

# Datenschutzerklärung

der Avelios Medical GmbH

03. September 2024

In dieser Datenschutzerklärung wird erläutert, wie die Avelios Medical GmbH als für die Datenverarbeitung Verantwortlicher (nachfolgend auch als "der Verantwortliche", "wir", "uns" oder "unser" bezeichnet) Ihre personenbezogenen Daten im Rahmen der Bereitstellung unserer Website/App und des Vertragsschlusses erhebt und verarbeitet.

Diese Datenschutzerklärung umfasst Folgendes:

1. Kontaktdaten des Verantwortlichen
2. Wie erheben wir Ihre personenbezogenen Daten?
3. Wie erheben wir Ihre personenbezogenen Gesundheits-Daten?
4. Details über die Verarbeitung Ihrer personenbezogenen Daten
5. Details über die Verarbeitung Ihrer personenbezogenen Gesundheits-Daten
6. An wen geben wir Ihre personenbezogenen Daten weiter?
7. An wen geben wir Ihre personenbezogenen Gesundheits-Daten weiter?
8. Wie bewahren wir Ihre persönlichen Daten sicher auf?
9. Wann übermitteln wir Ihre personenbezogenen Daten außerhalb des Europäischen Wirtschaftsraumes?
10. Ihre Rechte in Bezug auf Ihre personenbezogenen Daten
11. Automatisierte Entscheidungsfindung/Profiling
12. Verwendung von Plug-ins
13. Externes Web- und Apphosting
14. Aktualisierung dieser Datenschutzerklärung
15. Kundeninformationen und Newsletter

## 1. Kontaktdaten des Verantwortlichen:

Der Datenverantwortliche verarbeitet Ihre personenbezogenen Daten in dem nachfolgend dargelegten Zusammenhang.

Der Datenverantwortliche: Avelios Medical GmbH

Adresse: Ridlerstraße 39, 80339 München

Kontakt: [datenschutz@avelios.com](mailto:datenschutz@avelios.com)

Vertretung: Geschäftsführer: Christian Albrecht, Nicolas Jakob  
Registrierung: Handelsregister München, HRB 270765  
Tax-ID: DE334616294

Das Avelios Datenschutzteam kann per E-Mail oder per Post kontaktiert werden:

E-Mail: [datenschutz@avelios.com](mailto:datenschutz@avelios.com)  
Post: Avelios Medical GmbH, Ridlerstraße 39, 80339 München  
Datenschutzbeauftragter: Dipl.Ing. Walter Lukmann

Im Falle einer Kontaktaufnahme wird der Datenverantwortliche Ihre personenbezogenen Daten verarbeiten zur:

- Kontaktaufnahme über die Webseite/App
- Kontaktaufnahme per Telefon, sofern angeboten
- Kontaktaufnahme per E-Mail
- Vertragsabwicklung

## **2. Wie erheben wir Ihre personenbezogenen Daten?**

Avelios erhebt personenbezogene Daten über Sie auf folgende Weise:

- Direkt bei Ihnen im Rahmen der Registrierung Ihres Nutzeraccounts sowohl auf der Website als auch bei Nutzung der App.
- Wenn Sie das Patientenportal über die Webseite/App nutzen und die Verwendung von Cookies akzeptieren, erheben wir die Cookies, die Sie akzeptiert haben. Sie können die Cookies über den Cookie Banner bei Webseiten-Besuch verwalten und Ihren Browser so einstellen, dass Sie über das Setzen von Cookies informiert werden und Cookies nur im Einzelfall erlauben. Sie können die Annahme von Cookies für bestimmte Fälle oder generell ausschließen sowie das automatische Löschen der Cookies beim Schließen des Browsers aktivieren. Die hierfür erforderlichen Schritte und Maßnahmen hängen jedoch von Ihrem konkret genutzten Internet-Browser ab. Sollten Sie die Installation der Cookies verhindern oder einschränken, kann dies allerdings dazu führen, dass nicht sämtliche Funktionen des Webauftritts vollumfänglich nutzbar sind.
- Bei der Kontonutzung über die zugehörige Webseite/App.

## **3. Wie erheben wir Ihre personenbezogenen Gesundheits-Daten?**

Während der Nutzung des Accounts, indem Ihre Patientendaten erfasst werden.

