeldung ist einer individuellen Person zuordenbar.

1.3 Zugriffskontrolle

Es ist sichergestellt, dass berechtigte Benutzer ausschließlich auf die personenbezogenen Daten zugreifen können, die ihrer jeweiligen Rolle und Berechtigung unterliegen, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, verändert oder entfernt werden können. Hierzu ist ein rollenbasiertes Berechtigungskonzept implementiert, das dem Grundsatz der minimalen Rechtevergabe folgt. Jeder Nutzer (sowohl interne Mitarbeiter von 321 MED als auch berechtigte Endanwender auf Kundenseite) erhält nur die Zugriffsrechte, die für die Erfüllung seiner Aufgaben erforderlich sind. Die Rechte sind nach Rollen und Funktionen abgestuft und werden durch ein zentrales Identity- und Access-Management verwaltet. Es existieren klar definierte Prozesse zur Vergabe, Änderung und Entziehung von Zugriffsrechten – beispielsweise im Rahmen von Onboarding, Rollenwechsel oder Austritt eines Mitarbeiters; sämtliche Berechtigungsänderungen werden dokumentiert und von berechtigten Stellen kontrolliert. Die Anzahl der System-Administratoren wird auf das notwendige Minimum begrenzt, und ihre Aktivitäten unterliegen einem erhöhten Kontrollniveau (Protokollierung administrativer Aktionen und ggf. Vier-Augen-Prinzip bei sicherheitskritischen Änderungen). Alle Beschäftigten der 321 MED GmbH sind vertraglich auf das Datengeheimnis und die Vertraulichkeit verpflichtet. Sie werden regelmäßig sensibilisiert, unberechtigte Zugriffe oder Datenweitergaben konsequent zu unterbinden.

1.4 Trennungskontrolle

Die Verarbeitung von Daten unterschiedlicher Kunden erfolgt strikt getrennt, um eine Vermischung oder unbefugte Nutzung über Zweckgrenzen hinaus zu verhindern. Die SaaS-Plattform von 321 MED ist mandantenfähig aufgebaut, wobei für jeden Auftraggeber eine logische Isolation der Daten umgesetzt ist (Mandantentrennung auf Datenbank- und Anwendungsebene). Die Daten eines Kunden sind ausschließlich diesem Kunden zugeordnet und für andere Mandanten nicht einsehbar. Es findet keine Aggregation oder gemeinsame Auswertung personenbezogener Daten über verschiedene Auftraggeber hinweg statt. Test-, Entwicklungs- oder Staging-Systeme sind physisch und/oder logisch von der produktiven Umgebung getrennt; Echt-Daten aus dem Produktivsystem werden in solchen nicht-produktiven Umgebungen grundsätzlich nicht verwendet bzw. nur nach vorheriger Anonymisierung/Pseudonymisierung eingesetzt. Durch diese Trennungsmaßnahmen wird sichergestellt, dass jeder Auftraggeber ausschließlich Zugriff auf seine eigenen Daten hat und keinerlei Datenlecks oder Zweckentfremdungen zwischen den Mandanten auftreten.

1.5 Pseudonymisierung und Verschlüsselung

Wo immer möglich, werden personenbezogene Daten in pseudonymisierter oder anonymisierter Form verarbeitet, um die Identifizierbarkeit betroffener Personen zu minimieren. Beispielsweise werden in Protokolldateien oder Support-Datensätzen anstelle von Klarnamen eindeutige interne Kennungen verwendet, sodass ein Rückschluss auf die Person nur mittels zusätzlicher Informationen möglich ist. Soweit eine vollständige Anonymisierung zu Test- oder Analysezwecken durchführbar ist, wird diese vorgenommen, um echte Personenbezüge zu vermeiden.

