

Allgemeine Nutzungsbedingungen

der Avelios Medical GmbH

September 2024

1. Einleitung

Die Avelios Medical GmbH, Ridlerstraße 39, 80339 München (nachfolgend "Avelios" genannt) bietet diverse Dienste an.

Die vorliegenden Allgemeinen Geschäftsbedingungen (nachfolgend "(Allgemeine) Nutzungsbedingungen" genannt) gelten für die nachfolgenden Inhalte, Apps, Tools, Produkte und sonstigen Dienstleistungen (nachfolgend "Dienste" genannt). Mit diesen Diensten können Patienten und ihre Angehörigen besondere Services von Avelios (nachfolgend "Funktionen" genannt) vor, während und nach dem Aufenthalt bzw. einer ambulanten Behandlung in medizinischen Vertragspartnerleistungserbringern (nachfolgend auch "Gesundheitsdienstleister" genannt) nutzen.

Avelios ermöglicht den Zugang zu diesen Diensten und deren Nutzung ausschließlich auf der Grundlage der vorliegenden Nutzungsbedingungen, die das Verhältnis zwischen Avelios als dem Betreiber der Dienste und den Patienten und Angehörigen als Nutzer der Dienste in ihrer Funktion als Patienten der medizinischen Leistungserbringer regeln.

Die Nutzung der Dienste setzt voraus, dass sich der Patient oder Angehörige im Internet oder in der App im Avelios Patientenportal (nachfolgend "Patientenportal" genannt) registriert.

Als "Nutzer" wird im Folgenden jeder Patient oder jeder Angehörige eines Patienten der medizinischen Vertragspartnerleistungserbringer bezeichnet, der sich im Patientenportal ordnungsgemäß registriert hat und die Dienste nutzt.

"Avelios" bezeichnet im Folgenden die Betreiberin des Patientenportals und sonstiger Dienste.

Als "(Vertragspartner-)Klinik" bzw. "(Vertragspartner-)Kliniken" werden im Folgenden die betreffenden medizinischen Leistungserbringer bzw. Gesundheitsdienstleister bezeichnet, welche an dem jeweiligen Standort eine medizinische Einrichtung (z.B. ein Krankenhaus, ein Medizinisches Versorgungszentrum oder eine Arztpraxis, gemeinsam sogenannte Medizinische Leistungserbringer) betreiben und die Avelios Dienste ihren Patienten als Servicedienstleistung zur Verfügung stellen.

Bitte beachten Sie:

Die Avelios Service-Plattform dient nicht zur Vereinbarung von Terminen für Notfälle. In diesem Fall müssen die Patienten direkt den medizinischen Leistungserbringer telefonisch kontaktieren oder den Notruf 112 wählen.

Avelios als Plattformanbieter ist selbst keine Gesundheitseinrichtung, erbringt keine Gesundheitsdienstleistungen und beschränkt sich daher auf die Rolle eines technischen Dienstleisters und Vermittlers.

2. Leistungsumfang

2.1 Die Nutzung der Dienste ist ausschließlich für private Zwecke gestattet. Jegliche Nutzung außerhalb der vorgesehenen Zwecke bedarf der vorherigen schriftlichen Zustimmung durch Avelios.

2.2 Die Nutzung der Dienste erfordert bestimmte System- und Gerätevoraussetzungen (z.B. aktuelle Betriebssysteme) auf den vom Nutzer verwendeten Endgeräten (z.B. Tablet, Smartphone, Computer). Zusätzlich benötigt der Nutzer für den Zugriff und die Nutzung einzelner Dienste und Funktionen Authentifizierungsinstrumente und/oder personalisierte Sicherheitsmerkmale (z.B. 2-Faktor-Authentifizierung), um sich als berechtigter Nutzer auszuweisen. Diese Voraussetzungen werden dem Nutzer im Rahmen der beabsichtigten und/oder laufenden Registrierung/Nutzung automatisch angezeigt. Dem Nutzer obliegt die Erfüllung dieser Voraussetzungen.

2.3 Die Nutzer erkennen an, dass eine permanente Verfügbarkeit der Dienste technisch nicht zu realisieren ist und ein Anspruch hierauf gegenüber Avelios oder den einzelnen Vertragspartnerkliniken nicht besteht. Insbesondere Wartungs-, Sicherheits- oder Kapazitätsbelange sowie Ereignisse, die nicht im Machtbereich von Avelios stehen (wie z. B. Störungen von öffentlichen Kommunikationsnetzen, Stromausfälle), können zu kurzzeitigen Störungen oder zur vorübergehenden Einstellung der Dienste oder einzelner Funktionen führen.

3. Registrierung

3.1 Die Nutzung der Dienste erfordert eine Registrierung des Nutzers im Patientenportal. Während des Registrierungsprozesses hat der Nutzer insbesondere diesen Nutzungsbedingungen und den Datenschutzbestimmungen des Patientenportals zuzustimmen. Die Registrierung und Nutzung ist kostenlos.

3.2 Der Nutzer sichert zu, dass er zum Zeitpunkt der Registrierung mindestens 16 Jahre alt ist.

3.3 Bei der Registrierung gibt der Nutzer seinen Vornamen, Nachnamen, Geburtsdatum, Telefonnummer und eine E-Mail-Adresse an ("Zugangsdaten"). Abschließend setzt der Nutzer ein Passwort. Er ist verpflichtet, seine Zugangsdaten geheim zu halten und vor dem Zugriff durch unbefugte Dritte aufzubewahren. Sind dem Nutzer die Zugangsdaten abhandengekommen, oder stellt er fest, oder hegt er den Verdacht, dass seine Zugangsdaten von einem Dritten genutzt werden, so hat er dies Avelios umgehend mitzuteilen. Avelios wird die Zugangsdaten nicht an Dritte weitergeben und den Nutzer zu keinem Zeitpunkt nach dem Passwort fragen.

3.4 Nach Absendung des Registrierungsformulars erhält der Nutzer eine E-Mail mit einem Bestätigungslink.

3.5 Durch den Abschluss des Registrierungsvorgangs gibt der Nutzer ein Angebot zum Abschluss des Vertrages über die Nutzung des Patientenportals und die Nutzungsberechtigung weiterer Dienste ab. Avelios nimmt dieses Angebot durch Freischaltung des Nutzers an. Durch diese Annahme kommt der Nutzungsvertrag zustande.

3.6 Ein Anspruch auf Registrierung und Abschluss eines Nutzungsvertrages besteht nicht. Avelios kann eine Registrierung ohne Angabe von Gründen ablehnen, sofern nicht eine unmittelbare Drittwirkung von Grundrechten (Kontrahierungszwang) dem entgegensteht.

Anmerkung: Avelios sichert darüber hinaus den Login mittels 2-Faktor Authentifizierung ab.

4. Einrichtung eines Benutzerprofils

Der Nutzer hat die Möglichkeit, ein Benutzerprofil im Patientenportal einzurichten. Soweit er von dieser Möglichkeit Gebrauch macht, verpflichtet sich der Nutzer in seinem Benutzerprofil wahre, vollständige und nicht irreführende Angaben zu seiner Person zu machen, insbesondere seinen Klarnamen und keine Pseudonyme oder Künstlernamen zu verwenden. Bei Änderungen der bei der Einrichtung des Benutzerprofils gemachten Angaben, hat der Nutzer seine Angaben in seinem Benutzerprofil stets unverzüglich zu aktualisieren.

Sofern der Nutzer das Nutzerprofil verwendet, um im Namen und in Vertretung Termine für einen Angehörigen zu buchen oder zu verwalten, verpflichtet sich der Nutzer,

- dass er dem Angehörigen eine Kopie der Datenschutzerklärung zur Verfügung gestellt hat,
- dass der Angehörige den Nutzer bevollmächtigt hat, in seinem Namen der Verarbeitung seiner personenbezogenen Daten zuzustimmen,
- dass er sich verpflichtet, diese Bevollmächtigung auf Verlangen von Avelios mit Beweismitteln der ZPO nachzuweisen,
- und dass er rechtlich vertretungsberechtigt ist, sofern der Angehörige nicht geschäftsfähig sein sollte.

5. Dienste und Funktionen

5.1 Nicht alle in diesen Nutzungsbedingungen genannten Dienste und/oder Funktionen können in jeder oder für jede Vertragspartnerklinik verfügbar sein.

5.2 Patientenportal

5.2.1 *"Dokumente"*: Über diese Funktion kann der Nutzer auf patientenindividuelle Unterlagen (z.B. Arztbriefe, Laborberichte) zugreifen, eigene Unterlagen im Avelios Portal hochladen sowie diese an Gesundheitsdienstleister übermitteln. Ansprüche des Nutzers auf die Zurverfügungstellung von Behandlungsunterlagen über diese Funktion bestehen nicht, insbesondere wird eine Aktualität und Vollständigkeit nicht gewährleistet, da Avelios nur die Plattform zur Verfügung stellt.

Hinweis: Unberührt von dieser Funktion bleibt das Recht des Patienten gemäß § 630g BGB auf Einsichtnahme in seine Behandlungsunterlagen in der Vertragspartnerklinik vor Ort oder auf Übersendung von Abschriften.

Ein solcher Anspruch besteht in dem Vertragsverhältnis zur behandelnden Klinik, nicht gegenüber Avelios als Servicedienstleister.