## **4. Details über die Verarbeitung Ihrer personenbezogenen Daten**

- a) Warum wir Ihre personenbezogenen Daten verarbeiten (**Spezifischer Zweck**):
- Ihre personenbezogenen Daten werden zur Erstellung eines Nutzeraccounts und für die Nutzung des Patientenportals verarbeitet.

- b) Welche personenbezogenen Daten sind betroffen (**betroffene personenbezogene Daten**):
- Vorname, Nachname, Geburtsdatum, Kontaktdaten (E-Mail, Telefonnummer).
- c) Auf Basis welcher Rechtsgrundlage wir Ihre personenbezogenen Daten verarbeiten (**Rechtsgrundlage**):
- Erfüllung eines Vertrags/Vertragsanbahnung; Ermächtigungsgrundlage: Artikel 6 Absatz 1 lit. b DSGVO.
- d) Wie lange wir Ihre personenbezogenen Daten speichern (**Aufbewahrungsfrist**):
- Bis zur vollständigen Beendigung des Vertrages. Alle gesammelten personenbezogenen Daten werden in Abhängigkeit von dem Zweck der Verarbeitung und der für die Services geltenden rechtlichen Aufbewahrungsfristen für einen begrenzten Zeitraum verarbeitet und aufbewahrt. Avelios hält sich an die gesetzlichen Aufbewahrungsfristen für personenbezogene Daten.
  - Für jede Frage oder Klärung bezüglich der Aufbewahrungsdauer von personenbezogenen Daten, für die Avelios nur ein Auftragsverarbeiter ist, empfehlen wir, dass Sie sich direkt an Ihren Gesundheitsdienstleister, der für die Datenverarbeitung verantwortlich ist, wenden.
  - Bitte beachten Sie: In Anbetracht der gesetzlichen Archivierungspflichten von Gesundheitsdienstleistern können diese die personenbezogenen Daten der Nutzer in ihren eigenen Einrichtungen länger aufbewahren, um eine optimale medizinische Betreuung und Versorgung der Patienten zu gewährleisten.
- Nach Ablauf der Aufbewahrungsfrist, werden die personenbezogenen Daten dauerhaft gelöscht.
- e) Welche Rechte Sie in Bezug auf Ihre personenbezogenen Daten ausüben können (**Rechte**):
- Auskunft;
  - Berichtigung;
  - Löschung;
  - Einschränkung der Verarbeitung;
  - Übertragbarkeit.

## 5. Details über die Verarbeitung Ihrer personenbezogenen Gesundheits-Daten

Personenbezogene Gesundheits-Daten werden von Avelios lediglich in kryptographisch gesicherter Form gespeichert. Dabei werden die Daten mit einem für Avelios unbekanntem nutzerbezogenen Schlüssel symmetrisch mittels AES-Verschlüsselung verschlüsselt und sind somit nicht für Avelios zugänglich. Diese Daten enthalten ohne Entschlüsselung durch den Nutzer faktisch leeren Informationsgehalt. Damit ist sichergestellt, dass Avelios keinen Einblick in gespeicherte Gesundheits-Daten der Nutzer hat.

Die Daten werden erst auf der Nutzerseite auf dem Endgerät des Nutzers entschlüsselt und lesbar, sowie in bereits verschlüsselter Form hochgeladen.

Bei der Freigabe von personenbezogenen Gesundheits-Daten durch den Nutzer überträgt Avelios die Daten geschützt durch eine Transportverschlüsselung in die Gesundheitsdienstleister, wobei die Daten jeweils nur innerhalb der Gesundheitsdienstleister permanent gespeichert werden.

Bereits übertragene medizinische Daten, die nach Nutzerfreigabe an die Gesundheitsdienstleister übertragen wurden, können nur durch Löschanforderung des Nutzers an die Gesundheitsdienstleister direkt gelöscht werden.

