

# Datenschutzerklärung

## 1. Personenbezogene Daten

Wir, Andrea Moser und Thomas Wieser, Entwickler der MAT MoserAssessTherapy, erheben, verarbeiten und nutzen Ihre personenbezogenen Daten nur mit Ihrer Einwilligung bzw. Mandatierung oder Bestellung zu den mit Ihnen vereinbarten Zwecken oder wenn eine sonstige rechtliche Grundlage im Einklang mit der DSGVO vorliegt; dies unter Einhaltung der datenschutz- und zivilrechtlichen Bestimmungen. Es werden nur solche personenbezogenen Daten erhoben, die für die Durchführung und Abwicklung meiner vertraglichen Verpflichtung Ihnen gegenüber erforderlich sind oder die Sie mir freiwillig zur Verfügung gestellt haben. Personenbezogene Daten sind alle Daten, die Einzelangaben über persönliche Verhältnisse enthalten, beispielsweise Name, Anschrift, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Alter, Geschlecht, Sozialversicherungsnummer, Fotos von Personen. Auch sensible Daten, wie Gesundheitsdaten oder Daten im Zusammenhang mit einem Unfallhergang, der zu einer zu behandelnden Handverletzung führt, können mitumfasst sein.

## 2. Auskunft und Löschung

Als Betroffener haben Sie bezüglich der von mir verarbeiteten Daten das Recht auf Auskunft über Ihre gespeicherten personenbezogenen Daten, deren Herkunft und Empfänger und den Zweck der Datenverarbeitung sowie ein Recht auf Berichtigung, Datenübertragung, Widerspruch, Einschränkung der Bearbeitung sowie Sperrung oder Löschung unrichtiger bzw. unzulässig verarbeiteter Daten. Wenn Sie glauben, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei uns (e-Mail-Adresse: andrea@therapie-analogisch.at) oder der Datenschutzbehörde beschweren.

Insoweit sich Änderungen Ihrer persönlichen Daten ergeben, ersuche ich um entsprechende Mitteilung. Sie haben jederzeit das Recht, eine erteilte Einwilligung zur Nutzung Ihrer personenbezogenen Daten zu widerrufen.

*Durch den Widerruf wird die Rechtmäßigkeit der bis dahin erfolgten Verarbeitung nicht berührt.*

Ihre Eingabe auf Auskunft, Löschung, Berichtigung, Widerspruch und/oder Datenübertragung, im letztgenannten Fall, sofern damit nicht ein unverhältnismäßiger Aufwand verursacht wird, kann an die in Punkt 6. angeführte Stelle/E-Mail-Adresse gerichtet werden. Wenn Sie der Auffassung sind, dass die Verarbeitung Ihrer personenbezogenen Daten durch mich gegen das geltende Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche in einer anderen Weise verletzt worden sind, besteht die Möglichkeit, sich bei der zuständigen Aufsichtsbehörde zu beschweren. In Österreich zuständig ist hierfür die Datenschutzbehörde.

Die Löschung der erhobenen personenbezogenen Daten erfolgt, wenn Ihre Daten zur Erfüllung des mit der Speicherung verfolgten Zwecks nicht mehr erforderlich sind oder wenn ihre Speicherung aus sonstigen gesetzlichen Gründen unzulässig wird. Daten für die Rechnungslegung und buchhalterische Zwecke unterliegen der gesetzlichen Aufbewahrungspflicht von sieben Jahren gemäß Bundesabgabenordnung (BAO).

## 3. Datensicherheit

Der Schutz Ihrer personenbezogenen Daten erfolgt durch entsprechende organisatorische und technische Vorkehrungen. Diese Vorkehrungen betreffen insbesondere den Schutz vor unerlaubtem, rechtswidrigem oder auch zufälligem Zugriff, Verarbeitung, Verlust, Verwendung und Manipulation. Ungeachtet der Bemühungen der

Einhaltung eines stets angemessen hohen Standes der Sorgfaltsanforderungen kann nicht ausgeschlossen werden, dass Informationen, die Sie mir über das Internet bekannt geben, von anderen Personen eingesehen und genutzt werden. Bitte beachten Sie, dass ich daher keine wie immer geartete Haftung für die Offenlegung von Informationen aufgrund nicht von mir verursachter Fehler bei der Datenübertragung und/oder unautorisiertem Zugriff durch Dritte übernehme (z.B. Hackangriff auf E-Mail-Account).

#### **4. Bekanntgabe von Datenpannen**

Ich bin bemüht sicherzustellen, dass Datenpannen frühzeitig erkannt und gegebenenfalls unverzüglich Ihnen bzw. der zuständigen Aufsichtsbehörde unter Einbezug der jeweiligen Datenkategorien, die betroffen sind, gemeldet werden.

#### **5. Aufbewahrung der Daten**

Ich werde Daten nicht länger aufbewahren als dies zur Erfüllung meiner vertraglichen bzw. gesetzlichen Verpflichtungen und zur Abwehr allfälliger Haftungsansprüche erforderlich ist.