Avelios ist nicht für die inhaltliche Richtigkeit der Dokumente der Gesundheitsdienstleister/behandelnden Kliniken verantwortlich.

5.2.2 *"Medizinischer Steckbrief"*: Über diese Funktion hat der Nutzer die Möglichkeit medizinische Informationen in Form von einem medizinischen Steckbrief einzugeben (z.B. Informationen über (vorherige) Diagnosen, Medikation, Allergien und seinen Vitalzustand).

5.2.3 *"Termine"*: Diese Funktion bietet dem Nutzer die Möglichkeit, bei einer medizinischen Einrichtung einer Partnerklinik (z.B. ein Krankenhaus oder ein Medizinisches Versorgungszentrum) online einen Termin über die Avelios Dienste zu buchen. Hierfür hat der Nutzer insbesondere Angaben zur gewünschten Fachrichtung, zum Ort der Behandlung und Grund der Terminvereinbarung zu machen. Für den Abschluss des Buchungsvorgangs des/der gewünschten Arztes/Sprechstunde/Praxis/Gesundheitsdienstleisters und freien Termins ist ein Benutzerprofil im

Patientenportal erforderlich. Erst mit Anzeige einer Bestätigung im Avelios Portal ist der Termin vereinbart. Mit der Terminbuchung werden die Benutzerdaten an die gewünschte Einrichtung übermittelt.

Die behandelnde Gesundheitsfachkraft des jeweiligen Gesundheitsdienstleister kann dem Nutzer über die Avelios-Plattform nach Maßgabe unserer datenschutzrechtlichen vertraglichen Regelungen und auf Grundlage unseres Auftragsdatenverarbeitungsvertrages Benachrichtigungen

- für die Terminbestätigung, -stornierung oder -erinnerung;
- zur Information über etwaige Dokumentenübermittlung;
- zur Information über etwaige Terminänderungen
- und für sonstige Informationen, die zur Durchführung des jeweiligen Termines notwendig sind,

zusenden.

Termin-Stornierungsbedingungen richten sich nach den jeweiligen Vertragsbedingungen der Gesundheitsdienstleister.

5.2.4 *"Fragebögen"*: Diese Funktion bietet dem Nutzer die Möglichkeit terminspezifische Fragebögen auszufüllen, welche nach Befüllen an den medizinischen Leistungserbringer übermittelt werden.

5.2.5 *"Kommunikation"*: Diese Funktion bietet dem Nutzer die Möglichkeit, sofern der Gesundheitsdienstleister die Avelios Software nutzt und der Nutzer in den Informationsaustausch eingewilligt hat, über einen Chat verschlüsselt mit der medizinischen Einrichtung zu kommunizieren. Zudem bietet diese Funktion dem Nutzer die Möglichkeit einer Videosprechstunden-Kommunikation mit dem medizinischen Leistungserbringer an.

5.2.6 *„Videosprechstunde“*: Diese Funktion bietet dem Nutzer, sofern von dem Gesundheitsdienstleister angeboten, die Möglichkeit eine Gesundheitsdienstleistung über Videokonferenz als Ferndiagnose in Anspruch zu nehmen.

Für die Inanspruchnahme werden folgende Endgeräte/Leistungen benötigt:

- ein Smartphone oder ein internetfähiger Computer mit einer Kamera mit hinreichender Auflösung und
- eine ausreichend schnelle Internetverbindung.

Sollten diese technischen Voraussetzungen nicht vorliegen, kann der Gesundheitsdienstleister die Videosprechstunde beenden und dem Nutzer ggf. die Kosten für die durchgeführten Behandlungen in Rechnung stellen. Der Plattformanbieter Avelios dient lediglich als technischer Vermittler zwischen Nutzer und Gesundheitsdienstleister, der die Videokonferenz und den elektronischen Dokumentenversand ermöglicht.

Zum angegebenen und gebuchten Termin wird der Nutzer oder der teilnehmende Bevollmächtigte und vertretungsbefugte Angehörige gebeten, einige Minuten vor der Videosprechstunde an der Telekonferenz teilzunehmen, damit die Qualität der Audio- und Videoverbindung auf dem Smartphone oder dem Computer sichergestellt werden kann.

Bei der Herstellung der Verbindung für die Videosprechstunde (Beitritt) wird der Nutzer oder teilnehmende Angehörige dann in ein virtuelles Wartezimmer platziert, wobei die Wartedauer im Ermessen des Gesundheitsdienstleister als freigebendem Moderator liegt. Der Gesundheitsdienstleister startet dann die Videokonferenz. Avelios haftet nicht für Verzögerungen oder Stornierungen, die von dem Gesundheitsdienstleister verschuldet wurden.

Nutzungsregeln: Der Nutzer verpflichtet sich dazu, den Service unter Bedingungen zu nutzen, die es ihm ermöglichen, die Vertraulichkeit und den reibungslosen Ablauf des Austausches mit dem Gesundheitsdienstleister als Datenverarbeiter zu gewährleisten. Insbesondere muss der Nutzer sicherstellen, dass die Telekonsultation an einem sicheren Ort durchgeführt wird, um eine qualitativ hochwertige Konferenz zu ermöglichen.

Der Gesundheitsdienstleister ist allein befugt und verpflichtet, über die Geeignetheit einer Fernbehandlung des Nutzers zu entscheiden und kann, wenn die Bedingungen für eine Fernbehandlung nicht erfüllt sein sollten, diese abbrechen. Die Dauer einer Videosprechstunde unterliegt analog einer realen Sprechstunde dem Ermessen des Gesundheitsdienstleisters. Der Nutzer muss bei der Videosprechstunde den Anweisungen des Gesundheitsdienstleisters Folge leisten, damit eine optimale Behandlung und/oder Diagnose gewährleistet werden kann.

Die Gesundheitsdienstleister führen die Videosprechstunde unabhängig von Avelios und nach Maßgabe berufsrechtlicher und sonstiger gesetzlicher Bestimmungen durch.

Der Nutzer verpflichtet sich dazu, keine Inhalte oder Auszüge von Inhalten im Zusammenhang mit der Videosprechstunde aufzuzeichnen, zu kopieren oder zu verbreiten. Die Videosprechstunde wird weder vom Gesundheitsdienstleister noch von Avelios oder sonstigen Dritten aufgezeichnet.

6. Informationen gemäß Art.246 EGBGB

Informationen gemäß Art. 246 a § 1 EGBGB (Fernabsatzvertrag) und § 246 c EGBGB (Verträge im elektronischen Geschäftsverkehr).

6.1 Informationen gemäß Art. 246a § 1 EGBGB

Bei Fernabsatzverträgen über Dienstleistungen muss Avelios dem Nutzer bestimmte Informationen zukommen lassen. Dem kommt Avelios hiermit nach:

Wesentliche Merkmale der Dienstleistung: Verwendung von Webseite und Smartphone-App, als Patientenportal für den Aufenthalt oder Besuch bzw. die Inanspruchnahme von Gesundheitsdienstleistungen bei medizinischen Leistungserbringern.

Identität und öffentliches Register: Avelios Medical GmbH, Ridlerstraße 39

80339 München, Geschäftsführer: Christian Albrecht, Nicolas Jakob, Handelsregister München

HRB 270765, Tax-ID: DE334616294

Ladungsfähige Anschrift und Niederlassungsort: Avelios Medical GmbH, Ridlerstraße 39

80339 München, Deutschland

Erreichbarkeit über Telemedien: info@avelios.com

Gesamtpreis der Dienstleistung: Kosten entstehen nicht.

Zustandekommen des Vertrags: Der Vertrag kommt zustande, wenn man sich auf der Webseite oder in der App registriert.

Laufzeit: Der Vertrag läuft soweit und solange die Webseite bzw. App genutzt wird.

Beschwerdemanagement: Beschwerden können persönlich, telefonisch, schriftlich oder per E-Mail eingegeben werden und werden binnen 30 Tagen durch die Geschäftsführung geprüft und beantwortet.

Laufzeit des Vertrags, Mindestdauer: Der Vertrag kann von beiden Seiten jederzeit außerordentlich gekündigt werden. Eine ordentliche Kündigung ist darüber hinaus ebenfalls jederzeit möglich.

Außergerichtliche Beschwerdemöglichkeiten: Plattform der EU-Kommission zur Online-Streitbeilegung: www.ec.europa.eu/consumers/odr.

6.2 Informationen gemäß Art. 246c EGBGB

Technische Schritte, die zum Vertragsschluss führen: Man wird im Rahmen der Registrierung durch einen selbsterklärenden Prozess geführt. Dazu müssen zunächst persönliche Daten in die dafür vorgesehenen Felder eingefügt, und die Kenntnisnahme von Verbraucherinformationen bestätigt werden. Durch die Nutzung kommt der Nutzungsvertrag zustande.

Speichern des Vertragstexts: Der Vertragstext wird auf den internen Systemen des Anbieters gespeichert. Die Allgemeinen Geschäftsbedingungen kann der Nutzer jederzeit auf der Webseite oder in der App einsehen.

Vertragssprache: Für den Vertragsschluss steht die deutsche Sprache zur Verfügung.

Verhaltenskodizes, denen wir unterworfen sind: Es gibt keine Verhaltenskodizes, denen sich Avelios freiwillig unterworfen hat. Dessen ungeachtet unterliegt unsere Tätigkeit den allgemeinen Gesetzen.