## **6. An wen geben wir Ihre personenbezogenen Daten weiter?**

Wir können Ihre personenbezogenen Daten weitergeben an:

- Auftrags- und Subauftragsverarbeiter. Wir veröffentlichen und aktualisieren die Liste unserer aktuellen Auftragsverarbeiter regelmäßig und führen darin den Firmennamen, die Firmenanschrift und den spezifischen Zweck der Verarbeitung des Dienstleisters auf;
- jede zuständige Behörde oder Stelle zum Zweck der Beantwortung gesetzlicher oder behördlicher Anfragen, gerichtlicher Anordnungen, Vorladungen oder rechtlicher Verfahren, wenn dies zur Einhaltung geltender Gesetze erforderlich ist;
- jeden Erwerber, wenn personenbezogene Daten im Rahmen des Verkaufs oder einer sonstigen Übertragung unseres gesamten oder eines Teils unseres Vermögens an ein anderes Unternehmen übertragen werden;
- Versicherern, Anwälten, anderen Beratern und Gerichten zur Durchsetzung von Ansprüchen und/oder der Verteidigung unserer Position.

## **7. An wen geben wir Ihre personenbezogenen Gesundheits-Daten weiter?**

Personenbezogene Gesundheits-Daten werden von Avelios lediglich an Gesundheitsdienstleister gesendet, für die eine Terminbuchungsanfrage oder eine konkrete Terminbuchung des Nutzers vorliegt.

Die Übertragung des medizinischen Steckbriefes findet nur nach expliziter Nutzerzustimmung pro Gesundheitsdienstleister statt.

Die Datenübertragung ist zudem mittels Transportverschlüsselung gesichert.

## **8. Wie bewahren wir Ihre persönlichen Daten sicher auf?**

Wir nehmen die Sicherheit aller bei uns gespeicherten personenbezogenen Daten sehr ernst und verpflichten uns, Ihre personenbezogenen Daten zu schützen. Wir haben daher alle notwendigen rechtlichen, technischen und organisatorischen Sicherheitsmaßnahmen (TOMs) getroffen und unsere Dienstleister entsprechend ausgewählt und verpflichtet.

Wir haben mit den Gesundheitsdienstleister jeweils spezifische Auftragsdatenverarbeitungsverträge abgeschlossen, die sicherstellen, dass deren allgemeine technische und organisatorische Maßnahmen (TOMs) hinreichend erfüllt werden. Die Gesundheitsdienstleister sind ausschließlich befugt, die Daten als Auftragsverarbeiter unter Einhaltung der Bestimmungen dieser Datenschutzerklärung und der Verpflichtungen des jeweiligen Auftragsdatenverarbeitungsvertrages in unserem Auftrag und gemäß unseren Weisungen zu verarbeiten.

Wir können jedoch nicht alle Risiken kontrollieren, die mit der Nutzung des Internets verbunden sind. Die Datensicherheit hängt auch von der Wachsamkeit jedes Einzelnen und dem richtigen Umgang mit diesen Technologien ab. Daher bitten wir unsere Nutzer, bei der Nutzung von Internetdiensten auf mögliche inhärente Risiken zu achten.

## **9. Wann übermitteln wir Ihre personenbezogenen Daten außerhalb des Europäischen Wirtschaftsraumes?**

Wir nutzen ausschließlich Drittanbieter, die ihren Sitz innerhalb des Europäischen Wirtschaftsraumes haben und Sicherheits- und Vertraulichkeitsverpflichtungen unterliegen, die mit dieser Datenschutzerklärung und dem geltenden Recht übereinstimmen.

Damit stellen wir sicher, dass wir Ihre personenbezogenen Daten zu keinem Zeitpunkt außerhalb des europäischen Wirtschaftsraumes übermitteln und somit bestmöglich vor unerlaubten Zugriff schützen.

