Datenschutzerklärung der Heyfoot App

Verantwortliche Stelle gemäß Art. 4 Nr. 7 DSGVO:

Valipes Medical Solutions GmbH

Schlierseestr. 10b

83101 Rohrdorf

E-Mail: info@heyfoot.de

Datenschutzbeauftragter:

heyData GmbH

Schützenstraße 5

10117 Berlin

Deutschland

E-Mail: datenschutz@heydata.eu

Telefon: +49 89 41325320

Wichtig: Bitte sende uns keine Gesundheitsdaten per E-Mail.

1. Kurzübersicht

Heyfoot verarbeitet nur Daten, die für die Funktionen der App wirklich nötig sind, sowie solche, denen du ausdrücklich zustimmst. Gesundheitsdaten nutzen wir ausschließlich mit deiner ausdrücklichen Einwilligung. Für die bestimmungsgemäße Nutzung prüfen wir Ihren Freischaltcode. Für Erstattung und Abrechnung arbeiten wir nach dem Prinzip der Datenminimierung. Deine Daten werden übertragen und gespeichert verschlüsselt, und beauftragte Dienstleister handeln strikt vertraglich gebunden. Bei Übermittlungen in Staaten außerhalb der EU/EWR beachten wir die Vorgaben der Art. 44 ff. DSGVO sowie die zusätzlichen Anforderungen des § 4 Abs. 3 DiGAV.

Du kannst erteilte Einwilligungen jederzeit in der App widerrufen. Widerrufst du die für die Therapie erforderliche Einwilligung, können wir die Therapieunterstützung nicht weiter anbieten. Der Widerruf einer optionalen Einwilligung allein führt nicht zur Sperrung deines Kontos. Personenbezogene Daten löschen wir fristgerecht oder anonymisieren sie, soweit gesetzliche Pflichten dem nicht entgegenstehen. Sie haben Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch sowie das Recht auf Beschwerde bei einer Aufsichtsbehörde. Welche Daten wir wofür verarbeiten, auf welcher Rechtsgrundlage, wie lange wir sie speichern und an wen sie übermittelt werden, erläutern die folgenden Kapitel.

2. Zweck der Datenverarbeitung

Wir verarbeiten deine Daten, damit du die Heyfoot App bestimmungsgemäß nutzen kannst und wir dir eine sichere, verlässliche Therapieunterstützung bieten. Dafür benötigen wir folgende Datentypen: personenbezogene Daten, Gesundheitsdaten sowie technische – und Nutzungsdaten. Wenn du ein Nutzerkonto einrichtest, dann fragt die App nach Daten, die wir für die Verwaltung deines Kontos benötigen und für die Erstellung, sowie fortlaufende Anpassung deiner Übungen und Trainingspläne. Außerdem dienen deine Daten der Dokumentation deiner Fortschritte. Deine Postanschrift verwenden wir, um dir bei Wunsch ein Trainingsband und begleitende Informationsmaterialien per Post zuzusenden, in einem Willkommenspaket.

Für einen stabilen und sicheren Ablauf des Trainingsprogramms erfassen wir technisch notwendige Informationen zur Bereitstellung der App, zur Fehlerdiagnose und zur Abwehr von Störungen oder Missbrauch. Diese Betriebsdaten sind auf das erforderliche Maß beschränkt und dienen nicht der Profilbildung.

Wenn du uns kontaktierst, nutzen wir deine Angaben zur Beantwortung deiner Anfragen und für relevante Hinweise zur Nutzung der App. Beachte bitte, dass unverschlüsselte E-Mails technische Risiken bergen können. Bitte sende uns keine Gesundheitsdaten per E-Mail.

Zur Abrechnung und, falls angeboten, zur Erstattung durch deine Krankenkasse prüfen wir deinen Freischaltcode und verarbeiten nur die dafür unbedingt erforderlichen Angaben. Wo möglich, arbeiten wir nach dem Prinzip der Datenminimierung und verzichten auf zusätzliche personenbezogene Informationen. Den Freischaltcode behandeln wir getrennt vom Nutzerkonto und löschen ihn nach der Freischaltung; die Einzelheiten erläutern wir in Abschnitt 7.

Zur Qualitätsverbesserung und für Forschungsvorhaben verwenden wir ausschließlich Daten, die wirksam anonymisiert sind und keinen Rückschluss auf deine Person zulassen. Auch aggregierte Daten verwenden wir hierfür nur, wenn sie diese Voraussetzung erfüllen. Soweit wir personenbezogene Daten zum Zweck der technischen Funktionsfähigkeit, Nutzerfreundlichkeit und Weiterentwicklung anonymisieren, erfolgt dies nur aufgrund deiner hierfür getrennt erteilten ausdrücklichen Einwilligung nach Art. 6 Abs. 1 lit. a und, bei Gesundheitsdaten, Art. 9 Abs. 2 lit. a DSGVO in Verbindung mit § 4 Abs. 2 Satz 1 Nr. 4 DiGAV. Eine Verarbeitung personenbezogener Daten für zusätzliche Forschungsvorhaben ist davon nicht umfasst.