Die Vertragsbestimmungen sind unter dem Stichwort "AGB" auf der Webseite des Patientenportals zu finden.

Informationen über Kundendienst und geltende Gewährleistungs- und Garantiebedingungen: Für die Haftung gelten die gesetzlichen Vorschriften.

Funktionsweise digitaler Inhalte: Sie werden im Rahmen der Registrierung durch einen selbsterklärenden Prozess geführt.

Ende der Informationen nach Art. 246 EGBGB

7. Widerrufsrecht, Erlöschen des Widerrufsrechtes durch sofortige Leistungserbringung

Verbraucher haben grundsätzlich das Recht, binnen vierzehn Tagen ohne Angabe von Gründen Fernabsatzverträge zu widerrufen.

Die Widerrufsfrist beträgt vierzehn Tage ab dem Tag des Vertragsabschlusses.

Um das Widerrufsrecht auszuüben, müssen Sie als Verbraucher uns mittels einer eindeutigen Erklärung (z.B. ein mit der Post versandter Brief oder eine E-Mail) über den Entschluss, diesen Vertrag zu widerrufen, informieren.

Dazu benötigen wir die Angabe von Nutzernamen, Geburtsdatum und E-Mail.

Zur Wahrung der Widerrufsfrist reicht es aus, dass Sie die Mitteilung über die Ausübung des Widerrufsrechtes vor Ablauf der Widerrufsfrist absenden.

Kontakt Daten: Avelios Medical GmbH, Ridlerstraße 39, 80339 München

E-Mail: info@avelios.com

Folgen des Widerrufs:

Wenn Sie diesen Vertrag widerrufen, wird das Vertragsverhältnis beendet.

Haben Sie konkludent verlangt, dass die Dienstleistung während der Widerrufsfrist beginnen soll, haben Sie keine Möglichkeit den Vertrag zu widerrufen, sofern wir die Dienstleistung bereits vollständig erbracht haben. Durch die sofortige Ausführung der Dienstleistung erlischt Ihr Widerrufsrecht.

Ihnen verbleibt jedoch weiterhin die Möglichkeit der Ordentlichen Kündigung.

Ausschluss des Widerrufsrechts: Das Widerrufsrecht gegenüber Avelios gilt nicht hinsichtlich solcher Verträge, die nicht zwischen dem Nutzer und Avelios, sondern zwischen dem Nutzer und einem Drittanbieter zu Stande kommen. Etwaige Widerrufsrechte können diesbezüglich nur gegenüber dem Drittanbieter geltend gemacht werden.

8. Pflichten der Nutzer

8.1 Das Patientenportal und die weiteren Dienste sind unter anderem auch eine Kommunikationsplattform, über die Personen Informationen austauschen, eigene Aussagen machen oder fremde Aussagen rezipieren. Die Einhaltung nachfolgender Verhaltensvorschriften und Nutzerpflichten ist unabdingbare Voraussetzung für das Funktionieren einer Kommunikationsplattform.

8.2 Der Nutzer ist verpflichtet, stets wahrheitsgemäße Angaben zu machen und die Daten hinsichtlich aller von ihm genutzten Dienste und Funktionen, insbesondere zu seinem Benutzerprofil und seiner Person, während der gesamten Nutzungszeit wahr und vollständig zu halten. Bei Zweifeln über die Identität des Nutzers behält sich Avelios vor, die Identität des Nutzers unter Übermittlung einer Kopie seines Personalausweises oder anderweitigen Ausweisdokumentes (z.B. Reisepass) zu überprüfen.

8.3 Es liegt im Verantwortungsbereich jedes einzelnen registrierten Nutzers, sicherzustellen, dass sämtliche Informations- und Aussageinhalte rechtmäßig sind, vor allem nicht gegen gesetzliche Verbote oder die guten Sitten verstoßen, keine Rechte Dritter einschließlich Persönlichkeitsrechte und Urheberrechte verletzen oder jugendgefährdend sind. Insbesondere ist es dem Nutzer untersagt,

- beleidigende, verleumderische oder volksverhetzende Inhalte zu verwenden,
- pornografische, gewaltverherrlichende oder gegen Jugendschutzgesetze verstoßende Inhalte zu verbreiten,
- gesetzlich (z. B. durch Urheber-, Marken- oder sonstige Schutzrechte) geschützte Inhalte zu verwenden, ohne dazu berechtigt zu sein, oder gesetzlich geschützte Waren oder Dienstleistungen zu bewerben, anzubieten oder zu vertreiben sowie

wettbewerbswidrige Handlungen vorzunehmen oder zu fördern, einschließlich progressiver Kundenwerbung.

8.4 Der Nutzer ist ferner verpflichtet, belästigende Handlungen zu unterlassen, auch wenn diese konkret keine Gesetze verletzen sollten. Insbesondere ist es den Nutzern untersagt, direkt oder indirekt politische und religiöse Anschauungen Dritter zu verletzen. Anzügliche oder sexuell geprägte Kommunikation in Schrift und Bild ist zu unterlassen. Die Verbreitung und öffentliche Wiedergabe von Inhalten über die Dienste und/oder von anderen Nutzern ist untersagt.

8.5 Dem Nutzer sind ferner jegliche Handlungen untersagt, die geeignet sind, die technische Funktionalität der von ihm genutzten Dienste zu beeinträchtigen, insbesondere diese übermäßig zu

belasten. Es ist verboten, die Dienste oder einzelne Nutzer über elektronischen Maßnahmen jedweder Art (einschließlich sämtlicher zum Betrieb des Patientenportals eingesetzter Hard- und Software) technisch oder inhaltlich zu stören, zu versuchen, Sicherheitsmechanismen zu umgehen, Daten jeglicher Art elektronisch oder manuell zu Missbrauchszwecken abzufangen oder sonstige Hacking-Versuche vorzunehmen.

8.6 Jeder Nutzer wird gebeten, Verstöße gegen diese Nutzungsbedingungen, insbesondere gegen die Pflichten dieser Ziffer 8, per E-Mail (datenschutz@avelios.com) an Avelios zu melden. Im Fall von Verstößen kann Avelios vom Nutzer eingestellte oder ihm sonst zuzuordnende Inhalte und Informationen entfernen oder den Zugang zu diesen Inhalten sperren und den Nutzer gegebenenfalls vorübergehend oder dauerhaft von der Nutzung des Patientenportals und damit der weiteren Dienste ausschließen.

8.7 Der Nutzer stellt Avelios von Ansprüchen, die andere Nutzer oder sonstige Dritte gegenüber Avelios geltend machen, insoweit frei, als diese Ansprüche auf einem schuldhaften Verstoß des Nutzers gegen die vorstehenden Pflichten beruhen. Die Freistellungsverpflichtung umfasst auch die angemessenen Kosten für die notwendige Rechtsverteidigung.

9. Schutzrechte und Rechteeinräumung

9.1 Die von Avelios im Rahmen der Dienste bereitgestellten Inhalte sind grundsätzlich urheber- bzw. leistungsschutzrechtlich geschützt. Avelios ist bestrebt, bei allen Inhalten die Urheberrechte der verwendeten Bilder, Grafiken, Tondokumente, Videosequenzen und Texte zu beachten, von ihr selbst erstellte Bilder, Grafiken, Tondokumente, Videosequenzen und Texte zu nutzen oder auf lizenzfreie Bilder, Grafiken, Tondokumente, Videosequenzen und Texte zurückzugreifen. Alle innerhalb des Patientenportals genannten und gegebenenfalls durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind. Das Copyright für veröffentlichte, selbst erstellte Inhalte liegt allein bei Avelios. Eine Vervielfältigung oder Verwendung solcher Bilder, Grafiken, Tondokumente, Videosequenzen und Texte in anderen elektronischen oder gedruckten Publikationen ist ohne ausdrückliche vorherige schriftliche Genehmigung durch Avelios nicht gestattet.

9.2 Mit der Nutzung der Dienste räumt der registrierte Nutzer Avelios unentgeltlich die nicht-ausschließlichen, zeitlich und räumlich unbeschränkten Rechte ein, die von ihm eingestellten Inhalte über alle im Rahmen des Patientenportals verwendeten Medien entsprechend den Zwecken des Patientenportals zu erheben, zu nutzen oder zu verarbeiten. Hiervon umfasst ist auch das Recht, die eingestellten Inhalte zu bearbeiten, um alle technisch erforderlichen Anpassungen (z.B. Änderung der Auflösung von Fotos und Videos) vorzunehmen.

9.3 Der Nutzer und die Partnerklinik garantieren, über alle erforderlichen Rechte an den von ihm eingestellten Inhalten zu verfügen. Für den Fall, dass Avelios von Dritten (eingeschlossen staatliche Institutionen) in Anspruch genommen wird wegen einer Verletzung von Urheber-, Nutzungs- oder sonstigen Leistungsschutzrechten Dritter an den Inhalten oder wegen einer Verletzung des allgemeinen Persönlichkeitsrechts oder des Rechts am eigenen Bild durch die Inhalte, wird der Nutzer Avelios von derartigen Ansprüchen Dritter freistellen und Avelios die angemessenen Kosten für die notwendige Rechtsverteidigung ersetzen.