Zum Schutz der Vertraulichkeit sensibler Daten setzt 321 MED zudem auf starke Verschlüsselungsverfahren. Sämtliche personenbezogenen Daten, die in der Produktivumgebung gespeichert werden (Data-at-Rest in Datenbanken und Dateisystemen), sind durch aktuelle kryptographische Verfahren (z.B. AES-256) geschützt. Die Speicherung erfolgt auf verschlüsselten Datenträgern bzw. innerhalb verschlüsselter Datenbank-Container. Das Management der kryptographischen Schlüssel erfolgt getrennt vom Applikationsbetrieb in einem sicheren Key-Management-System. Die Schlüssel sind nur einem eng begrenzten Personenkreis zugänglich; der Zugriff darauf erfordert besondere Berechtigungen und unterliegt dem Vier-Augen-Prinzip. Es findet eine regelmäßige Rotation der Schlüssel statt, um langfristige Risiken zu minimieren (Schlüsselwechsel in definierten Abständen bzw. bei sicherheitsrelevanten Ereignissen). Auch Datensicherungen (Backups) werden verschlüsselt abgelegt, sodass ein Zugriff auf gespeicherte Backup-Daten ohne Berechtigung nicht möglich ist. Durch diese Maßnahmen ist gewährleistet, dass selbst im Falle eines unbefugten Zugriffs auf Hardware oder Datenspeicher kein Klartext-Zugriff auf personenbezogene Informationen erfolgen kann.

2. Integrität

Maßnahmen, um die Unverfälschtheit, Konsistenz und Authentizität von Daten sicherzustellen und unautorisierte Änderungen oder Verluste zu verhindern.

2.1 Weitergabekontrolle

Um die Vertraulichkeit und Integrität personenbezogener Daten bei der elektronischen Übertragung zu schützen, werden bei 321 MED alle Datenübermittlungen ausschließlich verschlüsselt durchgeführt. Insbesondere ist die SaaS-Plattform nur über gesicherte HTTPS-Verbindungen erreichbar; es kommt eine Transportverschlüsselung mittels TLS (Transport Layer Security) in den aktuellen Versionen 1.2/1.3 mit starken Chiffren zum Einsatz. Unverschlüsselte Zugriffsversuche werden vom Server abgewiesen bzw. automatisch auf HTTPS umgeleitet (HSTS – HTTP Strict Transport Security – ist aktiviert). Durch diese Netzwerkverschlüsselung ist sichergestellt, dass Daten auf dem Transportweg nicht von Unbefugten mitgelesen oder unbemerkt verändert werden können.

Über die reinen Transportmaßnahmen hinaus implementiert 321 MED weitere Mechanismen, um unautorisierte Datenweitergaben oder -manipulationen zu verhindern. In der Web-Software kommen moderne Sicherheits-Header zum Einsatz: Eine Content Security Policy (CSP) stellt sicher, dass Browser nur ausdrücklich erlaubte Ressourcen (Skripte, Stylesheets etc.) laden, wodurch Cross-Site-Scripting- und Injection-Angriffe erheblich erschwert werden. Ebenso ist Cross-Origin Resource Sharing (CORS) restriktiv konfiguriert, sodass ausschließlich

vertrauenswürdige Ursprungsdomänen (etwa die Domains der angebundenen Praxishomepages) berechtigten Zugriff auf die APIs erhalten – fremde Websites können keine unautorisierten Datenabfragen im Hintergrund durchführen. Falls externe Ressourcen in die Web-Anwendung eingebunden werden (z.B. Bibliotheken von verifizierten CDN-Anbietern), wird nach Möglichkeit Subresource Integrity (SRI) genutzt, um die Unveränderheit dieser externen Komponenten sicherzustellen.

Netzwerkseitig schützen Firewalls und Intrusion-Detection-Systeme die Server-Infrastruktur vor unbefugten externen Zugriffen und Angriffen. Alle API-Endpunkte sind zudem mit automatischen Rate Limits versehen, welche übermäßige oder atypische Aufrufraten erkennen und bei Überschreitung temporär blockieren. Hierdurch werden automatisierte Massenanfragen, Denial-of-Service- und Brute-Force-Angriffe bereits an der Peripherie unterbunden. Verdächtige Aktivitäten (z.B. eine ungewöhnlich hohe Zahl fehlgeschlagener Login-Versuche oder auffällige Zugriffsmuster) werden durch ein Echtzeit-Monitoring erkannt. In solchen Fällen erfolgt umgehend eine Alarmierung des Sicherheitsteams, damit entsprechende Gegenmaßnahmen (Sperrungen, weitere Analysen, Einleitung des Incident-Response-Prozesses) unverzüglich eingeleitet werden können.