3. Rechtliche Grundlagen der Datenverarbeitung

Die für den bestimmungsgemäßen Gebrauch der DiGA erforderlichen personenbezogenen Daten, insbesondere Konto-, Freischaltungs-, Therapie- und hierfür notwendige Betriebsdaten, verarbeiten wir auf Grundlage deiner ausdrücklichen Einwilligung (Art. 6 Abs. 1 lit. a DSGVO in Verbindung mit § 4 Abs. 2 Satz 1 Nr. 1 DiGAV). Gesundheitsdaten verarbeiten wir nur auf Grundlage deiner ausdrücklichen Einwilligung (Art. 6 Abs. 1 lit. a i. V. m. Art. 9 Abs. 2 lit. a DSGVO). Diese Einwilligung kannst du jederzeit mit Wirkung für die Zukunft in der App widerrufen; die Therapieunterstützung ist dann nicht mehr nutzbar. Für zusätzliche Verarbeitungen zur technischen Funktionsfähigkeit, Nutzerfreundlichkeit und

Weiterentwicklung nach § 4 Abs. 2 Satz 1 Nr. 4 DiGAV holen wir eine getrennte Einwilligung ein.

Darüber hinaus verarbeiten wir Daten, wenn und soweit wir hierzu gesetzlich verpflichtet sind, etwa zur Erfüllung regulatorischer Nachweis- und Aufbewahrungspflichten als Hersteller einer DiGA (Art. 6 Abs. 1 lit. c DSGVO).

Außerhalb der nach § 4 Abs. 2 DiGAV einwilligungsbedürftigen Verarbeitung stützen wir uns in eng begrenzten Fällen stützen wir uns auf berechtigte Interessen (Art. 6 Abs. 1 lit. f DSGVO), zum Beispiel zur Gewährleistung der IT-Sicherheit, zur Abwehr von Missbrauch oder zur Durchsetzung rechtlicher Ansprüche. Dabei achten wir auf strikte Datenminimierung und darauf, dass kein Gesundheitsbezug besteht. Analyse- oder Marketingzwecke auf Basis berechtigter Interessen nutzen wir in der App nicht; Aspekte wie die Reichweitenmessung der Website sind nicht Bestandteil dieser App-Datenschutzerklärung.

4. Kategorien verarbeiteter Daten in der App

Kontodaten / Identifikationsdaten

- E-Mail-Adresse
- Kennwort-Hash
- Freischaltcode
- Name
- Postanschrift (für Versand von Trainingsband/Infomaterial)

Gesundheitsdaten

- Indikation/Beschwerdebereich
- Schmerzangaben
- Ergebnisse von Bewegungstests
- Kontraindikationen
- Übungsfeedback
- Therapiefortschritt

Technische Daten

- Plattform (iOS/Android)
- App-Version
- Gerätetyp
- Betriebssystemversion
- grundlegende Diagnosedaten
- Fehlermeldungen

Nutzungsdaten

- Zeitpunkte und Häufigkeit der Nutzung
- aufgerufene Bereiche der App
- Nutzungsdauer
- in der App gesetzte Einstellungen

5. Art der Datenerhebung

Wir erhalten deine Daten direkt von dir, wenn du sie in der App eingibst (Kontodaten/Identifikationsdaten, gegebenfalls Versanddaten und Gesundheitsdaten). Außerdem werden Daten während der Nutzung der App erhoben (Übungsdauer, technische Daten und Nutzungsdaten).

Die für Konto, Freischaltung und Therapie erforderlichen Angaben benötigen wir zur Bereitstellung der jeweiligen Funktion. Ohne diese Angaben ist die betreffende Funktion nicht nutzbar. Deinen Namen und deine Postanschrift benötigen wir nur für den Versand. Optionale Angaben und Einwilligungen kennzeichnen wir gesondert.