10. Folgen einer Kündigung

Mit Ablauf der Kündigungsfrist werden sämtliche Daten und Inhalte, die der Nutzer auf bzw. in den Diensten eingestellt hat, vollständig gelöscht. Die Löschung aller Inhalte kann technisch bedingt eine gewisse Zeitspanne - maximal 48 Stunden - in Anspruch nehmen. Unberührt davon bleibt die längere Speicherung von Inhalten im Rahmen von gesetzlichen Vorhaltevorschriften. Zu diesem Zwecke ist Avelios befugt, Kopien der vertraulichen Informationen vorzuhalten, sofern dafür eine Ermächtigungsgrundlage und/oder gesetzliche Pflicht (z.B. Aufbewahrungsfristen) besteht.

11. Support

Der Nutzer kann sich im Falle von Problemen bei der Nutzung des Patientenportals per E-Mail (info@avelios.com) an den Support wenden. Avelios wird als Plattformbetreiber den Nutzer gelegentlich zu freiwilligen Nutzerzufriedenheits-Umfragen einladen, um die Qualität des dargebotenen Services zu bewerten und verbessern zu können.

12. Haftung

12.1 Die von Avelios im Rahmen der Dienste bereitgestellten Inhalte und Informationen werden durch die jeweiligen Partnerkliniken als Vertragspartner des Behandlungsvertrages zwischen Klinik und Patienten zusammengestellt und gepflegt. Dennoch kann ein fehlerfreies, vollständiges, aktuelles und jederzeit verfügbares Informationsangebot nicht garantiert werden. Bei Fehlern wenden Sie sich bitte unverzüglich an den verantwortlichen medizinischen Leistungserbringer.

Eine Haftung für eventuelle direkte oder indirekte Schäden materieller oder ideeller Art, die durch die Nutzung oder Nichtnutzung der dargebotenen Information verursacht wurden, ist gegenüber Avelios ausgeschlossen. Die Nutzung erfolgt ausschließlich auf eigenes Risiko des Nutzers, es sei denn, fehlerhafte Informationen wurden vorsätzlich oder grob fahrlässig aufgenommen. Eine solche Haftung richtet sich gegen den medizinischen Leistungserbringer als Vertragspartner.

12.2 Avelios übernimmt darüber hinaus keine Verantwortung für die von registrierten Nutzern bereitgestellten Inhalte und Informationen sowie für Inhalte auf verlinkten externen Websites. Avelios gewährleistet insbesondere nicht, dass diese Inhalte und Informationen wahr sind, einen bestimmten Zweck erfüllen oder einem solchen Zweck dienen können. Avelios haftet nicht für die Pflichtverletzung eines Nutzers gegenüber einer Partnerklinik aufgrund zwischen diesen geschlossenen Verträgen. Ein Vertrag mit Schutzwirkung zugunsten Dritter (Patienten) liegt mangels Schutzbedürftigkeit aufgrund der Partnerklinik als direkten Anspruchsgegner nicht vor.

12.3 Nach den gesetzlichen Bestimmungen ist Avelios nicht dazu verpflichtet, die übermittelten oder gespeicherten Inhalte und Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Sollte Avelios allerdings Kenntnis von der rechtswidrigen Handlung eines Nutzers oder einer Partnerklinik innerhalb des Patientenportals erlangen, werden die Informationen unverzüglich entfernt oder wird der Zugang zu diesen Inhalten gesperrt und der Nutzer oder die Partnerklinik gegebenenfalls vorübergehend oder dauerhaft von der Nutzung ausgeschlossen.

12.4 Die Haftung von Avelios und der jeweiligen Klinik ist auf Vorsatz und grobe Fahrlässigkeit beschränkt, soweit es sich nicht um die Verletzung einer vertragswesentlichen Pflicht oder die Verletzung des Lebens, des Körpers oder der Gesundheit handelt. Gleiches gilt für die Haftung der Erfüllungsgehilfen von Avelios und der jeweiligen Klinik. Unberührt bleibt die Haftung nach dem Produkthaftungsgesetz und für Garantieerklärungen.

12.5 Schadensersatzansprüche – gleich aus welchem Rechtsgrund – gegen Avelios (einschl. ihrer Erfüllungsgehilfen) bestehen nur, wenn eine wesentliche Vertragspflicht vorsätzlich oder fahrlässig verletzt worden ist. Wesentlich ist eine Vertragspflicht, wenn der Nutzer auf deren Einhaltung vertrauen durfte und deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht. Schadensersatzansprüche sind in diesem Fall der Höhe nach auf den typischen vorhersehbaren Schaden beschränkt. Es besteht keine Haftung für entgangenen Gewinn oder Einsparungen, Schäden aus Ansprüchen Dritter und sonstige mittelbare und unmittelbare Folgeschäden.

12.6 Ansprüche wegen Körperschäden sowie wegen Sachschäden nach dem Produkthaftungsgesetz bleiben unberührt. Die vorgenannten Haftungsausschlüsse und Beschränkungen gelten außerdem nicht im Fall der Übernahme von Garantien.

13. Datenschutz

Die Erhebung, Verarbeitung und Nutzung von personenbezogenen (Gesundheits-)Daten durch Avelios richtet sich nach den geltenden datenschutzrechtlichen Bestimmungen und der Datenschutzerklärung für das Patientenportal.

14. Änderungen der Nutzungsbedingungen und der Dienste

14.1 Avelios behält sich vor, die angebotenen Dienste zu ändern, zu beenden oder abweichende Dienste anzubieten, außer dies ist für den Nutzer nicht zumutbar. Avelios behält sich darüber hinaus vor, die angebotenen Dienste zu ändern, zu beenden oder abweichende Dienste anzubieten,

- soweit Avelios verpflichtet ist, die Übereinstimmung der von Avelios angebotenen Dienste mit dem auf die Dienste anwendbaren Recht herzustellen, insbesondere wenn sich die geltende Rechtslage ändert;
- soweit Avelios damit einem gegen Avelios gerichteten Gerichtsurteil oder einer Behördenentscheidung nachkommt;
- soweit die jeweilige Änderung notwendig ist, um bestehende Sicherheitslücken zu schließen;
- wenn die Änderung lediglich vorteilhaft für den Nutzer ist; oder
- wenn die Änderung rein technischer oder prozessualer Natur ohne wesentliche Auswirkungen für den Nutzer ist.

Änderungen mit lediglich unwesentlichem Einfluss auf die Dienste oder deren Funktionen stellen keine Änderung im Sinne dieser Ziffer dar. Dies gilt insbesondere für Änderungen rein graphischer Art und die bloße Änderung der Anordnung von Diensten und/oder Funktionen.

14.2 Avelios behält sich vor, diese Nutzungsbedingungen jederzeit ohne Nennung von Gründen zu ändern, es sei denn, dies ist für den Nutzer nicht zumutbar. Avelios wird den Nutzer über Änderungen der Nutzungsbedingungen rechtzeitig benachrichtigen. Widerspricht der Nutzer der Geltung der neuen Nutzungsbedingungen nicht innerhalb von sechs (6) Wochen nach der Benachrichtigung, gelten die geänderten Nutzungsbedingungen als vom Nutzer angenommen. Avelios wird den Nutzer in der Benachrichtigung auf sein Widerspruchsrecht und die Bedeutung der Widerspruchsfrist hinweisen. Avelios behält sich darüber hinaus vor, Nutzungsbedingungen zu ändern,

- wenn die Änderung lediglich vorteilhaft für den Nutzer ist;
- wenn die Änderung rein technisch oder prozessual bedingt ist, es sei denn, sie haben wesentliche Auswirkungen für den Nutzer;

- soweit Avelios verpflichtet ist, die Übereinstimmung der Nutzungsbedingungen mit anwendbarem Recht herzustellen, insbesondere wenn sich die geltende Rechtslage ändert;
- soweit Avelios damit einem gegen Avelios gerichteten Gerichtsurteil oder einer Behördenentscheidung nachkommt; oder
- soweit Avelios zusätzliche, gänzlich neue Dienstleistungen, Dienste oder Dienstelemente einführt, die einer Leistungsbeschreibung in den Nutzungsbedingungen bedürfen, es sei denn, dass bisherige Nutzungsverhältnis wird dadurch nachteilig verändert.

Avelios wird über solche Änderungen der Nutzungsbedingungen informieren, zum Beispiel per E-Mail.

14.3 Das Kündigungsrecht des Nutzers nach Ziff. 6 bleibt von etwaigen Änderungen der Dienste oder Nutzungsbedingungen nach dieser Vorschrift unberührt.

15. Schlussbestimmungen

15.1 Für den Fall, dass

der Nutzer seinen Wohnsitz oder gewöhnlichen Aufenthaltsort nicht in dem Geltungsbereich der Zivilprozessordnung (ZPO) - Inland - hat oder

- der Nutzer nach Abschluss dieses Nutzungsvertrages seinen Wohnsitz oder gewöhnlichen Aufenthaltsort ins Ausland verlegt oder
- der Wohnsitz oder gewöhnliche Aufenthaltsort des Nutzers zum Zeitpunkt einer gerichtlichen Geltendmachung von Ansprüchen nicht bekannt ist,

wird München (Deutschland) als Gerichtsstand vereinbart.

Bei sämtlichen Ansprüchen aus diesem Vertrag gilt deutsches Recht.