2.2 Eingabekontrolle

Zur Gewährleistung der Datenintegrität wird umfassend protokolliert, welche Aktionen an personenbezogenen Daten vorgenommen werden und durch wen. Es ist jederzeit nachvollziehbar, ob, wann und von wem Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle). Insbesondere werden Administrationsvorgänge und Zugriffe mit erhöhten Rechten lückenlos in Protokolldateien aufgezeichnet. Ebenso wird die Nutzung der Programmierschnittstellen (API) vollständig mitgeloggt. Die Logdateien enthalten mindestens Angaben zu Datum/Uhrzeit, verantwortlichem Benutzer bzw. Dienst und Art der Aktion (z.B. Datensatz erstellt, geändert oder gelöscht). Diese Protokolle werden auf sicheren Log-Servern bzw. in einem zentralen Audit-Log-System gespeichert, das gegen Manipulationen geschützt ist (z.B. revisionssichere, schreibgeschützte Ablage). Der Zugriff auf Roh-Logdaten ist strikt reglementiert und nur einem kleinen berechtigten Personenkreis zu Analysezwecken gestattet. Ein internes Audit-Konzept stellt sicher, dass die Protokolle regelmäßig ausgewertet werden. Auffälligkeiten oder sicherheitsrelevante Ereignisse in den Logdaten werden durch automatisierte Analysen erkannt und von den zuständigen Sicherheitsverantwortlichen umgehend überprüft. So können unautorisierte Änderungen oder Zugriffsversuche zeitnah erkannt und entsprechende Gegenmaßnahmen ergriffen werden. Sollten Protokolle auf einen möglichen Datenschutzvorfall hindeuten, werden interne Meldewege ausgelöst (inkl. Einbindung des Datenschutzbeauftragten), um unverzüglich weitere Untersuchungen und erforderlichenfalls Benachrichtigungen einzuleiten (siehe auch Abschnitt 5.4 Incident-Response-Management).

3. Verfügbarkeit

Maßnahmen, um personenbezogene Daten und Systeme gegen zufällige oder vorsätzliche Zerstörung oder Verlust zu schützen und die Betriebsbereitschaft auch im Störungsfall aufrechtzuerhalten.

321 MED ergreift umfangreiche Maßnahmen, um eine hohe Verfügbarkeit der Systeme sicherzustellen und Ausfallrisiken zu minimieren. Alle serverseitigen Daten werden regelmäßig gesichert: Es werden mindestens einmal täglich automatische Backups der Datenbanken und zentralen Dateispeicher erstellt. Die Sicherungskopien werden räumlich getrennt in einer redundanten Speicherumgebung vorgehalten und verbleiben verschlüsselt im selben Rechtsraum (EU). Eine Vorhaltung der Backups für 30 Tage ist gewährleistet, um auch länger zurückliegende Wiederherstellungspunkte zur Verfügung zu haben. Darüber hinaus ist ein versioniertes Archivierungskonzept implementiert, das punktuelle Wiederherstellungen älterer Stände ermöglicht. Die Integrität und Funktionsfähigkeit der Datensicherungen wird durch regelmäßige Wiederherstellungstests überprüft – dabei werden Backups stichprobenartig eingespielt und die Konsistenz der wiederhergestellten Daten verifiziert.

Die Rechenzentrumsumgebung bei Hetzner bietet eine hochverfügbare Infrastruktur: Klimatisierung, Brandmelde- und Löschanlagen sowie USV (unterbrechungsfreie Stromversorgung) und Notstromgeneratoren stellen sicher, dass ein Ausfall von Versorgungsleistungen (Strom, Kühlung) die Server nicht beeinträchtigt. Die Server sind in einem Cluster-Verbund organisiert, sodass bei Hardwareausfällen automatische Failover-Mechanismen greifen bzw. betroffene Komponenten umgehend ersetzt werden können. Soweit möglich, sind kritische Komponenten redundant vorhanden, um Single Points of Failure zu vermeiden.