6. Auftragsverarbeiter (Art. 28 DSGVO) und weitere Empfänger

Wir setzen sorgfältig ausgewählte Auftragsverarbeiter ein, die personenbezogene Daten in unserem Auftrag auf vertraglicher Grundlage nach Art. 28 DSGVO verarbeiten. Weitere Empfänger sind die nachfolgend genannten Versandunternehmen sowie, soweit für die Abrechnung erforderlich, Krankenkassen oder Abrechnungsstellen. Deren Rolle richtet sich nach der jeweiligen Verarbeitung. Für etwaige Übermittlungen außerhalb der EU/EWR gelten die Art. 44 ff. DSGVO und zusätzlich § 4 Abs. 3 DiGAV. Für Verarbeitungen im Anwendungsbereich dieser Vorschrift sind nur die dort zugelassenen Staaten zulässig; Standardvertragsklauseln allein erweitern diesen Kreis nicht.Im Folgenden werden die eingesetzten Dienstleister und weiteren Empfänger namentlich aufgeführt:

Hosting / Cloud (EU)

Amazon Web Services EMEA SARL (AWS), Luxemburg: Betrieb von App-Servern, Datenbanken und verschlüsseltem Speicher in Frankfurt. Die Daten werden bei der Übertragung und Speicherung verschlüsselt. Sicherheitszertifizierungen dienen als Nachweis geprüfter Sicherheitsmaßnahmen.

Support / Kommunikation

Microsoft Corporation: E-Mail-Kommunikation

Für den Versand von Push-Benachrichtigungen nutzen wir Firebase Cloud Messaging von Google. Dabei werden technische Installationskennungen und Registrierungstoken verarbeitet, um die Nachrichten der richtigen App-Installation zuzuordnen. Wir nutzen Firebase ausschließlich für den Nachrichtenversand und nicht zur Analyse deines Nutzungsverhaltens. Namen, E-Mail-Adressen und Therapieinhalte übermitteln wir hierfür nicht. Die Benachrichtigungen enthalten keine Gesundheitsangaben. Push-Benachrichtigungen sind zunächst deaktiviert und werden erst nach deiner ausdrücklichen

Einwilligung aktiviert. Du kannst sie jederzeit in den Benachrichtigungseinstellungen deines Smartphones deaktivieren; die übrigen Funktionen der App bleiben nutzbar. Deine Einwilligung kannst du außerdem über die in Abschnitt 9 genannten Kontaktwege widerrufen.

Google betreibt Firebase Cloud Messaging auf einer globalen Infrastruktur. Dabei ist eine Verarbeitung der technischen Daten außerhalb der EU bzw. des EWR, insbesondere in den USA, möglich. Soweit Daten an die unter dem EU-US Data Privacy Framework zertifizierte Google LLC in den USA übermittelt werden und die Übermittlung von dieser Zertifizierung erfasst ist, gilt der entsprechende Angemessenheitsbeschluss nach Art. 45 DSGVO. Zusätzlich beachten wir die besonderen Anforderungen des § 4 Abs. 3 DiGAV. Weitere Informationen: https://firebase.google.com/support/privacy.

Versand von Trainingsmaterialien

Deutsche Post AG / DHL: Zustellung von Trainingsband und Informationsmaterial

7. Speicherdauer, Kontoschließung und Löschung

Wir speichern deine Daten für die Dauer der Nutzung der Heyfoot App. Nach Ende deines Abonnements speichern wir deine Daten für ein weiteres Jahr, sofern du dein Benutzerkonto nicht vorher löschst und die hierfür erforderliche Einwilligung fortbesteht. So kannst du bei einer Wiederaufnahme deines Abonnements innerhalb dieses Jahres an deinen bereits erreichten Trainingsfortschritt anknüpfen.

30 Tage vor der vorgesehenen Datenlöschung senden wir dir eine Erinnerungs-E-Mail. Darin informieren wir dich über die bevorstehende Löschung und die Möglichkeit, dein

Abonnement wieder aufzunehmen. Wird dein Abonnement bis zum Ablauf der Jahresfrist nicht wieder aufgenommen, löschen wir deine Daten, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Du kannst die Nutzung der App jederzeit beenden und dein Benutzerkonto unter Profil → Einstellungen → Daten verwalten löschen. Nach Eingang deines Löschauftrags sperren wir dein Konto und löschen deine personenbezogenen Daten unverzüglich. Die einjährige Speicherfrist nach Aboende gilt in diesem Fall nicht. Eine Reaktivierung des gelöschten Kontos ist nicht vorgesehen.

Auch bei einem früheren Widerruf deiner Einwilligung löschen wir die davon betroffenen Daten unverzüglich, sofern keine andere Rechtsgrundlage ihre weitere Verarbeitung erlaubt oder verlangt. Daten, die aufgrund gesetzlicher Aufbewahrungspflichten weiterhin gespeichert werden müssen, beschränken wir auf die hierfür erforderlichen Zwecke und löschen sie nach Ablauf der vorgeschriebenen Fristen.

Achtung: Die Deinstallation der App auf deinem Smartphone löscht dein Benutzerkonto und die bei uns gespeicherten Daten nicht.