## **10. Ihre Rechte in Bezug auf Ihre personenbezogenen Daten**

10.1 Gemäß allen anwendbaren Gesetzen haben Sie das Recht:

- a) auf Auskunft über Ihre personenbezogenen Daten (Art. 15 DSGVO):
  - wir stellen Ihnen detaillierte Informationen über die Verarbeitung Ihrer persönlichen Daten bereit;
- b) auf Berichtigung Ihrer personenbezogenen Daten (Art. 16 DSGVO):
  - wenn die personenbezogenen Daten, die wir verarbeiten, unrichtig sind;
- c) auf Löschung Ihrer personenbezogenen Daten (Art. 17 DSGVO):
  - wenn Sie möchten, dass wir einige oder alle Ihrer personenbezogenen Daten löschen;
- d) der Verarbeitung Ihrer persönlichen Daten zu widersprechen (Art. 21 DSGVO):
  - wenn Sie möchten, dass wir die Verarbeitung Ihrer personenbezogenen Daten einstellen, bis wir zwingende schutzwürdige Gründe für die Verarbeitung nachweisen können, die gegenüber Ihren Interessen, Rechten und Freiheiten überwiegen, oder für die Begründung, Ausübung oder Verteidigung von Rechtsansprüchen;
- e) auf Einschränkung der Verarbeitung Ihrer personenbezogenen Daten (Art. 18 DSGVO):
  - wenn Sie die Richtigkeit, die Rechtmäßigkeit oder die Notwendigkeit der Verarbeitung Ihrer personenbezogenen Daten bestreiten, werden wir die Verarbeitung Ihrer personenbezogenen Daten auf ein Mindestmaß beschränken (Speicherung) und sie gegebenenfalls nur zur Begründung, Ausübung oder Verteidigung von Rechtsansprüchen oder, soweit erforderlich, zum Schutz einer anderen natürlichen oder juristischen Person oder aus einem anderen, durch geltende Gesetze vorgeschriebenen Grund verarbeiten;
- f) Ihre personenbezogenen Daten in einem strukturierten und standardisierten Format zu erhalten oder die Übertragung dieser Daten an einen anderen Verantwortlichen zu verlangen (Portabilität) (Art. 20 DSGVO).

10.2 Widerruf Ihrer Einwilligung(en):

Wenn die Rechtsgrundlage der Verarbeitung wie vorliegend Ihre Einwilligung ist, können Sie Ihre erteilte(n) Einwilligung(en) jederzeit ohne Angabe von Gründen widerrufen.

Wenn Sie dies tun, werden wir jede weitere Verarbeitung auf der Grundlage dieser Einwilligung beenden. Bitte beachten Sie, dass der Widerruf Ihrer Einwilligung die Rechtmäßigkeit einer Verarbeitung, die bisher auf der Grundlage Ihrer Einwilligung erfolgte, nicht berührt.

### 10.3 Ausübung Ihrer Rechte:

Wenn Sie diese Rechte ausüben und/oder alle relevanten Informationen erhalten möchten, wenden Sie sich bitte an die folgende E-Mail-Adresse:

**[datenschutz@avelios.com](mailto:datenschutz@avelios.com)**

Um eine effektive Ausübung Ihrer Rechte zu gewährleisten, beachten Sie bitte, dass Sie sich für Ihre Fragen und Forderungen im Zusammenhang mit der Verarbeitung über die oben genannte E-Mail-Adresse an den Verantwortlichen richten können.

Um die Verletzung von Rechten Dritter zu vermeiden, behalten wir uns das Recht vor, im Fall von begründetem Zweifel eine vorherige Überprüfung Ihrer Identität vorzunehmen, indem wir Sie um Nachweis durch ein Ausweisdokument bitten.

Wir werden innerhalb von einem Monat nach Erhalt Ihrer Anfrage antworten, behalten uns jedoch das Recht vor, diese Frist um zwei Monate zu verlängern, wenn dies aufgrund der Komplexität Ihrer

Anfrage erforderlich ist. Wir werden Sie in jedem Fall innerhalb von einem Monat nach Eingang Ihrer Anfrage informieren, wenn wir uns für eine Verlängerung der Antwortfrist entscheiden.

### 10.4 Beschwerden:

Sie haben das Recht, sich beim Bayerischen Landesbeauftragten für Datenschutz, über die Art und Weise zu beschweren, wie wir Ihre personenbezogenen Daten verarbeiten.

Bayerische Landesbeauftragte für den Datenschutz (BayLfD):

Prof. Dr. Thomas Petri

Schreiben: Postfach 22 12 19, 80502 München

Besuchen: Wagnmüllerstraße 18, 80538 München (Bitte nur nach vorheriger Terminabsprache)

Anrufen: +49 89 212672-0

Faxen: +49 89 212672-50

Mailen: [poststelle@datenschutz-bayern.de](mailto:poststelle@datenschutz-bayern.de)

USt-IdNr.: DE 811335517

## 11. Automatisierte Entscheidungsfindung/Profiling

Es findet derzeit keine automatisierte Entscheidungsfindung oder Profiling statt, die/das Sie rechtlich oder anderweitig erheblich beeinträchtigen würde. Wir werden Ihnen aber auf Basis Ihrer individuellen personenbezogenen Daten und der Analyse Ihres Nutzerverhaltens gezielt Angebote unterbreiten.