Ferner verfügt 321 MED über einen Notfallplan bzw. ein Disaster-Recovery/Business-Continuity-Konzept. Darin sind klare Verfahren und Verantwortlichkeiten für den Umgang mit gravierenden Störfällen festgelegt – etwa bei einem größeren Hardwaredefekt oder einem erheblichen Datenverlust durch technisches Versagen oder höhere Gewalt. In solchen Fällen kann auf definierte Notfallressourcen zurückgegriffen und eine Wiederherstellung der Daten aus den Backups innerhalb kurzer Zeit vorgenommen werden. Zuständige Mitarbeiter werden regelmäßig in den Notfallverfahren geschult, und es finden Testdurchläufe statt, um die Effektivität der Maßnahmen zu überprüfen. Die Systemlandschaft wird außerdem durch Monitoring kontinuierlich auf wichtige Leistungskennzahlen überwacht (z.B. Auslastung, Speicherplatz, Antwortzeiten), sodass bei beginnenden Engpässen proaktiv reagiert werden kann (etwa durch Hinzuschaltung zusätzlicher Serverressourcen). Insgesamt ist so gewährleistet, dass die Dienste von 321 MED mit hoher Verfügbarkeit laufen und im Falle von Störungen schnellstmöglich wiederhergestellt werden können.

4. Belastbarkeit

Maßnahmen, um die Widerstandsfähigkeit der Systeme gegenüber Angriffen oder außergewöhnlichen Belastungen sicherzustellen.

Neben der allgemeinen Verfügbarkeit wird großer Wert auf die Belastbarkeit der Systeme gelegt. 321 MED sorgt durch ein konsequentes Patch-Management und regelmäßige Software-Updates dafür, dass alle Server und Anwendungen stets auf dem aktuellen Stand sind und bekannte Sicherheitslücken umgehend geschlossen werden. Die Systemumgebung wird kontinuierlich gehärtet (System Hardening): Nicht benötigte Dienste und Ports sind deaktiviert, sicherheitsrelevante Parameter werden gemäß Best Practices konfiguriert, und es werden regelmäßige Schwachstellen-Scans durchgeführt. Identifizierte potenzielle Schwachstellen oder Fehlkonfigurationen werden zeitnah behoben.

Die Netz- und Serverarchitektur ist darauf ausgelegt, Angriffen von außen möglichst standzuhalten. Durch die in Abschnitt 2.1 beschriebenen Maßnahmen (Firewalls, Intrusion Detection, Rate Limiting etc.) sowie durch DDoS-Schutzmechanismen seitens des Rechenzentrumsbetreibers können typische Angriffsarten abgewehrt oder ihre Auswirkungen deutlich reduziert werden. Sollte es dennoch zu Beeinträchtigungen kommen, gewährleisten die redundante Auslegung der Systeme und automatisierte Neustart- bzw. Failover-Prozesse, dass der Dienst schnell wieder in einen stabilen Zustand versetzt wird. Die Plattform ist zudem skalierbar konzipiert, sodass sie auch bei Lastspitzen oder wachsenden Nutzerzahlen performant und stabil bleibt (dynamische Hinzufügung von Ressourcen bei Bedarf).

Alle Mitarbeiter werden für den Ernstfall regelmäßig geschult und mit aktuellen Bedrohungsszenarien vertraut gemacht. So ist sichergestellt, dass im Falle eines sicherheitsrelevanten Vorfalls alle Beteiligten wissen, welche Schritte einzuleiten sind, um den ordnungsgemäßen Betrieb schnellstmöglich wiederherzustellen bzw. aufrechtzuerhalten (siehe auch Abschnitt 5.4 Incident-Response-Management). Durch diese präventiven und reaktiven Maßnahmen erreicht 321 MED eine hohe Resilienz seiner IT-Systeme gegenüber Störungen, Angriffen und außergewöhnlichen Belastungen.