15.2 Sollte eine Bestimmung dieser Nutzungsbedingungen oder eine später in ihnen aufgenommene Bestimmung ganz oder teilweise nichtig sein oder werden oder sollte sich eine Lücke in diesen Nutzungsbedingungen oder seinen Ergänzungen herausstellen, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Den Parteien ist die Rechtsprechung des Bundesgerichtshofs bekannt, wonach eine salvatorische Erhaltungsklausel lediglich die Beweislast umkehrt. Es ist jedoch der ausdrückliche Wille der Parteien, die Wirksamkeit der übrigen Nutzungsbestimmungen unter allen Umständen aufrechtzuerhalten und damit § 139 BGB insgesamt abzubedingen. Anstelle der nichtigen Bestimmung oder zur Ausfüllung der Lücke ist diejenige wirksame und durchführbare Regelung zu vereinbaren, die rechtlich und wirtschaftlich dem am nächsten kommt, was die Parteien gewollt haben oder nach dem Sinne und Zweck der Nutzungsbedingungen und ihrer späteren eventuellen Ergänzungen gewollt hätten, wenn sie diesen Punkt beim Abschluss des Vertrages bedacht hätten. Beruht die Nichtigkeit einer Bestimmung auf einem darin festgelegten Maß der Leistung oder der Zeit (Frist oder Termin), so ist die Bestimmung mit einem dem ursprünglichen Maß am nächsten kommenden rechtlich zulässigen Maß zu vereinbaren.

15.3 Webseiten Dritter: Avelios ist nicht verantwortlich für den Betrieb, die Qualität der Informationen und den Inhalt von Webseiten Dritter, die nicht der Kontrolle von Avelios unterstehen, aber auf welche von den Services des Patientenportals verwiesen wird und auf welchen auf das Patientenportal von Avelios verwiesen wird.

15.4 Sind seit dem letzten Zugriff des Nutzers auf sein Nutzerkonto mehr als drei Jahre vergangen, behält sich Avelios vor, das Nutzerkonto einschließlich der gespeicherten (Gesundheits-)Daten zu löschen, wenn der Nutzer nicht innerhalb von weiteren sechs Wochen auf dieses zugreift. Hierauf wird

der Nutzer zuvor per E-Mail hingewiesen. Die E-Mail wird an die vom Nutzer zuletzt bekannte E-Mail-Adresse versandt.

Datenschutzerklärung

der Avelios Medical GmbH

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

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

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 unbekannten 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 and 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

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

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).

VEREINBARUNG ZUR AUFTRAGSDATENVERARBEITUNG

Zwischen der

Avelios Medical GmbH

Ridlerstraße 39

80339 München, Deutschland

(„nachfolgend als **Verantwortlicher** bezeichnet“)

Und

-hier bitte ihren jeweiligen Vertragspartner (jede Klinik) eintragen-

(„nachfolgend als **Auftragsverarbeiter** bezeichnet“)

(Verantwortlicher und Auftragsverarbeiter, jeweils eine „Partei“ und gemeinsam die „Parteien“)

Präambel

Der Auftragsverarbeiter ist ein Beauftragter des Verantwortlichen, der im Rahmen eines Vertrages („Hauptvertrag“) Leistungen aus dem Gesundheitsbereich („Hauptleistungen“) an den Verantwortlichen bzw. an dessen Nutzern erbringt.

Zur Erbringung der Hauptleistungen hat der Auftragsverarbeiter Zugriff auf Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen („Personenbezogene Gesundheitsdaten“), des Verantwortlichen oder erhebt und verarbeitet diese im Auftrag des Verantwortlichen. Diese Vereinbarung zur Auftragsverarbeitung („Vereinbarung“) regelt den Umgang des Auftragsverarbeiters mit diesen personenbezogenen Gesundheits- und Nutzerdaten. Der Gesundheitsdienstleister erhebt die personenbezogenen Daten vornehmlich zur eignen Vertragsabwicklung und Erfüllung. Im Verhältnis zum Verantwortlichen als Serviceplattformdienstleister erhebt er die Daten jedoch als Auftragsdatenverarbeiter (Befüllen des Nutzerkontos etc.)

A. Umfang, Art und Zweck der Auftragsverarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene (Gesundheits-)Daten nur im Auftrag und nach Weisungen des Verantwortlichen gemäß Art. 28 EU Datenschutzgrundverordnung (DSGVO). Der Auftragsverarbeiter darf personenbezogene Daten ferner nur erheben, verarbeiten oder nutzen, soweit dies zur Erbringung der eigenen Hauptleistungen an seine Patienten bzw. die Nutzer des Verantwortlichen erforderlich ist, es sei denn eine Weisung des Verantwortlichen geht hierüber hinaus.

Der Verantwortliche wird dem Auftragsverarbeiter nur Daten zur Verfügung stellen oder zugänglich machen, wenn die Rechtmäßigkeit der Verarbeitung nach Art. 6 DSGVO gegeben ist. Der Auftragsverarbeiter hat sicherzustellen, dass er die personenbezogenen Gesundheitsdaten seiner Patienten rechtmäßig und durch Einwilligung erhoben hat.

Die Weisungen des Verantwortlichen sind durch den Auftragsverarbeiter zu dokumentieren. Dies erfolgt entweder, indem der Verantwortliche die Weisungen in Textform erteilt, oder – falls der Verantwortliche die Weisungen nur mündlich erteilt – indem der Auftragsverarbeiter die Weisungen an den Verantwortlichen unverzüglich nach den Weisungen in Textform bestätigt.

Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen anwendbare Datenschutzvorschriften verstößt, hat der Auftragsverarbeiter den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter kann die Ausführung der Anweisung bis zu einer Bestätigung durch den Verantwortlichen aussetzen.

Zweck der Auftragsverarbeitung ist es, dass der Auftragsverarbeiter auf die Daten zugreifen kann, die zur Erbringung der Hauptleistungen an seine Patienten aus dem jeweiligen Behandlungsvertrag erforderlich sind, wie dies im Hauptvertrag zwischen den Parteien bzw. nach Gesetzesrecht (Behandlungsvertrag) näher beschrieben ist. Die Verarbeitung erfolgt in automatisiertem Verfahren auf IT-Systemen des Auftragsverarbeiters oder auf IT-Systemen des Verantwortlichen. Die Verarbeitung personenbezogener Gesundheits-Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen, findet ausschließlich innerhalb der Europäischen Union oder innerhalb des Europäischen Wirtschaftsraums statt. Jegliche Übermittlung Personenbezogener Daten an ein Land außerhalb der Europäischen Union oder außerhalb des Europäischen Wirtschaftsraums, erfordert die vorherige schriftliche Zustimmung des Verantwortlichen. Für alle Subunternehmer, deren Einschaltung der Auftraggeber zugestimmt hat, gilt die Zustimmung für die Datenverarbeitung in Drittländern ebenfalls als erteilt, sofern der Verantwortliche über die Datenverarbeitung in Drittländern informiert wurde und die besonderen Voraussetzungen des Art. 44 ff DSGVO erfüllt sind. Dies umfasst die in Anlage 2 aufgeführten Subunternehmer und solche deren Einschaltung der Verantwortliche nicht innerhalb von 4 Wochen nach Unterrichtung widersprochen hat.

Daten des Verantwortlichen werden vom Auftragsverarbeiter verarbeitet, um die Hauptleistungen nach dem Hauptvertrag zu erbringen.

B. Art der Daten und der Kreis der Betroffenen

I. Der Auftragsverarbeiter verarbeitet folgende Art der Daten:

- Berufliche Kontaktinformationen (z.B.: Name, E-Mail-Adresse, Telefonnummer, Position im Unternehmen) von Beschäftigten des Verantwortlichen
- Personenbezogene Gesundheits-Daten (z.B. Gesundheitsfragebögen, Arztbriefe, radiologische Bildaufnahmen, etc.)

II. Kreis der Betroffenen:

- Patienten des Auftragsverarbeiters

C. Pflichten des Auftragsverarbeiters

Erfolgt die Verarbeitung auf IT-Systemen des Auftragsverarbeiters, wird der Auftragsverarbeiter in seinem Verantwortungsbereich die erforderlichen technischen und organisatorischen Maßnahmen

(TOMs) treffen, um für die Personenbezogenen Daten des Verantwortlichen ein angemessenes Schutzniveau zu gewährleisten. Insbesondere wird der Auftragsverarbeiter seine innerbetriebliche Organisation so gestalten, dass er den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragsverarbeiter wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Verantwortlichen vor Missbrauch und Verlust treffen, die den Anforderungen des anwendbaren Datenschutzrechts entsprechen. Dies umfasst mindestens die technischen und organisatorischen Maßnahmen.

Der Verantwortliche bestätigt, dass die technischen und organisatorischen Maßnahmen für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten, und stimmt diesen zu.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

Erfolgt die Verarbeitung auf IT-Systemen des Verantwortlichen ist der Auftragsverarbeiter verpflichtet diese nur gemäß den Weisungen des Verantwortlichen einzusetzen. Der Verantwortliche wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Verantwortlichen vor Missbrauch und Verlust treffen, die den Anforderungen des anwendbaren Datenschutzrechts entsprechen.

Hinsichtlich der Berichtigung, Löschung und Sperrung von Personenbezogenen Gesundheits-Daten hat der Auftragsverarbeiter die Weisungen des Verantwortlichen zu befolgen. Vor einer Berichtigung, Löschung oder Sperrung von Personenbezogenen Daten hat der Auftragsverarbeiter den Verantwortlichen hierüber rechtzeitig zu informieren; der Auftragsverarbeiter wird dann die daraufhin vom Verantwortlichen gegebenenfalls erteilten Weisungen befolgen.