Da wir Sie nicht mit Informationen und Angeboten belästigen möchten, die für Sie möglicherweise nicht relevant sind, werten wir Ihr Kundenprofil aus, d.h. Informationen wie Alter und Geschlecht, die

wir durch Ihre Nutzung unserer Dienste sammeln, um Ihnen nur Informationen und Angebote zu senden, die wir als interessant oder relevant für Sie erachten.

## **12. Verwendung von Plug-ins**

Für ein besseres und effizienteres Webseiten-/App-Design verwenden wir Plug-ins diverser Hersteller. Diese haben wir folgend aufgeführt und deren Verwendungszweck beschrieben. Weitere Informationen und insbesondere die Datenschutzerklärung der Drittanbieter finden Sie auf deren jeweiliger Webseite.

Diese Drittanbieter fungieren als sogenannte Auftragsdatenverarbeiter. Wir haben diesbezüglich darauf geachtet, nur seriöse Auftragsdatenverarbeiter zu verwenden, um die Sicherheit Ihrer Daten weitestmöglich zu gewährleisten.

Um mit Blick auf Ihre personenbezogenen Daten dem Grundsatz der Datensparsamkeit und der Verhältnismäßigkeit gerecht zu werden, haben wir uns darauf beschränkt, nur notwendige und soweit möglich Standardbibliotheken zu verwenden.

Sofern Sie weitere Verbesserungsvorschläge haben, zögern Sie nicht uns zu kontaktieren.

### **Plug-ins:**

#### Google Play Core-Bibliotheken:

Die Google Play Core-Bibliotheken sind die Laufzeitschnittstelle unserer App mit dem Google Play Store. Wir können dadurch:

- zusätzliche Sprachressourcen herunterladen
- die Bereitstellung von Funktionsmodulen verwalten
- die Bereitstellung von Asset Packs verwalten
- In-App-Updates auslösen
- In-App-Bewertungen anfordern

Die Play Core-Bibliotheken sind in Java, Kotlin und Native verfügbar. Weitere Informationen zu den neuesten Versionen finden Sie in den Versionshinweisen.

Wir verwenden die Google Play Core-Bibliotheken, um einen reibungslosen Ablauf und bestmögliche Funktionalität gewährleisten zu können. Unter Abwägung Ihrer Datenschutzinteressen und dem Gebot der Datensparsamkeit stellt dies auch eine angemessene Abwägung zugunsten des Einsatzes der Play Core-Bibliotheken dar.

#### Apple Core Foundation:

Core Foundation ist ein Framework, das grundlegende Software-Dienste bereitstellt, die für Anwendungsdienste, Anwendungsumgebungen und die Anwendungen selbst nützlich sind. Core Foundation bietet außerdem Abstraktionen für gängige Datentypen, erleichtert die Internationalisierung mit der Speicherung von Unicode-Zeichenfolgen und bietet eine Reihe von Hilfsprogrammen wie Plug-in-Unterstützung, XML-Eigenschaftslisten, URL-Ressourcenzugriff und Voreinstellungen.

Wir verwenden die Apple-Standardbibliothek, um einen reibungslosen Ablauf und bestmögliche Funktionalität gewährleisten zu können. Unter Abwägung ihrer Datenschutzinteressen und dem Gebot

der Datensparsamkeit stellt dies eine angemessene Abwägung zugunsten des Einsatzes der Apple-Standardbibliothek dar.

#### Next.JS:

Next.JS ist ein von Vercel erstelltes Open-Source-Webentwicklungs-Framework, das React-basierte Webanwendungen mit serverseitigem Rendering und der Generierung statischer Websites ermöglicht.