5. Weitere organisatorische Maßnahmen und Datenschutz-Management

5.1 Datenschutzbeauftragter und interne Zuständigkeiten

Die 321 MED GmbH hat einen betrieblichen Datenschutzbeauftragten (Herr Syndikusrechtsanwalt Stephan Hendel, LL.M., E-Mail: shendel@321med.com) benannt, der die Einhaltung der datenschutzrechtlichen Vorschriften überwacht und das Unternehmen in Datenschutzfragen berät. Er steht den Mitarbeitern sowie den Kunden als unabhängiger Ansprechpartner zur Verfügung und wird in sicherheits- und datenschutzrelevante Vorgänge frühzeitig eingebunden. Der Datenschutzbeauftragte kümmert sich um die Entwicklung, Umsetzung und Kontrolle der technischen und organisatorischen Schutzmaßnahmen im Unternehmen.

5.2 Schulungen und Verpflichtung der Mitarbeiter

Alle Beschäftigten von 321 MED werden auf Vertraulichkeit verpflichtet und schriftlich auf das Datengeheimnis gemäß § 53 BDSG sowie auf die Wahrung der Weisungen des Verantwortlichen nach Art. 28 Abs. 3 DSGVO hingewiesen. Neue Mitarbeiter durchlaufen vor Tätigkeitsaufnahme eine umfassende Datenschutz- und IT-Sicherheitsschulung, in der sie mit den geltenden Richtlinien, Sicherheitsstandards und ihren Pflichten vertraut gemacht werden. Für alle Mitarbeiter finden zudem regelmäßige Auffrischungs- und Sensibilisierungsschulungen statt (mindestens einmal jährlich oder anlassbezogen, z.B. bei Einführung neuer Technologien oder gesetzlicher Änderungen). Durch diese Maßnahmen soll ein hohes Bewusstsein für Datenschutz und Datensicherheit der Beschäftigten sichergestellt und die Einhaltung der TOM im Arbeitsalltag verankert werden. Verstöße gegen die Sicherheitsrichtlinien werden sanktioniert, um eine konsequente Umsetzung der Maßnahmen zu gewährleisten.

5.3 Verfahren zur regelmäßigen Überprüfung und Weiterentwicklung

Zur Wahrung eines hohen Sicherheitsniveaus hat 321 MED ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen etabliert (Art. 32 Abs. 1 lit. d DSGVO). Im Rahmen dieses kontinuierlichen Verbesserungsprozesses (Plan-Do-Check-Act-Zyklus) werden alle relevanten Schutzvorkehrungen in definierten Abständen sowie anlassbezogen (z.B. nach Sicherheitsvorfällen, organisatorischen Änderungen oder neuen gesetzlichen Anforderungen) auf ihre Effektivität und Angemessenheit geprüft. Diese Prüfungen erfolgen intern durch das zuständige Sicherheits- und Datenschutzteam und bei Bedarf zusätzlich durch externe Auditoren oder Fachgutachter. Die gewonnenen Erkenntnisse fließen in die Aktualisierung der Sicherheitskonzepte ein, sodass die TOM stets dem aktuellen Stand der Technik und der Risikolage entsprechen. Auch interne Richtlinien und Dokumentationen (z.B. Sicherheitsleitlinien, Berechtigungskonzepte, Notfallpläne) werden regelmäßig gepflegt und versioniert, um im Prüfungsfall einen revisionssicheren Nachweis der getroffenen Maßnahmen erbringen zu können.