#### **6. Kontaktdaten**

Der Schutz Ihrer Daten ist **uns** besonders wichtig. **Wir sind** für Sie unter den unten angeführten Kontaktdaten jederzeit für Ihre Fragen oder Ihren Widerruf erreichbar.

Name: Andrea Moser

Betreff „Datenschutz“

Adresse: Lastenstraße 26a, 9300 St. Veit an der Glan

E-Mail: [andrea@therapie-nalogisch.at](mailto:andrea@therapie-nalogisch.at)

**Thomas Wieser**

**Betreff“ Datenschutz“**

**Adresse:**

**E-Mail**

#### **Technisch-organisatorische Maßnahmen (TOMs)**

Zum Schutz der Daten werden gemäß dem bestehenden Sicherheitskonzept umfassende technisch-organisatorische Maßnahmen umgesetzt. Diese beinhalten insbesondere:

- **Verschlüsselung:**

Alle Datenübertragungen erfolgen ausschließlich über TLS 1.2/1.3 (HTTPS). Ruhende Daten sind mit AES-256 verschlüsselt, Schlüsselverwaltung erfolgt über Azure Key Vault bzw. Hardware-Sicherheitsmodule.

- **Zugriffs- und Berechtigungskontrolle:**

Es besteht eine zentrale Benutzerverwaltung mit individuellen Accounts (kein Shared Account). Rollenbasiertes Zugriffskonzept (Admin/User), Passwort-Richtlinien (mind. 12 Zeichen, komplexe Anforderungen) sowie Account-Lockout bei mehrfach fehlerhafter Anmeldung sind umgesetzt.

- **Organisatorische Maßnahmen:**

Nur autorisierte und geschulte Personen erhalten Zugriff auf sensible Daten. Alle Nutzerinnen nehmen an regelmäßigen Schulungen zu Datenschutz, Passwortsicherheit, Phishing und Incident Response teil.

- **Netzwerksicherheit und Monitoring:**

Firewalls, Netzwerksegmentierung, Intrusion Detection/Prevention (IDS/IPS) sowie Logging und Audit-Trails sind implementiert. Zugriffe werden kontinuierlich überwacht und dokumentiert.

- **Regelmäßige Sicherheitsupdates:**

OS- und Framework-Patches werden zeitnah eingespielt. Kritische Komponenten werden wöchentlich, die gesamte Infrastruktur mindestens jährlich auf Schwachstellen überprüft.

- **Notfall- und Wiederanlaufplanung:**

Regelmäßige Backups werden erstellt und getestet. Wiederherstellungsprozesse sind definiert und werden dokumentiert überprüft.

**Hinweis:** Trotz umfassender Schutzmaßnahmen kann die Datenübertragung im Internet Sicherheitslücken aufweisen. Ein vollständiger Schutz vor unbefugtem Zugriff durch Dritte ist daher nicht möglich.

Die App wird auf dem Server von Paragraph Software, einem Softwareunternehmen mit Sitz in Graz, gehostet. Zugriff auf die Daten haben ausschließlich autorisierte Personen dieses Unternehmens, soweit dies zur Erfüllung der technischen Dienstleistungen erforderlich ist. Mit dem Hosting-Partner Paragraph Software GmbH, Graz, besteht ein Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO.

#### **Optionaler Punkt 7 Cookies und Tracking**

**wenn keine Cookies verwendet werden:** Die App verwendet keine Cookies und keine Technologien zur Nutzerverfolgung (Tracking).

**wenn technisch notwendige Cookies verwendet werden:** Die App verwendet ausschließlich technisch notwendige Cookies, die für den Betrieb der Anwendung erforderlich sind. Es erfolgt keine Nutzerverfolgung (Tracking).

#### **Hinweis zur Verantwortung der Nutzerin**

Vor der Dateneingabe in die Web-App ist die Nutzerin gesetzlich verpflichtet, ihre Patientinnen darüber aufzuklären, dass personenbezogene Gesundheitsdaten in eine webbasierte Software eingegeben werden. Die Patientin ist über **Zweck, Art und Umfang der Datennutzung** zu informieren. Die Zustimmung zur Dateneingabe ist von der Nutzerin der Web-App **aktiv einzuholen und zu dokumentieren**. Die Verantwortung für eine rechtlich gültige Einwilligung sowie deren Inhalt liegt ausschließlich bei der Nutzerin.

Ebenso ist die Nutzerin für die **ordnungsgemäße und datenschutzkonforme Speicherung sowie Verwaltung** der außerhalb der Web-App exportierten Daten (z. B. PDF-Dateien) verantwortlich. Darüber hinaus hat sie sicherzustellen, dass die Web-App nach der Nutzung **ordnungsgemäß geschlossen** wird, um einen unbefugten Zugriff auf Patient:innendaten in unbeaufsichtigten Momenten zu verhindern.