Auf Anfrage des Auftraggebers stellt der Auftragsverarbeiter dem Verantwortlichen alle Angaben zur Verfügung, die zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten benötigt werden.

Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Personenbezogenen Daten des Verantwortlichen befugten Mitarbeiter auf das Datengeheimnis und die Vertraulichkeit verpflichtet haben und in die Schutzbestimmungen des anwendbaren Datenschutzrechts eingewiesen werden.

Der Auftragsverarbeiter hat einen Datenschutzbeauftragten benannt: **-bitte jeweils ergänzen-**

Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich über einen Wechsel des Datenschutzbeauftragten informieren. Im Rahmen der Datenverarbeitung etwaig angefallenes Test- und Ausschussmaterial wird vom Auftragsverarbeiter unter Verschluss aufbewahrt. Der Auftragsverarbeiter wird vorbehaltlich etwaiger Weisungen des Verantwortlichen die Materialien entweder dem Verantwortlichen zur Verfügung stellen oder unter Aufsicht und gemäß den Weisungen des Verantwortlichen vernichten.

Gegebenenfalls ist es für die Erfüllung der im Hauptvertrag beschriebenen Dienstleistungen erforderlich, dass der Auftragsverarbeiter Daten über soziale Netzwerke, Plattformen oder ähnliche Technologien, wie z.B. Facebook verarbeitet. Zu diesem Zweck und soweit zutreffend, ermächtigt der Verantwortliche den Auftragsverarbeiter hiermit, die Richtlinien, Bedingungen und andere Rechtstexte, die die Nutzung der genannten sozialen Netzwerke, Plattformen oder ähnlichen Technologien regeln, in seinem Namen und in seinem Auftrag zu akzeptieren.

Der Auftragsverarbeiter wird den Verantwortlichen dabei unterstützen, seinen Pflichten gegenüber den betroffenen Personen nachzukommen.

Dies gilt insbesondere im Fall, wenn der Verantwortliche gegenüber einer Einzelperson verpflichtet ist, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten dieser Person zu geben. Dann wird der Auftragsverarbeiter den Verantwortlichen dabei unterstützen, diese Informationen bereit zu stellen. Ist der Verantwortliche gegenüber einer Einzelperson verpflichtet, Kopien seiner/ihrer Daten bereitzustellen oder deren Übermittlung zu ermöglichen, wird der Auftragsverarbeiter alle benötigten Daten im erforderlichen Format für den Verantwortlichen vorbereiten, so dass es dem Verantwortlichen möglich ist, der Anfrage der betroffenen Person nachzukommen. Sollte die Unterstützung für den Auftragsverarbeiter unverhältnismäßig oder unzumutbar sein oder werden, trägt der Verantwortliche alle damit verbundenen Kosten. Entsprechende Anfragen Betroffener an den Auftragsverarbeiter hat der Auftragsverarbeiter an den Verantwortlichen zur Beantwortung weiterzureichen bzw. wie vom Verantwortlichen jeweils angewiesen zu beantworten.

Der Auftragsverarbeiter wird ferner den Verantwortlichen bei der Einhaltung der folgenden Pflichten unterstützen:

- Einschätzung des erforderlichen Schutzniveaus für die Sicherheit der Verarbeitung und Implementierung der geeigneten technischen und organisatorischen Maßnahmen.
- Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde,
- Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, und
- Datenschutz-Folgenabschätzung und vorherige Konsultation der Aufsichtsbehörden.

Insbesondere, wenn der Auftragsverarbeiter von einer Verletzung der Sicherheit Kenntnis bekommt, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu Personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden („Verletzung des Schutzes Personenbezogener Daten“), wird der Auftragsverarbeiter den Verantwortlichen unverzüglich benachrichtigen, wobei die entsprechende Benachrichtigung mindestens die folgenden Informationen und Vorschläge enthalten muss:

- (a) eine Beschreibung der Art der Verletzung des Schutzes Personenbezogener Daten, einschließlich der Kategorien und der ungefähren Anzahl der betroffenen Personen;
- (b) die Namen und Kontaktdaten der Kontaktperson beim Auftragsverarbeiter, von dem weitere Informationen erhältlich sind;
- (c) eine Beschreibung der im Zusammenhang mit der Verletzung des Schutzes Personenbezogener Daten ergriffenen oder vorgesehenen Maßnahmen, einschließlich Maßnahmen zur Minimierung möglicher, daraus resultierender nachteiliger Auswirkungen; und
- (d) einen Vorschlag für eine vorläufige, sofort umsetzbare Lösung zum Umgang mit der Verletzung des Schutzes Personenbezogener Daten, um weitere nachteilige Folgen für die betroffene Person und den Verantwortlichen zu vermeiden.

Wenn und soweit es nicht möglich ist, alle Informationen über die Datenverletzung unmittelbar bereitzustellen, können die Informationen ohne unangemessene weitere Verzögerung in Phasen bereitgestellt werden.

Der Auftragsverarbeiter wird in enger Zusammenarbeit mit dem Verantwortlichen sämtliche Maßnahmen ergreifen, die zur Sicherung der Daten und zur Begrenzung etwaiger nachteiliger Auswirkungen für die betroffenen Personen erforderlich sind. Sofern die Verletzung auf eine in diesem Vertrag geregelte Datenverarbeitung zurückzuführen ist, die der Auftragsverarbeiter zu verantworten

hat, wird der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung etwaiger Pflichten, die ihm gemäß geltenden datenschutzrechtlichen Bestimmungen obliegen, unterstützen. Die Parteien vereinbaren, sich hinsichtlich des Inhalts etwaiger öffentlicher Erklärungen hinsichtlich einer Verletzung des Schutzes Personenbezogener Gesundheits-Daten sowie etwaiger in diesem Zusammenhang erforderlicher Mitteilungen an die jeweils betroffenen Personen und/oder zuständigen Aufsichtsbehörden in gutem Glauben abzustimmen.

Darüber hinaus wird der Auftragsverarbeiter den Verantwortlichen unverzüglich informieren, wenn die Sicherheit der Personenbezogenen Daten des Verantwortlichen auf Seiten des Auftragsverarbeiters aufgrund einer Pfändung, Beschlagnahme, Zahlungsunfähigkeit, Insolvenzmaßnahmen oder sonstigen Maßnahmen Dritter gefährdet ist. In solchen Fällen wird der Auftragsverarbeiter alle Dritten davon in Kenntnis setzen, dass die Personenbezogenen Daten alleiniges Eigentum des Verantwortlichen sind.

D. Kontrollrechte

Der Verantwortliche kann sich (i) nach rechtzeitiger Anmeldung, wenigstens jedoch zehn (10) Werktagen im Voraus, (ii) zu den üblichen Geschäftszeiten und (iii) ohne den Betriebsablauf beim Auftragsverarbeiter zu stören, zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters von der Einhaltung der technischen und organisatorischen Maßnahmen und der für die Auftragsverarbeitung einschlägigen Datenschutzgesetze entweder selbst oder, sollte der Auftragsverarbeiter dies verlangen, durch einen zur Verschwiegenheit verpflichteten Dritten überzeugen. Der Auftragsverarbeiter hat das Recht einen beauftragten Prüfer abzulehnen, wenn dieser in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht. Dem Auftragsverarbeiter wird im Falle der Beauftragung eines Prüfers eine Kopie des Prüfberichtes auf Anfrage zur Verfügung gestellt. Die Kosten für die Beauftragung einer Prüfung durch einen Dritten trägt der Verantwortliche.

Der Auftragsverarbeiter hat diese Prüfungen zu dulden und wird an der Prüfung mitwirken. Der Auftragsverarbeiter wird dem Verantwortlichen auf Anforderung alle Auskünfte geben, die zur Durchführung einer umfassenden Auftragskontrolle erforderlich sind. Der Auftragsverarbeiter ist jedoch nicht verpflichtet, im Rahmen von Prüfungen Betriebs- und Geschäftsgeheimnisse, betriebliches Know-how und anderweitig gesetzlich geschützte Daten, wie etwa Daten anderer Leistungsempfänger, offenzulegen; solche Informationen können vor Offenlegung der Dokumente geschwärzt werden. Sollte die Unterstützung für den Auftragsverarbeiter unverhältnismäßig oder unzumutbar sein oder werden, trägt der Verantwortliche alle damit verbundenen Kosten.

Wird im Rahmen einer Kontrolle festgestellt, dass die Verarbeitung beim Auftragsverarbeiter gegen anwendbare Vorschriften über den Datenschutz verstößt, wird der Auftragsverarbeiter die Verarbeitung unverzüglich so ändern, dass diese Vorschriften künftig eingehalten werden, und den Weisungen des Verantwortlichen hierzu nachkommen.

Die Kontrollrechte des Verantwortlichen bestehen während der Laufzeit dieser Vereinbarung.

E. Subunternehmer

Der Verantwortliche genehmigt hiermit, dass der Auftragsverarbeiter Aufträge an Subunternehmer vergibt, die Zugriff auf Personenbezogene Daten des Verantwortlichen nehmen können, wenn die Voraussetzungen dieser Ziffer 6 eingehalten werden. Der Unterauftrag mit dem Subunternehmer ist

ebenfalls als Auftragsverarbeitung auszugestalten und muss den wesentlichen Anforderungen dieser Vereinbarung mindestens entsprechen.