5.4 Incident-Response-Management und Meldung von Datenschutzvorfällen

321 MED verfügt über ein dokumentiertes Sicherheitsvorfall-Management. Darin sind klare Meldewege und Reaktionspläne für den Umgang mit Sicherheits- und Datenschutzvorfällen festgelegt. Alle Mitarbeiter sind angewiesen, Anzeichen eines Datenschutzverstoßes oder eines Security Incidents unverzüglich dem Sicherheits- bzw. Datenschutzbeauftragten zu melden. Ein internes Incident-Response-Team bewertet und untersucht gemeldete Vorfälle umgehend. Sollte sich ein bestätigter Datenschutzvorfall ergeben, bei dem ein Risiko für die Rechte und Freiheiten von Betroffenen besteht, wird der betreffende Kunde als Verantwortlicher ohne schuldhaftes Zögern informiert. Dies erfolgt in der Regel binnen 72 Stunden nach Bekanntwerden des Vorfalls, damit der Verantwortliche seiner gesetzlichen Meldepflicht gegenüber der Aufsichtsbehörde gemäß Art. 33 DSGVO fristgerecht nachkommen kann. 321 MED unterstützt den Kunden dabei mit allen notwendigen Informationen über Art und Umfang des Vorfalls sowie die eingeleiteten Gegenmaßnahmen. Jeder Vorfall und dessen Bearbeitung wird intern dokumentiert und im Nachgang analysiert, um gegebenenfalls weitere Optimierungen der Sicherheitsmaßnahmen abzuleiten. Sofern erforderlich, wird 321 MED den Verantwortlichen auch bei der Benachrichtigung betroffener Personen gemäß Art. 34 DSGVO unterstützen.

5.5 Datenschutzfreundliche Technikgestaltung und Voreinstellungen

Bei der Entwicklung und Bereitstellung der Dienste achtet 321 MED auf Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy by Design und Privacy by Default gemäß Art. 25 DSGVO). Das System verarbeitet standardmäßig nur solche personenbezogenen Daten, die für den jeweiligen Zweck erforderlich sind (Datenminimierung). Viele Funktionen sind so gestaltet, dass sensible Daten gar nicht erst erhoben werden, sofern der Zweck auch mit anonymisierten oder pseudonymisierten Angaben erreicht werden kann.

Die Speicherdauer personenbezogener Daten ist auf das erforderliche Maß begrenzt. Temporäre Aufzeichnungen (etwa Sprachmitteilungen oder bestimmte Logdaten mit Personenbezug) werden nach Erreichung ihres Zwecks bzw. nach Sichtung durch den Kunden zeitnah gelöscht. Standardmäßig werden solche Daten maximal 14 Tage vorgehalten und danach automatisiert entfernt. In Absprache mit dem jeweiligen Kunden kann diese Frist im Einzelfall auf bis zu 30 Tage verlängert werden (z.B. wenn bestimmte Verlaufsdaten ausnahmsweise länger benötigt werden); eine darüberhinausgehende Speicherung erfolgt nicht ohne Weisung. Darüber hinaus haben

autorisierte Nutzer jederzeit die Möglichkeit, eine manuelle Löschung bestimmter Daten über die Anwendung oder den Support von 321 MED zu veranlassen. Nach Beendigung des Vertragsverhältnisses mit einem Kunden werden alle dessen personenbezogenen Daten, die bei 321 MED gespeichert sind, entweder nach dokumentierter Weisung an den Kunden zurückgegeben oder vollständig gelöscht. Eine Löschung erfolgt dabei innerhalb der vertraglich vereinbarten Frist, sofern keine gesetzlichen Aufbewahrungspflichten einer Löschung entgegenstehen.

Innovative Funktionen – insbesondere unter Einsatz von Künstlicher Intelligenz (KI) – werden von 321 MED von Anfang an datenschutzkonform konzipiert. Die Sprachverarbeitung für den telefonischen Annahmeservice (Speech-to-Text für eingehende Anrufe) erfolgt durch eine selbst gehostete KI-Lösung. Audioinhalte werden nicht an externe Cloud-Dienste oder Drittanbieter zur Spracherkennung übertragen, sondern direkt auf den eigenen Servern in Text umgewandelt. Die dabei eingesetzten KI-Modelle werden nicht mit realen personenbezogenen Kundendaten trainiert; personenbezogene Informationen dienen nicht zur Verbesserung von KI-Modellen außerhalb des jeweils aktuellen Nutzungsvorgangs. Die KI-Unterstützung beschränkt sich auf rein assistierende Funktionen (Transkription von Sprachnachrichten; Speech-to-Text und Text-to-Speech; Zusammenfassungen von Kommunikationsverläufen). Sie führt keine autonomen Entscheidungen mit rechtlichen oder ähnlichen erheblichen Auswirkungen für Betroffene durch. Damit findet keine ausschließlich automatisierte Entscheidungsfindung im Sinne des Art. 22 DSGVO statt – jeder Vorgang, der für Betroffene relevant ist, wird letztlich von einem menschlichen Nutzer gesteuert. Durch diese Vorsichtsmaßnahmen stellt 321 MED sicher, dass moderne Technologien zwar effizient im Dienst eingesetzt werden, dabei aber jederzeit die Privatsphäre der Patienten gewahrt bleibt und Verarbeitungen nur im legitimen, transparenten Rahmen erfolgen.