Für die Abrechnung erforderliche personenbezogene Daten (z. B. Freischaltcode und abrechnungsrelevante Angaben) speichern wir getrennt von deinen Gesundheitsdaten. Zugriffe sind rollenbasiert auf das erforderliche Maß beschränkt. Daten, die wir so anonymisieren, dass ein Bezug zu deiner Person nicht mehr herstellbar ist, können wir weiterhin zur Qualitätsverbesserung der App und für Forschung verwenden.

8. Sicherheitsmaßnahmen

Wir setzen technische und organisatorische Maßnahmen ein, damit deine Daten geschützt sind vor unerlaubtem Zugriff, Missbrauch bzw. Verlust.

Technische Maßnahmen:

- durchgehende Verschlüsselung der Datenübertragung (SSL/TLS)
- verschlüsselte Speicherung
- Server hinter Firewalls und mit Protokollierung/Monitoring;
- minimale lokale Speicherung auf dem Endgerät in verschlüsselter Form (nur erforderliche App-Daten)
- Betrieb der App- Server bei nach ISO 27001 zertifizierten Anbietern innerhalb der EU.

Organisatorische Maßnahmen

- Zugangskontrollen: Nur autorisierte Mitarbeiter und Dienstleister haben Zugriff
- Anonymisierung und Pseudonymisierung: Falls möglich, werden Daten anonymisiert oder pseudonymisiert zum Schutz deiner Privatsphäre. Pseudonymisierte Daten bleiben personenbezogene Daten.

9. Ihre Rechte

Im Rahmen der DSGVO hast du folgende Rechte:

- Auskunft (Art. 15 DSGVO): Du kannst Auskunft über die von uns verarbeiteten personenbezogenen Daten fordern.
- Berichtigung (Art. 16 DSGVO): Du kannst die unverzügliche Berichtigung unrichtiger sowie die Vervollständigung unvollständiger Daten verlangen.
- Löschung (Art. 17 DSGVO): Du kannst die Löschung deiner Daten verlangen, soweit keine gesetzlichen Aufbewahrungspflichten oder anderen Rechtsgründe entgegenstehen.
- Einschränkung der Verarbeitung (Art. 18 DSGVO): Du kannst die Verarbeitung deiner Daten einschränken, z. B. wenn die Richtigkeit der Daten bestritten wird oder die Verarbeitung unrechtmäßig ist.
- Datenübertragbarkeit (Art. 20 DSGVO): Du kannst die dich betreffenden Daten in einem strukturierten, gängigen und maschinenlesbaren Format erhalten oder – soweit technisch machbar – an einen anderen Verantwortlichen übermitteln lassen; dies gilt für Daten, die du uns bereitgestellt hast und die wir auf Grundlage von Einwilligung oder Vertrag automatisiert verarbeiten.
- Widerruf von Einwilligungen (Art. 7 Abs. 3 DSGVO): Du kannst eine erteilte Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen; die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung bleibt unberührt.
- Widerspruch (Art. 21 DSGVO): Du kannst aus Gründen, die sich aus deiner besonderen Situation ergeben, der Verarbeitung widersprechen, soweit diese auf Art. 6 Abs. 1 lit. e oder f DSGVO beruht (einschließlich ggf. darauf gestütztem Profiling).
- Beschwerde (Art. 77 DSGVO): Du hast das Recht, Beschwerde bei einer Datenschutzaufsichtsbehörde einzureichen, insbesondere in dem Mitgliedstaat deines gewöhnlichen Aufenthaltsorts, deines Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes. Zuständig für unseren Unternehmenssitz ist:

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)
Promenade 18, 91522 Ansbach
Telefon: +49 (0) 981 180093-0
E-Mail: poststelle@lda.bayern.de

Hinweis zur Ausübung deiner Rechte: Du kannst deine Rechte über die in dieser Erklärung genannten Kontaktwege geltend machen. Wir beantworten Anfragen grundsätzlich innerhalb eines Monats. Zur Sicherheit können wir vorab deine Identität bei begründeten Zweifeln verifizieren.

10. Änderung der Datenschutzerklärung

Wir behalten uns vor, diese Datenschutzerklärung bei Bedarf anzupassen. Änderungen werden auf unserer App bekanntgegeben. Soweit eine geänderte Verarbeitung eine neue oder erweiterte Einwilligung erfordert, informieren wir dich vorab und holen diese vor Beginn der betreffenden Verarbeitung ein.

11. Kontaktinformation

Solltest du Fragen haben hinsichtlich der Verarbeitung deiner Daten bzw. deiner Rechte, so wende dich bitte an uns:

Valipes Medical Solutions GmbH

Schlierseestr. 10b

83101 Rohrdorf

E-Mail: info@heyfoot.de