Der Auftragsverarbeiter hat den Verantwortlichen von der Datenverarbeitung durch den Subunternehmer schriftlich und vor Beginn der Verarbeitung zu informieren. Des Weiteren sind dem Verantwortlichen auf Verlangen des Verantwortlichen Informationen über den Subunternehmer, Informationen über die (beabsichtigte) Beauftragung sowie Informationen über die getroffenen technischen und organisatorischen Maßnahmen auszuhändigen. Der Verantwortliche erteilt seine Zustimmung zu den in Anlage 2 aufgeführten Unterauftragnehmern des Auftragsverarbeiters.

Die Zustimmung zum Einsatz eines Subunternehmers gilt auch als erteilt, wenn der Verantwortliche nicht innerhalb von 4 Wochen nach Unterrichtung widersprochen hat.

Der Verantwortliche kann der Beauftragung von Subunternehmern aus wichtigem Grund widersprechen, insbesondere wenn er der Meinung ist, dass die technischen und organisatorischen Maßnahmen des Subunternehmers nicht ausreichen sollten. In diesem Fall hat der Zugriff des Subunternehmers auf Personenbezogene Daten des Verantwortlichen zu unterbleiben. Der Verantwortliche darf seine Zustimmung zur Beauftragung eines Subunternehmers nicht unbillig verweigern.

Nicht als Subunternehmer im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern.

F. Vorgangsdauer, Dauer der Auftragsverarbeitung, Überlassene Datenträger und Löschung gespeicherter Daten

Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft und wird auf unbestimmte Zeit geschlossen. Der Verantwortliche kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters oder eines Unterauftragsverarbeiters gegen datenschutzrechtliche Vorschriften oder gegen diese Vereinbarung vorliegt.

Die Auftragsverarbeitung beginnt und endet mit der Erbringung der Hauptleistungen gegenüber den Nutzern des Verantwortlichen.

Überlassene Datenträger sowie sämtliche hiervon gefertigte Kopien verbleiben im Eigentum des Verantwortlichen. Der Auftragsverarbeiter hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragsverarbeiter wird dem Verantwortlichen jederzeit Auskünfte über seine Daten und Unterlagen erteilen.

Nach Beendigung der Auftragsverarbeitung gibt der Auftragsverarbeiter dem Verantwortlichen alle überlassenen Datenträger und etwaige Kopien zurück. Der Auftragsverarbeiter wird darüber hinaus alle noch verbliebenen Personenbezogenen Daten nach Wahl des Verantwortlichen entweder zurückgeben, oder sicher und dauerhaft löschen. Unberührt bleiben Daten, deren Löschung aus technischen Gründen nicht möglich ist oder einen unverhältnismäßig hohen Aufwand verursachen würde, sowie Kopien, die zum Nachweis der Ordnungsmäßigkeit der Datenverarbeitung oder zur Erfüllung von Haftungs- und Gewährleistungsansprüchen erforderlich sind.

Die Rückgabe von Daten kann auch durch eine Übertragung von Zugriffsrechten für Drittanbieter-Systeme, in denen personenbezogene Daten des Verantwortlichen verarbeitet werden, erfolgen. Der Auftragsverarbeiter stellt sicher, dass nach der Übertragung der Zugriffsrechte an den

Verantwortlichen kein Zugriff durch den Auftragsverarbeiter mehr möglich ist und die Zugriffsrechte durch den Auftragsverarbeiter auch nicht wiederhergestellt werden können. Der Verantwortliche bestätigt dem Auftragsverarbeiter die Übertragung.

Der Verantwortliche stimmt zu, dass berufliche Kontaktdaten und Kommunikationsdaten von Mitarbeitern des Verantwortlichen auch über die Beendigung der Hauptleistung hinaus gespeichert werden, um Weisungen (inkl. Freigaben und Briefings) zu dokumentieren.

Sofern für den Auftragsverarbeiter eine gesetzliche Verpflichtung besteht, die die Rückgabe oder Zerstörung der Daten (ganz oder teilweise) untersagt oder einschränkt, wird der Auftragsverarbeiter den Verantwortlichen unverzüglich darüber informieren und dem Verantwortlichen alle für ihn notwendigen Informationen zur Verfügung stellen, um beurteilen zu können, ob eine Zerstörung oder Rückgabe möglich ist und wenn ja, zu welchen Bedingungen.

G. Drittansprüche

Für den Ersatz von Schäden, die betroffene Personen wegen einer Verletzung des Schutzes personenbezogener Daten nach dem BDSG oder der DSGVO im Rahmen des Vertragsverhältnisses erleiden, haften Verantwortlicher und Auftragsverarbeiter entsprechend der in Art. 82 DSGVO getroffenen Regelung.

Der Auftragsverarbeiter muss den Verantwortlichen unverzüglich schriftlich benachrichtigen, sobald der Auftragsverarbeiter von einem möglichen Anspruch Dritter Kenntnis erlangt, der mit der Verarbeitung Personenbezogener Daten des Verantwortlichen durch den Auftragsverarbeiter zusammenhängt („Drittanspruch“).

Der Verantwortliche wird innerhalb von sieben (7) Werktagen nach Zugang der schriftlichen Benachrichtigung den Auftragsverarbeiter schriftlich informieren, ob der Verantwortliche die Führung der Verteidigung übernimmt und auf den Drittanspruch antworten wird. In diesem Fall wird der Auftragsverarbeiter dem Verantwortlichen alle Materialien, Informationen und Unterstützung in Bezug auf den Drittanspruch zukommen lassen. Der Verantwortliche wird keinem Vergleich ohne die vorherige schriftliche Zustimmung des Auftragsverarbeiters zustimmen (wobei diese Zustimmung nicht ungerechtfertigt verweigert werden darf).

Wenn der Verantwortliche verhindert ist oder es ablehnt, die Führung der Verteidigung wie unter G Absatz 3 beschrieben zu übernehmen, kann der Auftragsverarbeiter die Führung der Verteidigung des Drittanspruchs übernehmen, jedoch vorausgesetzt, dass der Verantwortliche auf eigene Kosten an der Verteidigung teilnehmen kann.

H. Schlussbestimmungen

Änderungen, Ergänzungen und die Aufhebung dieser Vereinbarung bedürfen der Schriftform oder der qualifizierten elektronischen Signatur. Gleiches gilt für eine Änderung oder Aufhebung des Schriftformerfordernisses.

Alleiniger Gerichtsstand für alle Streitigkeiten aus und in diesem Zusammenhang mit dieser Vereinbarung ist München, soweit kein ausschließlicher Gerichtsstand begründet ist.

Im Fall von Widersprüchen zwischen dieser Vereinbarung und Regelungen aus anderen Verträgen der Parteien, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus dieser Vereinbarung vor.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Ortsdatum und Unterschrift:

Name, Funktionsbezeichnung
(Verantwortlicher)

Name, Funktionsbezeichnung
(Auftragsverarbeiter)

Anlage 1

Technisch Organisatorische Maßnahmen der Klinik xy

(Version 15.9.2021)

Hintergrund

Die Unternehmen der Beispiel Media Group bieten Dienstleistungen aus dem Bereich Mediaplanung an. Diese umfassen das gesamte Spektrum von Analyse, Strategie, Planung über Verhandlung, Einkauf, Optimierung bis zur Umsetzung, Erfolgskontrolle und Reporting.

In diesem Zusammenhang werden auch persönliche Daten verarbeitet. Wir nehmen den Schutz der verarbeiteten Daten sehr ernst, insbesondere wenn uns diese Daten im Rahmen eines Auftragsverarbeitungsvertrages zur Verfügung gestellt wurden.

Um dies sicher zu stellen haben wir verschiedene technische und auch organisatorische Maßnahmen implementiert.

1. Vertraulichkeit

1.1 Zutrittskontrolle

- Rechenzentrum an externen Standorten (Frankfurt am Main und Berlin) mit ISO 27001 Zertifizierung
- Zutrittsbeschränkung über Schlüsselvergabe (oder Schlüsselkarten oder Transponder) an Mitarbeiter
- Anmeldung von Besuchern am Empfang
- Kameraüberwachung mit Aufzeichnung in den Zugangsbereichen (Gebäudeeingangstüren und Tiefgarage)
- Zusätzliche Zutrittssicherung in sensiblen Bereichen (HR, IT, Geschäftsführung und Archiv). Zutritt erhalten nur Mitarbeiter aus den entsprechenden Bereichen.
- Sperrung von Schlüsselkarten und Transpondern bei Verlust
- Protokollierte Vergabe der Schlüssel, Schlüsselkarten und Transponder

1.2 Zugangskontrolle

- Jeder Computer ist durch Bitlocker gesichert. PIN-Eingabe zum Start des Computers erforderlich.
- BIOS durch Admin Passwort gesichert
- Mitarbeiter müssen sich mit einem persönlichen Account und Passwort authentifizieren
- Erzwungene Passworrichtlinie (mindestens 8 Zeichen, Sonderzeichen, keine bereits verwendeten Passwörter, kein Zusammenhang mit Namen)
- Sperrung des Accounts nach 5 fehlgeschlagenen Anmeldeversuchen
- Automatische Sperrung Computers nach Inaktivität des Nutzers
- Rechtevergabe über Active Directory
- Fernzugriff nur über gesicherte VPN-Verbindung mit Zwei-Faktor-Anmeldung
- Sicherung durch Firewall. Regelmäßige Überprüfung der Firewallprotokolle
- Einsatz von Virens Scanner auf allen Computern
- Zentrale Überprüfung der Aktualität von Zugangs- und Sicherungssoftware durch IT-Abteilung
- Physikalisch getrenntes WLAN für Besucher