5.6 Auftragskontrolle und Unterstützung des Verantwortlichen

321 MED verarbeitet die personenbezogenen Daten der Kunden stets nur im Rahmen der vertraglich vereinbarten Zwecke und ausschließlich gemäß den Weisungen des Auftraggebers (Verantwortlichen) nach Art. 28 DSGVO. Interne Arbeitsanweisungen und Kontrollmechanismen stellen sicher, dass keine Verarbeitung zu eigenen, vom Auftrag abweichenden Zwecken erfolgt. Tätigkeiten, die nicht durch den Vertrag oder die dokumentierten Kundenweisungen gedeckt sind, werden nur nach schriftlicher Genehmigung des Verantwortlichen durchgeführt. Die Einhaltung dieser Weisungsgebundenheit wird regelmäßig kontrolliert und durch die Geschäftsführung überwacht.

Darüber hinaus unterstützt 321 MED die Kunden bei der Wahrnehmung ihrer Pflichten gegenüber betroffenen Personen und Aufsichtsbehörden. Es bestehen definierte Prozesse, um Betroffenenanfragen (Art. 15 ff. DSGVO), die an 321 MED herangetragen werden oder die der Kunde über die Plattform auslöst, unverzüglich zu bearbeiten. Beispielsweise können Auskünfte zu gespeicherten Daten bereitgestellt oder Löschungen und Berichtigungen im System zeitnah umgesetzt werden, sobald der Verantwortliche dies veranlasst. 321 MED stellt dem Verantwortlichen auch die erforderlichen Informationen zur Verfügung, die dieser für eine ggf. notwendige Datenschutz-Folgenabschätzung (Art. 35 DSGVO) benötigt, und unterstützt auf Anfrage bei der Durchführung einer solchen DSFA – insbesondere durch Angaben zu den eingesetzten Technologien, Datenkategorien, Verarbeitungszwecken und Schutzmaßnahmen.

Setzt die 321 MED weitere Unterauftragnehmer (Auftragsverarbeiter i. S. v. Art. 28 DSGVO) ein, erfolgt dies auf Grundlage der in der AVV vereinbarten allgemeinen Genehmigung mit Vorabinformation und Widerspruchsrecht des Auftraggebers; sämtliche Unterauftragnehmer werden sorgfältig ausgewählt, vertraglich auf das DSGVO-Schutzniveau verpflichtet und regelmäßig kontrolliert; eine stets aktuelle Übersicht wird bereitgestellt und bei Änderungen fortgeschrieben. Sämtliche im AVV genannten Unterauftragnehmer verarbeiten die im Auftrag verarbeiteten personenbezogenen Daten ausschließlich innerhalb der EU/EWR; etwaige Übermittlungen in Drittländer erfolgen nur nach vorheriger ausdrücklicher Zustimmung des Auftraggebers und unter Einhaltung der Art. 44 ff. DSGVO (z. B. EU-Standardvertragsklauseln oder Angemessenheitsbeschluss).

Ort, Datum

Unterschrift / Stempel Auftraggeber

321 MED GmbH · Ohmstraße 1a· 93055 Regensburg
Geschäftsführer: Dr. Magnus Baringer · HRB20917, AG Regensburg · USt-IdNr. DE299398795