Wir verwenden Next.JS als Grundlage unserer Anwendung, um einen reibungslosen Ablauf und bestmögliche Funktionalität gewährleisten zu können. Unter Abwägung ihrer Datenschutzinteressen und dem Gebot der Datensparsamkeit stellt dies eine angemessene Abwägung zugunsten des Einsatzes von Next.JS dar.

#### Google Sign-In:

Google Sign-In ermöglicht die direkte Authentifizierung von Nutzern auf Basis eines bereits bestehenden Google Accounts.

Wir verwenden Google Sign-In als optionaler Dienst, der erst durch aktives Handeln des Nutzers beim Speichern eines Termins in den Kalender aktiv wird. Dabei wird eine Authentifizierung (OAuth2) über Google durchgeführt, welche der Webanwendung bis zum Auslaufen des Authentifizierungs-Tokens Kalenderzugriff gibt. Wir verwenden diesen Zugriff, um einmalig ein Kalenderevent im Kalender des Nutzer zu speichern. Unter Abwägung ihrer Datenschutzinteressen und dem Gebot der Datensparsamkeit stellt dies eine angemessene Abwägung zugunsten des Einsatzes von Google Sign-In dar.

#### Friendly Captcha:

Friendly Captcha ist eine von einem deutschen Unternehmen entwickelte Lösung, um Webseiten und Online-Dienste sicher vor Spam und Bots zu schützen.

Wir verwenden Friendly Captcha bei ausgewählten Aktionen dazu, um zu verifizieren, dass es sich bei der durchgeführten Anfrage nicht um Spam handelt, sondern um einen Menschen. Unter Abwägung ihrer Datenschutzinteressen und dem Gebot der Datensparsamkeit stellt dies eine angemessene Abwägung zugunsten des Einsatzes von Friendly Captcha dar.

### **13. Externes Web- und Apphosting**

Die Webseite und die App werden bei einem externen Dienstleister gehostet (Hoster).

Die personenbezogenen Daten, die auf diesen Diensten erfasst werden, werden auf den Servern des Hosters gespeichert.

Die personenbezogenen Gesundheits-Daten werden als verschlüsseltes Backup so auf den Servern des Hosters gespeichert, dass Avelios und der Dienstleister diese nicht lesen kann.

Der Einsatz des Hosters erfolgt zum Zwecke der Vertragserfüllung gegenüber unseren potenziellen und bestehenden Kunden, den Gesundheitsdienstleistern, gemäß Art. 6 Abs. 1 lit. b DSGVO und im Interesse einer sicheren, schnellen und effizienten Bereitstellung unseres Online-Angebots durch einen professionellen Anbieter gemäß Art. 6 Abs. 1 lit. f DSGVO.

Unser Hoster wird Ihre Daten nur insoweit verarbeiten, wie dies zur Erfüllung seiner Leistungspflichten erforderlich ist und unsere Weisungen in Bezug auf diese Daten auf Grundlage eines AVVs befolgen.

Wir setzen folgenden Hoster ein:

netcup GmbH  
Daimlerstraße 25  
D-76185 Karlsruhe

#### **14. Aktualisierung dieser Datenschutzerklärung**

Wir können diese Datenschutzerklärung von Zeit zu Zeit überarbeiten oder aktualisieren. Jede Änderung dieser Datenschutzerklärung wird mit der Online-Veröffentlichung auf dieser Webseite wirksam. Wenn eine solche Änderung nach geltendem Recht eine Benachrichtigung oder Einwilligung erfordert, werden Sie benachrichtigt oder erhalten die Möglichkeit zur Einwilligung.

#### **15. Kundeninformationen und Newsletter**

Innerhalb Ihres Avelios Nutzeraccounts wird Ihnen möglicherweise die Möglichkeit eingeräumt, den Newsletter unseres Unternehmens sowie weitergehende Kundeninformationen mittels E-Mail-Nachrichten zu abonnieren. Der E-Mail-Versand erfolgt immer an die im Benutzerkonto bereits hinterlegte und bei der Registrierung von Ihnen bereits bestätigte E-Mail-Adresse. Diese Daten verwenden wir ausschließlich für den Versand der angeforderten Informationen und geben diese nicht an Dritte weiter. Die Verarbeitung erfolgt ausschließlich auf Grundlage Ihrer Einwilligung (Art. 6 Abs. 1 lit. a DSGVO).