1.3 Zugriffskontrolle

- Zentrale Administration der Zugriffsrechte (Laufwerke, Verzeichnisse, Dateien) über IT-Abteilung nach Freigabe durch Fachverantwortliche
- Separate Administrationsaccount für Verwaltung der Zugriffsrechte
- Sofern möglich, Zugriff über Single Sign On
- Zugriffsberechtigungen werden nach Aufgaben der Mitarbeiter vergeben
- Beschränkter Zugriff auf BackUps durch IT-Abteilung
- Verpflichtung von Mitarbeitern, nur von der IT-Abteilung geprüfte und freigegebene temporäre USB-Speichermedien zu verwenden

1.4 Pseudonymisierung

- Empfang und Weitergabe von persönlichen Daten, falls unter Berücksichtigung des jeweiligen Verarbeitungszwecks möglich, nur anonymisiert oder pseudonymisiert

1.5 Trennungsgebot

- Mandantentrennung auf Verzeichnisebene. Falls erforderlich getrennte logische Laufwerke für Mandanten
- Mitarbeiter erhalten nur auf für Ihre Arbeitsbereiche relevante Daten Zugriff
- Anwendungsdatenbanken (z.B.: Media-Einkauf, Finanzbuchhaltung, Zeiterfassung, Adserver, usw.) sind auf Datenbankinstanz- oder Datenbankserverebene getrennt.

2. Integrität

2.1 Weitergabekontrolle

- Verpflichtung der Mitarbeiter auf:
 - Einschränkung der Datenweitergabe
 - Persönliche oder sensible Daten werden vor Übertragung per E-Mail verschlüsselt bzw. mit einem Passwort geschützt
 - Es werden nur von der IT geprüfte Speichermedien verwendet
 - Persönliche und sensible Daten sind in den bereitgestellten Aktenvernichtern zu schreddern oder in den für Datenvernichtung vorgesehen verschlossenen Containern zu entsorgen.
- Fernzugriff nur über gesicherte VPN-Verbindung mit Zwei-Faktor-Anmeldung
- Sicherung durch Firewall. Regelmäßige Überprüfung der Firewallprotokolle
- Einsatz von Virens Scanner auf allen Computern.
- Verpflichtung unseres Cloudspeicher-Anbieters auf Datensicherheit nach Stand der Technik
- Weitergabe an Dienstleister zur Datenvernichtung nur in verschlossenen Containern. Verpflichtung des Dienstleisters auf datenschutzkonforme Datenvernichtung.

2.2 Eingabekontrolle

- Protokollierung der Dateneingaben der verwendeten IT-Systeme
- Zentrale Administration der Zugriffsrechte (Laufwerke, Verzeichnisse, Dateien) über IT-Abteilung nach Freigabe durch Fachverantwortliche
- Separate Administrationsaccount für Verwaltung der Zugriffsrechte
- Sofern möglich, Zugriff über Single Sign On
- Zugriffsberechtigungen werden nach Aufgaben der Mitarbeiter vergeben

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

- Speicherung aller Daten in einem ISO 27001 zertifizierten Rechenzentrum
- Regelmäßige Sicherung der Daten in Rechenzentrum
- Verpflichtung der Mitarbeiter, persönlichen oder sensiblen Daten nicht ausschließlich lokal speichern

4. Regelmäßige Überprüfung, Bewertung und Evaluierung

4.1 Incident-Response-Management

- Interner Prozess zur Meldung, Diagnose, Dokumentation und Behebung aller Vorfälle
- Alle relevanten Vorfälle werden unmittelbar an den globalen IT-Sicherheitsbeauftragten (CISO) der Havas gemeldet
- Rechenzentrum an externen Standort (Frankfurt am Main und Berlin) reagiert auf Vorfälle gemäß ISO 27001 Zertifizierung

4.2 Datenschutzfreundliche Voreinstellungen

- Berücksichtigung von Privacy by design und Privacy by default bei der Anschaffung von Hard- oder Software sowie der Prüfung interner Verfahren
- Empfang und Weitergabe von persönlichen Daten, falls unter Berücksichtigung des jeweiligen Verarbeitungszwecks möglich, nur anonymisiert oder pseudonymisiert

4.3 Auftragskontrolle

- Sorgfältige Auswahl von Auftragsverarbeitern bzw. Unterauftragsverarbeitern
- Verpflichtung aller Dienstleister für die Verarbeitung von persönlichen Daten auf Einhaltung der datenschutzrechtlichen Anforderungen über Auftragsverarbeitungsverträge
- Verarbeitung im Auftrag erfolgt nur nach Weisung des Auftraggebers
- Prüfung aller Datenverarbeitungsverträge durch den Datenschutzbeauftragten

4.4. Datenschutz-Management

- Ernennung eines Datenschutzbeauftragten und von Datenschutzkoordinatoren in den einzelnen Fachabteilungen
- Regelmäßiger Austausch zwischen Datenschutzbeauftragten, Datenschutzkoordinatoren und IT-Abteilung
- Verbindliche interne Datenschutz- und IT-Sicherheits-Richtlinien für alle Beschäftigten
- Schulung von allen Beschäftigten
- Regelmäßige Prüfung aller Verfahren zur Verarbeitung von persönlichen Daten durch den Datenschutzbeauftragten

Anlage 2 (als Beispiel, zukünftig eine Liste der Subauftragsdatenverarbeiter der Partnerkliniken als Anlage 2 zum AVV anfügen.)

Subunternehmer des Auftragsverarbeiters (Partnerkliniken)

Unterauftragnehmer	Adresse	Ort der Verarbeitung	Zweck der Verarbeitung	Kategorie von betroffenen Personen	Arten personenbezogener Daten
DAP GmbH	Gärtnerweg 4-8, 60322 Frankfurt am Main	EU / EWR	Verwaltung des Kundenstammdaten	Beschäftigte des Auftraggebers	Berufliche Kontaktinformationen
Google Ireland Limited	Gordon House Barrow Street, Dublin 4, Irland	EU / EWR, USA und andere Länder (Standardvertragsklauseln)	Erfolgsmessung Online-Marketing-Maßnahmen	Besucher von Websites des Auftraggebers und von Websites auf denen Online-Werbung platziert wird	Siehe: https://privacy.google.com/businesses/adsservices/
Interoute Germany GmbH (part of GTT Communications, Inc.)	Weismüllerstraße 26, 60314 Frankfurt	EU / EWR	Rechenzentrum / IT-Infrastruktur	Alle im Rahmen dieses Vertrages übermittelten Daten	Alle im Rahmen dieses Vertrages übermittelten Daten
mediarithmics	10 rue Notre Dame, 94120, Fontenay-sous-Bois, Frankreich	EU / EWR	Data Management zur 1. Bereitstellung zielgerichteter personalisierter Werbe-Inhalte für Endkunde, Nutzer oder potenzielle Endkunden des	Besucher von Websites des Auftraggebers und von Websites auf denen Online-Werbung platziert wird; Umfrageteilnehmer; Personen deren	Daten zu persönlichen Merkmalen und demographische Informationen; Verhaltensdaten; Navigationsverhalten; Online-Werbekennungen; und Technische Informationen; Alle anderen Informationen, die eine Person identifizieren oder identifizieren könnten

			Auftraggebers 2. Verbesserung des Wissens über Endkunden, Nutzer oder potenzielle Endkunden des Auftraggebers	Daten in Datensätzen von Drittanbietern enthalten sind; Alle anderen Kategorien von betroffenen Personen, deren personenbezogene Daten verarbeitet werden	
Microsoft Ireland Operations, Ltd.	Attn: Data Protection One Microsoft Place South County Business Park Leopards town Dublin 18 D18 P521	EU / EWR	Email-Kommunikation (Outlook), Reporting (Power-BI, Excel), Cloud-Dienste (z.B.: OneDrive, Sharepoint und Azure)	Alle im Rahmen dieses Vertrages übermittelten Daten	Alle im Rahmen dieses Vertrages übermittelten Daten
Newsletter2Go GmbH	Nürnberg er Straße 8, 10787 Berlin	EU / EWR	Newsletterversand	Beschäftigte des Auftraggebers	Berufliche Kontaktinformationen

Impressum

Avelios Medical GmbH

Ridlerstraße 39
80339 München

Deutschland

Vertreten durch die Geschäftsführer:

Christian Albrecht, Nicolas Jakob

Kontakt:

Kontaktformular: [Hier klicken](#)

Allgemein: info@avelios.com

Jobs: recruiting@avelios.com

Eintragung im Handelsregister:

Handelsregister München
HRB 270765

Tax-ID: DE334616294

Verantwortlicher i.S.d. § 55 Abs. 2 RStV für die journalistisch-redaktionellen Inhalte: Avelios Medical GmbH (Anschrift wie oben).

Hinweis gem. ODR-Verordnung: Die Europäische Kommission stellt eine Plattform zur Online-Streitbeilegung bereit, die Sie unter <https://ec.europa.eu/consumers/odr> finden. Wir sind jedoch nicht bereit und verpflichtet an der Online-Streitbeilegung teilzunehmen.